UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

TEMA:

"IMPLEMENTACIÓN DEL DATACENTER DE OFICINA MATRIZ DE LA EMPRESA FARMAENLACE CÍA. LTDA. EN LA CIUDAD DE QUITO, CONSIDERANDO LAS RECOMENDACIONES DE LA NORMA TIA-942, Y CONFIGURANDO SERVICIOS DE ADMINISTRACIÓN DE SISTEMAS BAJO PLATAFORMA WINDOWS."

Autor: Marco Ramírez Flores

Director: Ing. Jorge Caraguay Procel

Ibarra – Ecuador

2012

CERTIFICACIÓN

Certifico que la Tesis que lleva por tema: "**IMPLEMENTACIÓN DEL DATACENTER DE OFICINA MATRIZ DE LA EMPRESA FARMAENLACE CÍA. LTDA. EN LA CIUDAD DE QUITO, CONSIDERANDO LAS RECOMENDACIONES DE LA NORMA TIA-942, Y CONFIGURANDO SERVICIOS DE ADMINISTRACIÓN DE SISTEMAS BAJO PLATAFORMA WINDOWS.**", previo a la obtención del Título de Ingeniero en Sistemas Computacionales, ha sido realizada en su totalidad por el señor Marco Ramírez Flores, portador de la cédula de identidad número 1002531133 con interés profesional y responsabilidad, lo cual certifico en honor a la verdad.

Ing. Jorge Caraguay P.

Director de la Tesis

CERTIFICACIÓN

Quito, 21 de julio del 2012

Señores

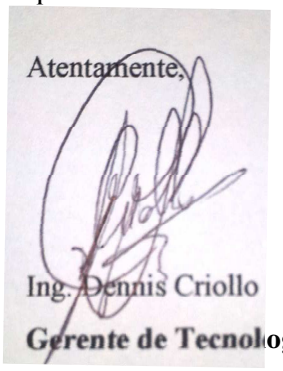
UNIVERSIDAD TÉCNICA DEL NORTE

Presente

De mis consideraciones.-

Yo, Ing. Dennis Criollo, en mi calidad de Gerente del Departamento de Tecnología y Sistemas de Farmaenlace Cía. Ltda., siendo auspiciantes del proyecto de tesis del señor Marco Ramírez Flores que lleva por tema: **"IMPLEMENTACIÓN DEL DATACENTER DE OFICINA MATRIZ DE LA EMPRESA FARMAENLACE CÍA. LTDA. EN LA CIUDAD DE QUITO, CONSIDERANDO LAS RECOMENDACIONES DE LA NORMA TIA-942, Y CONFIGURANDO SERVICIOS DE ADMINISTRACIÓN DE SISTEMAS BAJO PLATAFORMA WINDOWS."**, me es grato informar que se han superado con satisfacción las pruebas técnicas y la revisión de cumplimiento de los requerimientos funcionales, por lo que se recibe el proyecto como culminado y realizado por parte del egresado Marco Ramírez Flores. Una vez que hemos recibido la documentación respectiva, nos comprometemos a aprovechar este proyecto implementado en beneficio de nuestra empresa.

El egresado Marco Ramírez Flores puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.



Gerente de Tecnología y Sistemas
FARMAENLACE CÍA. LTDA.

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE INVESTIGACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, MARCO RAMÍREZ FLORES, con cédula de identidad Nro. 100253113-3, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, articulo 4, 5 y 6, en calidad de autor del trabajo de grado denominado: **"IMPLEMENTACIÓN DEL DATACENTER DE OFICINA MATRIZ DE LA EMPRESA FARMAENLACE CÍA. LTDA. EN LA CIUDAD DE QUITO, CONSIDERANDO LAS RECOMENDACIONES DE LA NORMA TIA-942, Y CONFIGURANDO SERVICIOS DE ADMINISTRACIÓN DE SISTEMAS BAJO PLATAFORMA WINDOWS."**, que ha sido desarrollada para optar por el título de Ingeniería en Sistemas Computacionales, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autor me reservo los derechos morales de la obra antes mencionada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para ningún grado o calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

Firma:.....

Nombre: MARCO RAMÍREZ FLORES

Cédula: 1002531133

Ibarra, a los 21 días del mes de julio del 2012

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO DE PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del Proyecto Repositorio Digital institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad.

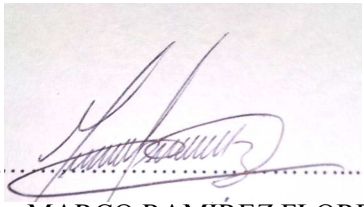
Por medio del presente documento, dejo sentada mi voluntad de participar en este proyecto, para lo cual ponemos a disposición la siguiente investigación:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD	1002531133
APELLIDOS Y NOMBRES	RAMÍREZ FLORES MARCO
DIRECCIÓN	Quito, Carlos Andrade Marín N-4836 y Av. Cap. Rafael Ramos
EMAIL	marcoramirez@farmaenlace.com
TELÉFONO FIJO	02-2993-100
TELÉFONO MÓVIL	09-6484-568

DATOS DE LA OBRA	
TITULO	**"IMPLEMENTACIÓN DEL DATACENTER DE OFICINA MATRIZ DE LA EMPRESA FARMAENLACE CÍA. LTDA. EN LA CIUDAD DE QUITO, CONSIDERANDO LAS RECOMENDACIONES DE LA NORMA TIA-942, Y CONFIGURANDO SERVICIOS DE ADMINISTRACIÓN DE SISTEMAS BAJO PLATAFORMA WINDOWS"**
AUTOR	RAMÍREZ FLORES MARCO
FECHA	21 DE JULIO DE 2012
PROGRAMA	PREGRADO
TITULO	INGENIERÍA EN SISTEMAS COMPUTACIONALES
DIRECTOR	ING. JORGE CARAGUAY PROCEL

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, MARCO RAMÍREZ FLORES, con cédula de identidad Nro. 1002531133, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la biblioteca de la universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior Artículo 143.



Firma:……

Nombre: MARCO RAMÍREZ FLORES

Cédula: 100253113-3

Ibarra, a los 21 días del mes de julio del 2012

DEDICATORIA

A Dios, el único fundamento y propósito de mi vida, que día a día me ha dado la fortaleza y la constancia para sacar adelante este proyecto, sin el cual el motivo de mi existencia pierde todo sentido y por Él he llegado a culminar y alcanzar esta anhelada meta.

A mis padres, que con su apoyo y su confianza depositada, produjeron en mí el anhelo de llegar a ser un profesional y que dedicara mi tiempo y mis recursos a lograr este gran objetivo en mi vida.

AGRADECIMIENTO

A mi familia entera, por su apoyo y consejos, inculcando en mi altos valores de responsabilidad y perseverancia, elementos esenciales en la vida de todo ser humano que desea progresar en su vida.

A Farmaenlace Cía. Ltda., sus directivos y colaboradores en general, que me brindaron la oportunidad de formar parte de esta empresa que es más una familia, con un mismo sentir y visión de progreso, en especial al Ing. Dennis Criollo Gerente de Sistemas, quien depositó su confianza en mí para sacar adelante este proyecto.

A todos los colaboradores y amigos del área técnica, incluyendo proveedores y asesores de empresas externas, que supieron dar pautas y guías para llegar a feliz término el presente proyecto.

A mi director de Tesis, Ing. Jorge Caraguay, quien me ha guiado con su oportuna opinión y consejos durante todo el proceso de desarrollo de esta Tesis.

A la Universidad Técnica del Norte, una de las mejores instituciones de educación superior en el territorio Ecuatoriano, en especial a la Facultad de Ingeniería en Ciencias Aplicadas y a la Carrera de Ingeniería en Sistemas computacionales, por todos los conocimientos impartidos para salir adelante como un nuevo profesional, con visión de servicio y colaboración por el progreso del país.

TABLA DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

RESUMEN

El presente documento, plasma el trabajo realizado en la implementación del DataCenter de Farmaenlace Cía. Ltda., documentando los pasos realizados y los temas a considerar; antes, durante y después del proceso de implementación, pudiendo ser utilizado como guía de consulta para casos de migración de sistemas e infraestructura tecnológica que contenga similares características.

El proceso inicia realizando una introducción y detalle de los antecedentes de la empresa auspiciante, contiene toda la información recabada, sus características, detalles arquitectónicos del DataCenter y la distribución de la red interna, servicios y equipamiento implementado; con toda esta información se realiza un levantamiento de todos los requerimientos necesarios para la realización del proyecto, en los aspectos: arquitectónico, de equipamiento, servicios y documentación, elementos primordiales para el desarrollo del proyecto hasta su culminación.

A continuación, es necesario recopilar la información necesaria que muestra en resumen todo el fundamento teórico que respalda la ejecución del proyecto, este resumen teórico contiene datos acerca de fundamentos de redes, tipos de redes, topología física y lógica, capas de transmisión de datos, descripción de comunicaciones, resumen de las recomendaciones de la norma TIA-942 para el diseño e implementación de DataCenter y fundamentos teóricos de los servicios de administración bajo plataforma Windows, Active Directory, DHCP, DNS y servicios de actualizaciones, toda esta información conforma el punto de consulta y guianza utilizada para generar recomendaciones, configuración y documentación necesaria en la implementación del DataCenter de Farmaenlace Cía. Ltda.

Con los antecedentes y fundamentos obtenidos, se da inicio a la implementación del proyecto referente a la infraestructura física del DataCenter de Farmaenlace Cía. Ltda., tomando en cuenta todas las recomendaciones de la norma TIA-942 para todos los aspectos que incluye la implementación de un DataCenter, tales como en lo eléctrico: instalaciones eléctricas, respaldo de energía con UPS y generadores; en el flujo de aire: definición de pasillos calientes y pasillos fríos y adquisición de sistemas de aire

acondicionado de precisión, detalles de locación y accesos. Además las características de todo el equipamiento que se adquirió: equipos de comunicaciones y servidores para complementar la infraestructura del DataCenter, se incluye además diagramas de documentación de la red de la empresa.

Luego de la implementación física, continua la implementación de servicios de administración y prestaciones para ser entregados a toda la empresa como Active Directory, donde se define los grupos o unidades organizativas, los permisos de acceso con los que se configuran las políticas de seguridad para todo el personal de la empresa, servicios DHCP y asignación de direcciones bajo reserva, para concesión de acceso a sistemas específicos o navegación por internet de manera personalizada para grupos de usuarios, y configuración de servicios de actualizaciones automáticas, lo que complementa al proyecto en cuanto a la implementación de servicios.

Como punto culminante del proyecto se elabora la documentación dedicada a procedimientos y políticas necesarios para el correcto funcionamiento y aprovechamiento de todos los recursos de la empresa, consta de recomendaciones y pasos a seguir para realizar configuraciones de los servicios que brinda la empresa como: correo electrónico, accesos a los sistemas, etc. También se documenta procedimientos de contingencia básicos para la recuperación de servicios en caso de una falla, con lo que se convierte en un material de consulta y guía para personal técnico de la empresa que necesite acceder a la administración de los sistemas.

Durante este proceso se contó con el apoyo y consultoría de varios proveedores externos, quienes basándose en normas y experiencias similares supieron dar pautas al Departamento de Sistemas y principalmente al área de Administración de Servicios Redes y Telecomunicaciones para lograr el objetivo planteado, tratando de minimizar en lo posible el impacto al usuario final.

El cumplimento de este proceso estuvo bajo la dependencia principalmente del factor económico, que limitó en algunas ocasiones el apego completo a las normas, debiendo complementar los trabajos con soluciones alternas pero que cubren las necesidades de la empresa, sin embargo, se continua con las recomendaciones de mejoramiento y se espera poder implementarlas en un futuro cercano.

SUMMARY

This document, represents the work done in the implementation of Farmaenlace Co. DataCenter. Ltd., documenting the steps taken and issues to consider before, during and after the implementation process and can be used as a reference guide in case of migration of systems and technology infrastructure that contains similar characteristics.

The process begins by performing a detailed introduction and background of the sponsoring company contains all the information collected, its features, architectural details of the DataCenter and distribution of the internal network, services and equipment in place and with all this information is carried out a survey of all requirements for the project in architectural aspects, equipment, services and documentation, essential elements for the project to completion.

Then it need to gather the necessary information that provides an overview of all the theoretical foundation behind the project, this theoretical summary contains data on network fundamentals, types of networks, physical and logical topology, layers of data, description communication, summary of the recommendations of the TIA-942 standard for the design and implementation of DataCenter and theoretical foundations of management services under Windows, Active Directory, DHCP, DNS and updates, all this information forms the point of consultation and guidance used to generate recommendations, configuration and documentation required in the implementation of Farmaenlace Co. DataCenter. Ltd.

With the background and rationale obtained initiates the implementation of the project concerning the physical infrastructure of Farmaenlace Co. DataCenter. Ltd., taking into account all the recommendations of the TIA-942 standard for all aspects including the implementation of a DataCenter, such as in electricity: electrical systems, backup power with UPS and generators, in the air flow: definition of hot aisles and cold aisles and acquisition of air-conditioners, location and access details. Also features all the equipment was purchased communications equipment and servers to complement DataCenter infrastructure, also includes diagrams of network documentation of the company.

Following implementation of continuous physical implementation and performance management services to be delivered to the entire company as Active Directory, which

defines the groups or organizational units, the access permissions that are configured with security policies for all company personnel, services and DHCP address assignment subject to granting access to specific systems or Internet browsing in a personalized way for groups of users, and configure Automatic Updates service, which complements the project in terms of implementation services.

As a highlight of the project documentation is produced dedicated to procedures and policies necessary for the proper functioning and utilization of all resources of the company, consists of recommendations and next steps for service configurations offered by the company as email, access to systems, etc. Also documented contingency procedures for the recovery of basic services in the event of a failure thus becomes a reference material and guidance for technical staff who need access to enterprise management systems.

During this process had the support and consultancy of various external suppliers who rules based on similar experiences and were able to give guidance to the Department of Systems and mainly to the administration area of Networking and Telecommunications Services to achieve the stated goal of trying to minimize the possible the impact end user.

The fulfillment of this process was mainly dependent on the economic factor limiting sometimes the complete attachment to the rules must complement the work but with alternate solutions that meet the needs of the company, however we continue with the recommendations for improvement and we expect to implement in the near future.

CAPÍTULO 1

1 INTRODUCCIÓN

FARMAENLACE CIA. LTDA. se inició como una empresa de distribución farmacéutica y cadena de farmacias en el año 2005, luego de la fusión de dos importantes empresas distribuidoras del campo farmacéutico: FARMALIDERES y REPRESENTACIONES ORTIZ CEVALLOS, quienes ocupaban los primeros sitiales en el mercado. En el año 2005 estas empresas deciden unir esfuerzos y formar un solo y gran emporio, que ocupara un alto porcentaje del mercado y tuviera miras de crecimiento, tanto en el área de distribución, como en puntos de venta al público en todo el país. Dando origen a FARMAENLACE Cía. Ltda., empresa que empieza a expandirse rápidamente con las marcas: FARMACIAS ECONÓMICAS y FARMACIAS MEDICITY, en varias ciudades

del país como: Quito, Cayambe, Santo Domingo, Ambato, Riobamba, Latacunga, Ibarra, Otavalo, Cotacachi, Tulcán, San Gabriel, Lago Agrio, El Coca y Cuenca.

Tecnológicamente, Farmaenlace emprende con pocos equipos de cómputo y servidores, para suplir las necesidades principales de administración y contabilidad, también en el área de comunicaciones inicia con una central telefónica análoga y enlaces dedicados de datos, únicamente con las principales farmacias y oficinas remotas en la ciudad de Ibarra.

Paulatinamente, con el crecimiento de Farmaenlace, se agregaron nuevos servidores más robustos para poder manejar un ERP[1] empresarial y servicios adicionales, como correo y navegación. Conforme crecía la empresa, se iban presentando y haciendo más evidentes las necesidades de automatización de nuevos procesos, es por esto que el ERP adquirido inicialmente, ya no cubría las expectativas y fue necesario desarrollar puertas adentro nuevas aplicaciones y también coordinar la implementación de un nuevo ERP de propiedad conjunta con una empresa de desarrollo, que pudiera crecer y adaptarse tanto como la empresa lo requiere.

Luego de varias reuniones conjuntas con el personal de administración de sistemas, se realizó el levantamiento de varios parámetros determinantes para la realización del presente proyecto, considerando: servicios, aplicaciones, servidores, infraestructura de comunicaciones, distribución de usuarios en el edificio matriz, locación de equipos servidores, nuevos equipos por implementar, seguridades tanto físicas como seguridad de la información, utilización y reemplazo de equipos, enlaces de datos y comunicaciones telefónicas.

Para iniciar el proyecto, se considera el levantamiento de características e inventario de equipos instalados en DataCenter de Farmaenlace Cía. Ltda., como se describe a continuación. Con esta información, se podrá tomar una decisión de cómo se realizará el proyecto, para alcanzar el objetivo de implementar un DataCenter adecuado a las necesidades de la empresa.

1.1 Infraestructura de Data-Center Farmaenlace Cía. Ltda.

El DataCenter o Centro de Procesamiento de Datos (CPD), es el sitio donde se agrupan todos los recursos necesarios para el procesamiento de información y comunicaciones de

[1] ERP: (Enterprise Resource Planning) - Software de información centralizada, orientado a registrar e integrar la mayoría de los procesos de negocios.

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

Como objetivo, Farmaenlace necesita tener un DataCenter adecuado para almacenar todos los datos de sus clientes y las operaciones que realizan pertinentes al negocio, tanto en matriz como en sucursales. Para garantizar la continuidad del servicio a clientes, empleados, proveedores y empresas colaboradoras. En este lugar es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

El DataCenter o centro de cómputo de Farmaenlace Cía. Ltda., al iniciarse el proyecto es un área de 2,7 x 3 metros aproximadamente, ubicada en la planta alta del edificio de la empresa, junto a las oficinas del Área de Servicios y Redes del Departamento de Sistemas, como muestra el diagrama a continuación:

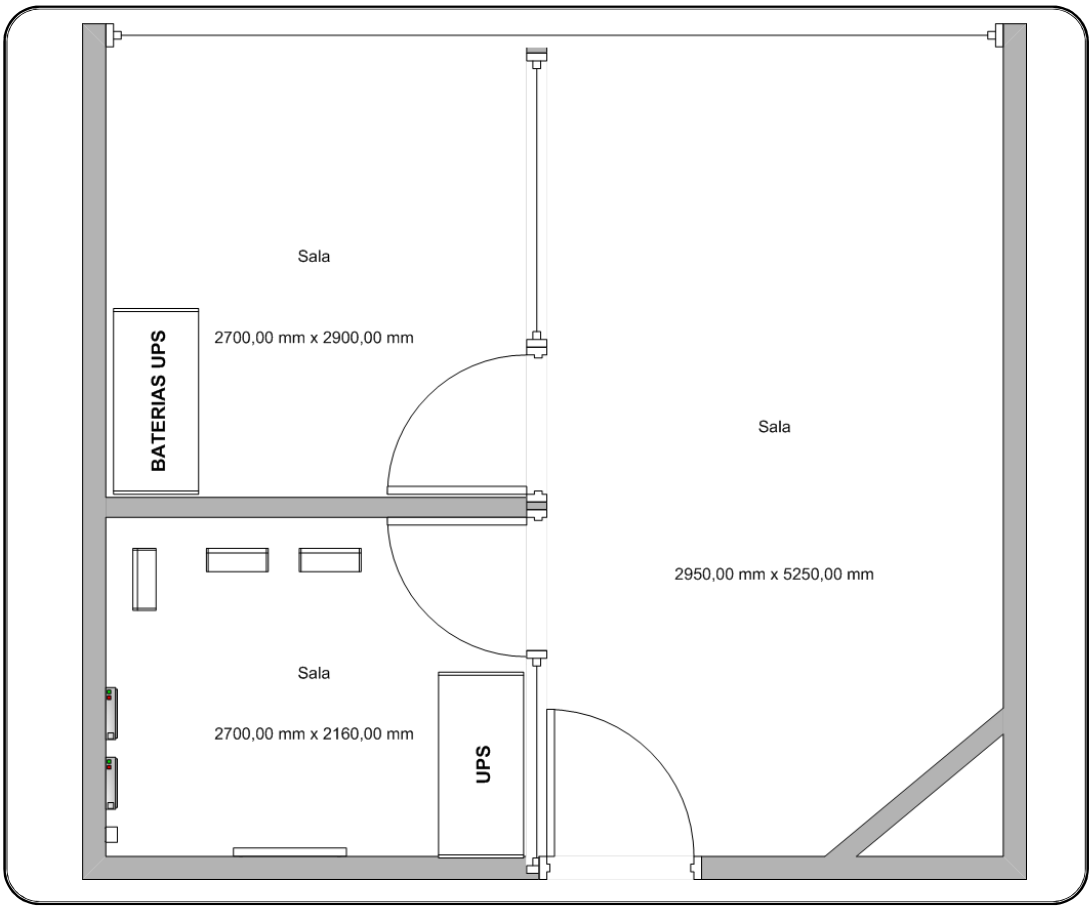


Ilustración 1:1 Datacenter Farmaenlace al inicio del proyecto

En su infraestructura física, cuenta con tres rack[2] abiertos de torre, organizados de la siguiente manera:

Rack 1 Cableado estructurado.- Contiene puntos de voz y datos del cableado horizontal de planta alta y planta baja del edificio de Farmaenlace, además de las tomas para las líneas telefónicas de la central análoga, organizadas en patch panels [3]y numeradas según su ubicación y tipo de servicio. El cableado estructurado se encuentra diseñado bajo cable Categoría 5e con switches 3com 2460.

Rack 2 Comunicaciones y servidores.- En este rack se encuentran los servidores y equipos de comunicaciones de:

a) Aplicaciones y base de datos del sistema LISA (ERP).- Corresponde al sistema de gestión empresarial que utilizó Farmaenlace en un inicio para manejo de los aspectos administrativos y contables, al volverse insuficiente debido al crecimiento que tiene la empresa es necesario reemplazarlo por el nuevo ERP diseñado por Farmaenlace con propiedad intelectual conjunta con Easysoft empresa de desarrollo de software. En el momento de la implementación de este proyecto Farmaenlace se encuentra en la transición de los sistemas ERP.

b) Aplicaciones y base de datos del sistema Gestión Empresarial EASYSOFT[4] (ERP).- Nuevo sistema ERP diseñado para ajustarse a las necesidades y crecimiento de Farmaenlace, para gestionar los campos administrativos, contables, y de manejo de inventarios; con posibilidad de crecimiento continuo, debido a que se pueden diseñar nuevos módulos y sistemas que tengan comunicación y centralización de la información, de manera constante y automática.

c) Servidor central del sistema TINI .- El sistema TINI se encuentra instalado en los puntos de venta de Farmaenlace, se encuentra diseñado en FoxPro y funcionando en la mayoría de puntos de venta a nivel nacional,

[2] RACK: **soporte metálico** destinado a alojar equipamiento electrónico, informático y de comunicaciones
[3] Patch Pannel: elemento encargado de recibir todos los cables del cableado estructurado, sirve como un organizador de las conexiones de la red
[4] EASYSOFT: Empresa Ecuatoriana desarrolladora de software que desarrolló el software de gestión empresarial sobre el cual Farmaenlace trabaja y desarrolla aplicaciones de propiedad intelectual conjunta.

posteriormente sería reemplazado por el sistema FARMAPOS[5] diseñado internamente por el equipo de desarrollo de Farmaenlace, basándose en la estructura del sistema Gestión Empresarial Easysoft.

d) Servidor de Control de Horarios Biométrico.- Equipo que recoge la información recabada por un lector biométrico, para registrar los horarios de ingreso y salida de personal que labora en Farmaenlace Cía. Ltda.

e) Ruteador de enlace dedicado hacia las farmacias.- Considerado como el router principal de Farmaenlace Cía. Ltda., equipo que se encarga de las comunicaciones de enlaces dedicados hacia oficinas y puntos de venta, provisto por el proveedor de enlaces Corporación Nacional de Telecomunicaciones (CNT).

f) Ruteador de Internet.- Equipo de ruteo encargado de brindar el servicio de Internet corporativo, servicio Provisto por Corporación Nacional de Telecomunicaciones (CNT).

g) Ruteador de enlace secundario de Internet y de Correo Electrónico.- Farmaenlace Cía. Ltda. mantiene un servicio de Internet alterno, utilizado principalmente para el servicio de envío y recepción de Correo Electrónico, configurado como enlace de Internet Backup en caso de una falla del enlace Principal, este servicio es provisto por el ISP[6] PowerFast.

Rack 3 Monitoreo y Servidores Linux.- En este rack se encuentra la consola para administración de servidores mediante un dispositivo Switch KVM [7],que permite con una interfaz de monitor, teclado y mouse, conectarse a los diferentes servidores. En la parte inferior se encuentran dos servidores con sistema Linux, encargados de proveer a la red interna servicios de navegación, firewall y correo electrónico corporativo respectivamente.

1.1.1 Inventario de equipos Servidores

[5] FARMAPOS: Software de punto de venta desarrollado por Farmaenlace Cía. Ltda. Para su cadena de farmacias.
[6] ISP: Internet Service Provider, empresa que brinda conexión a Internet a sus clientes
[7] Switch KVM: (Keyboard-Video-Mouse) dispositivo que permite el control de distintos equipos informáticos con un sólo monitor, teclado y ratón

A continuación se describe las características de los equipos computacionales ubicados dentro del DataCenter de Farmaenlace Cía. Ltda.

a) Lisa Aplicaciones

1. Modelo: HP PROLIANT ML370 G4
2. Procesador: Intel Xeon 3.4Ghz
3. Disco Duro:2 discos SCSI 72 Gb
4. Memoria RAM: 4 GB
5. Red:1 LAN 1 Gbps
6. Sistema Operativo: Windows 2003 Enterprise Server
7. Año de Fabricación: 2005

b) Lisa Base de Datos

1. Modelo: HP PROLIANT DL 380 G5
2. Procesador: Intel Xeon 3.4Ghz
3. Disco Duro:8 Discos serial SCSI 146GB
4. Memoria RAM: 8GB
5. Red:1 LAN 1Gbps
6. Sistema Operativo: Windows 2003 Enterprise Server
7. Software: Sql Server 2000 SP3
8. Año de Fabricación: 2007

c) Easy Soft Aplicaciones

1. Modelo: HP Proliant ML370 G5
2. Disco Duro:2 Discos serial SCSI 146GB
3. Memoria RAM: 8GB
4. Red:1 LAN 1Gbps
5. Sistema Operativo: Windows 2003 Enterprise Server
6. Año de Fabricación: 2007

d) Easy Soft Base de Datos

1. Modelo: HP Proliant ML370 G5
2. Disco Duro: 4 Discos serial SCSI 146GB
3. Memoria RAM: 8GB
4. Red:1 LAN 1Gbps
5. Sistema Operativo: Windows 2003 Enterprise Server
6. Software: Sql Server 2005 Estándar Edition
7. Año de fabricación: 2007

e) Tini Central

1. Modelo: CLON
2. Procesador: Intel Core 2 Duo 2.8Ghz
3. Disco Duro: 1 Disco 100GB
4. Memoria RAM: 2GB
5. Red:1 LAN 100Mbps
6. Sistema Operativo: Windows 2003 Enterprise Server
7. Año de Fabricación: 2005

f) Biométrico

1. Modelo: CLON
2. Procesador: Intel Pentium IV 2.66Ghz
3. Disco Duro: 1 Disco 80GB
4. Memoria RAM: 1GB
5. Red:1 LAN 100Mbps
6. Sistema Operativo: Windows XP Professional
7. Año de Fabricación: 2006

g) Linux Correo Corporativo

1. Modelo: CLON
2. Procesador: Intel Pentium IV 2.66Ghz
3. Disco Duro: 1 Disco 160GB
4. Memoria RAM: 2GB
5. Red: 2 LAN 100Mbps
6. Sistema Operativo: Linux Centos 5.3
7. Año de Fabricación: 2006

h) Linux Navegación y Firewall

1. Modelo: CLON
2. Procesador: Intel Core 2 duo 2.4Ghz
3. Disco Duro: 1 Disco 160GB
4. Memoria RAM: 2GB
5. Red: 2 LAN 100Mbps
6. Sistema Operativo: Linux Centos 5.3
7. Año de Fabricación: 2008

i) Servidor PL

1. Modelo: HP PROLIANT ML370 G4
2. Procesador: Intel Xeon 3.4Ghz
3. Disco Duro: 5 discos SCSI 72 Gb

4. Memoria RAM: 4 GB
5. Red:1 LAN 1 Gbps
6. Sistema Operativo: Windows 2003 Enterprise Server
7. Año de Fabricación: 2006

1.1.2 Inventario de equipos de redes y comunicaciones

a) Router Cisco 2600 para servicio de Internet 2Mbps
b) Router Cisco 1800 para servicio de enlace de datos con farmacias
c) Modem ADSL Huawei enlace secundario de Internet 256 Kbps
d) Bandeja de Conexión de Fibra Óptica para enlaces de datos e Internet
e) Transeiver de Fibra Óptica a Ethernet 10/100 Mbps para interconectar la fibra óptica con los ruteadores.
f) 2 Swich 3com 24 puertos 10/100 no administrables
g) 1 Switch Alied Telesyn 24 puertos 10/100/1000 semi-administrable.
h) Central telefónica Panasonic kx-td816 con modulo adicional para E1 y 8 líneas troncales

1.1.3 Servicios Implementados

Los servicios implementados en Farmaenlace Cía. Ltda.

a) Sistema ERP LISA Farmaenlace: manejo de información empresarial, administrativa, contable
b) Sistema ERP EasyFarma (en desarrollo) maneja información empresarial, administrativa contable, que una vez desarrollado por completo reemplazará a LISA Farmaenlace.
c) Sistema TINI que centraliza la información de ventas de las farmacias a nivel nacional recibidas diariamente por correo electrónico generadas en los puntos de venta TINI a nivel Nacional.
d) Sistema para registrar horarios de acceso del personal con un dispositivo lector biométrico que detecta la forma y estructura de mano del colaborador para registrarlo.
e) Servicio de Correo Electrónico corporativo bajo el dominio farmaenlace.com
f) Sistema PL (Programa de Logística) para manejo de certificación de pedidos y traspasos de mercadería en bodega y coordinación de logística de transporte.

1.2 Distribución de red LAN

A continuación, se presenta los diagramas de red de las instalaciones de Farmaenlace Cía. Ltda., punto de partida para el estudio de asignación de nuevos puntos y movimiento del personal en las instalaciones.

1.2.1 Plano de distribución LAN Farmaenlace

1. Planta Alta

En esta área se encuentran ubicadas las oficinas de los vicepresidentes ejecutivos y sus asistentes, el personal de adquisiciones, dos salas de reuniones, el DataCenter de Farmaenlace, las oficinas de administración de sistemas, las oficinas del área comercial, ventas, operaciones y manejo de las marcas de la empresa.

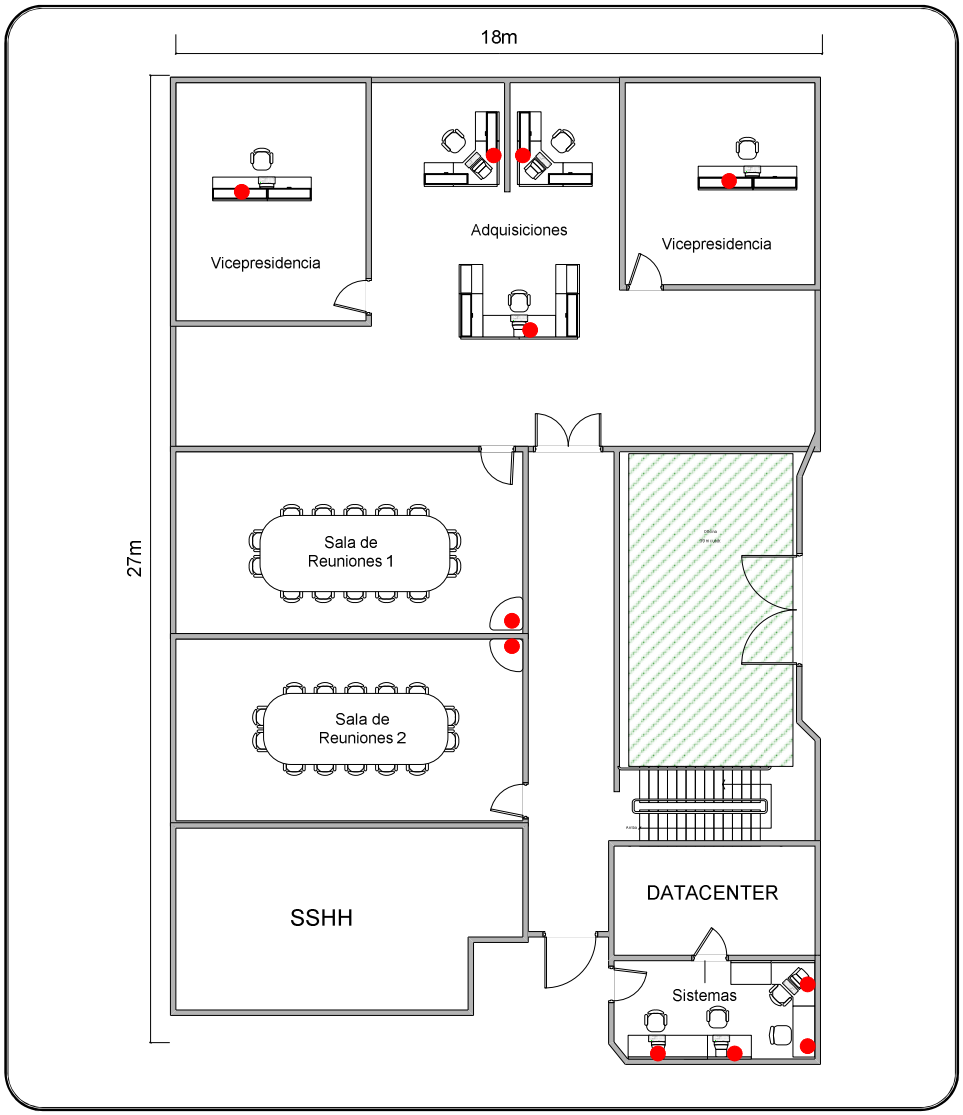


Ilustración 1:2 LAN Edificio Farmaenlace Planta Alta

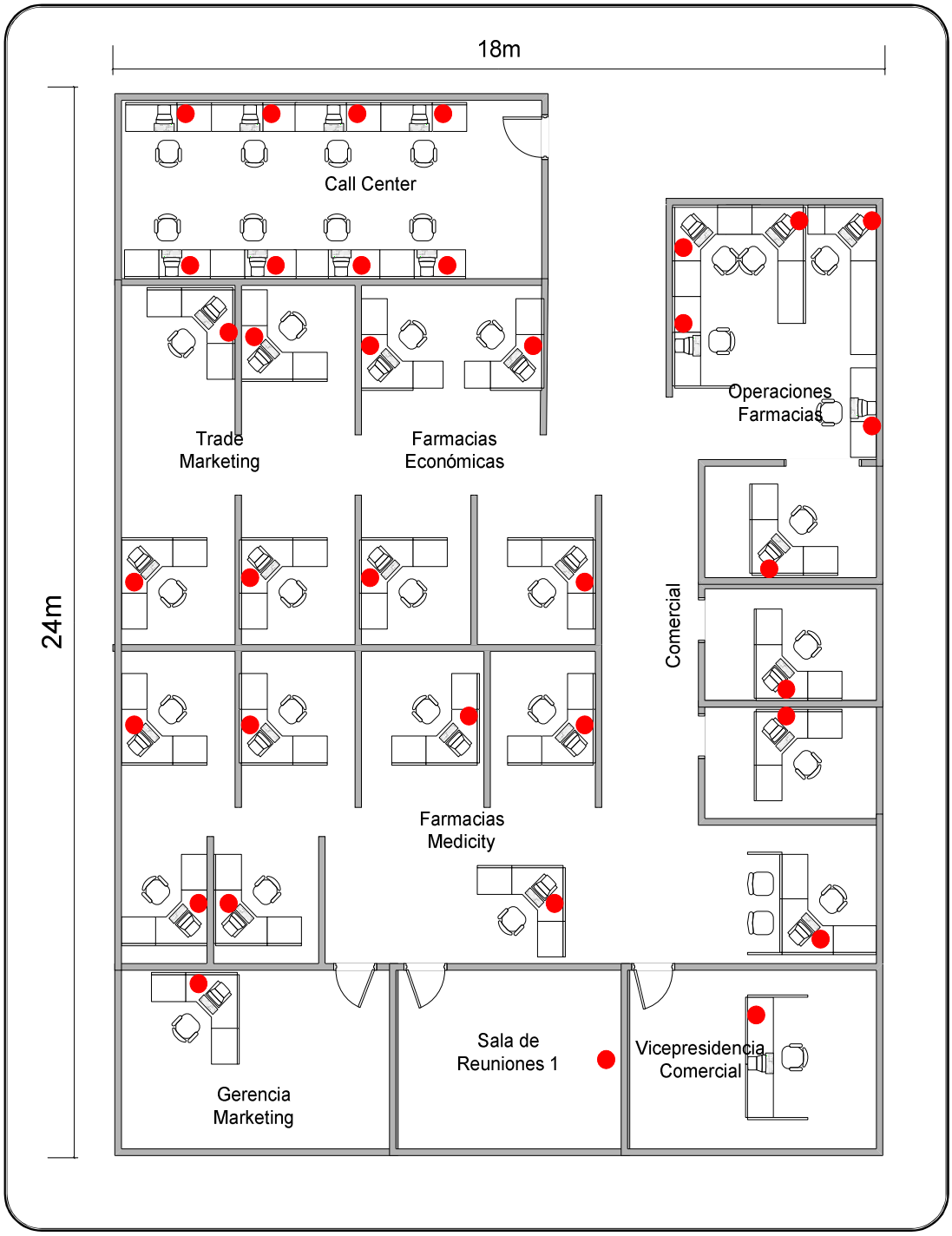


Ilustración 1:3 LAN Edificio Farmaenlace Planta Alta 2

2) Planta Baja

En esta área, se encuentran ubicados el auditorio de Farmaenlace, recepción y salas de reuniones para atención a visitantes, el área de administración general de Farmaenlace y los departamentos de crédito, cobranzas y auditoria.

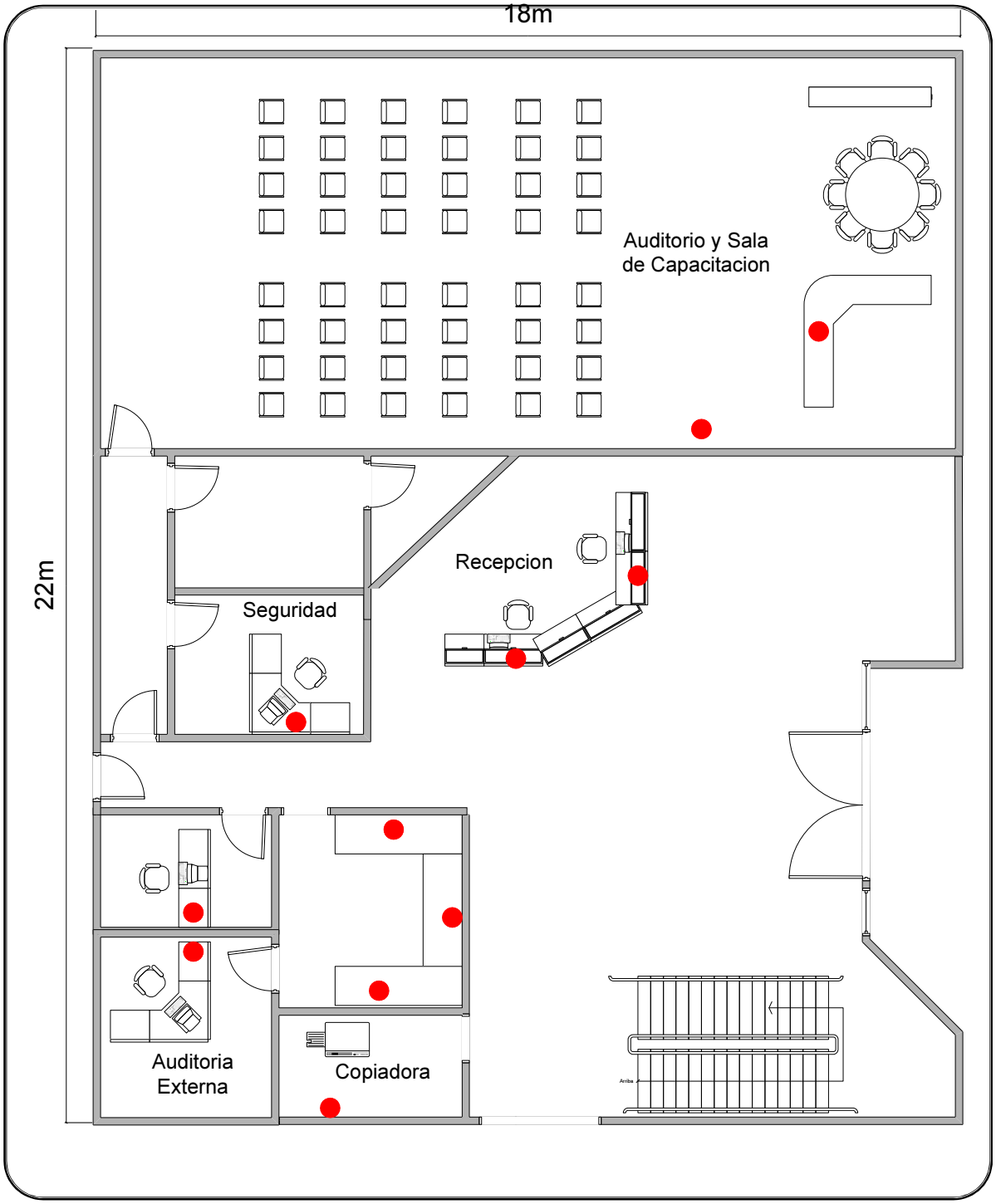


Ilustración 1:4 LAN Edificio Farmaenlace Planta Baja

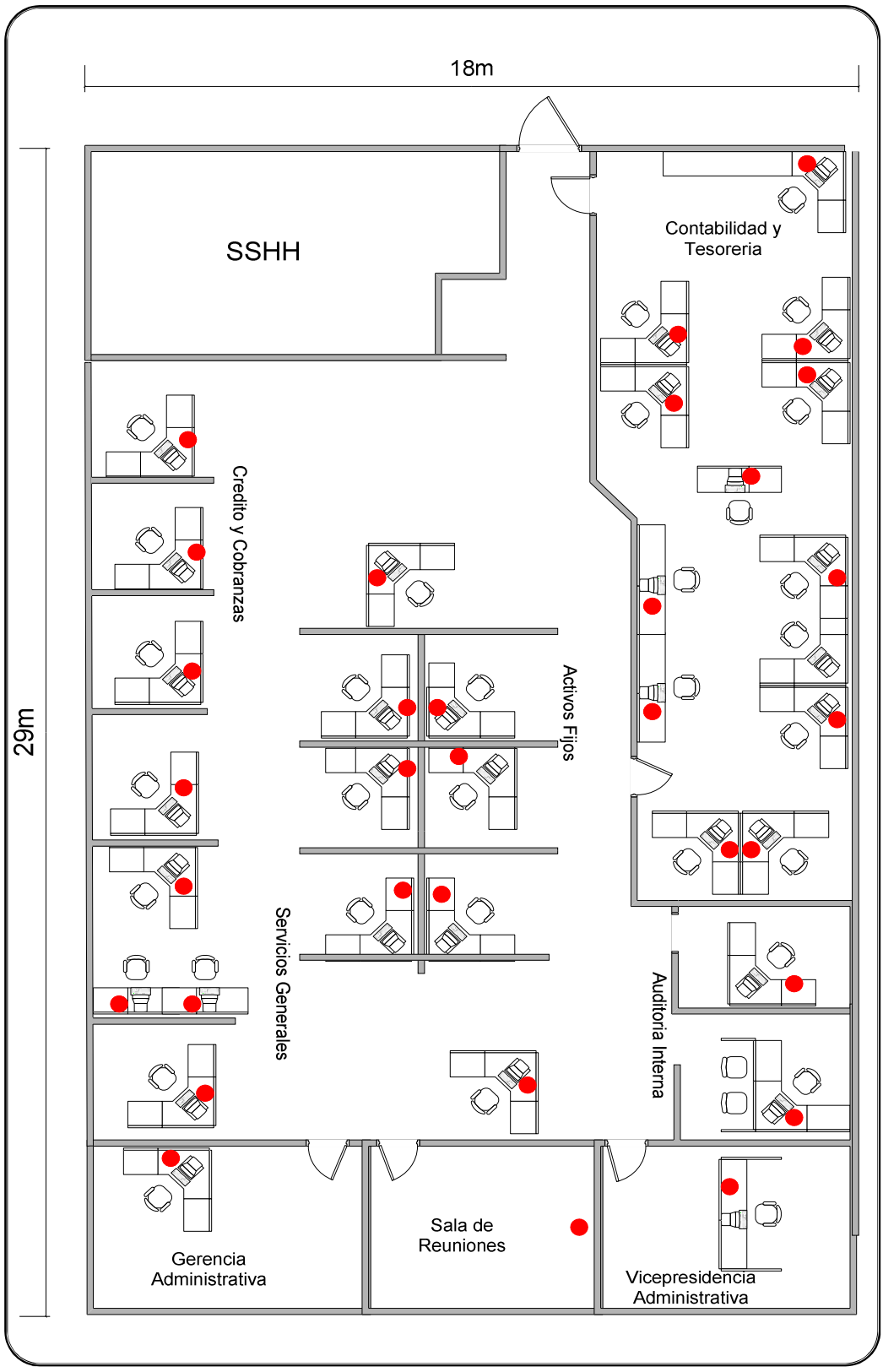


Ilustración 1:5 LAN Edificio Farmaenlace Planta Baja 2

3) Sistemas y Comedor

Detrás del edificio de Farmaenlace, se encuentra una zona destinada para el Departamento de Sistemas, donde se encuentran la gerencia de sistemas, soporte a usuarios y desarrollo de sistemas, junto a estas oficinas se encuentra el comedor del personal.

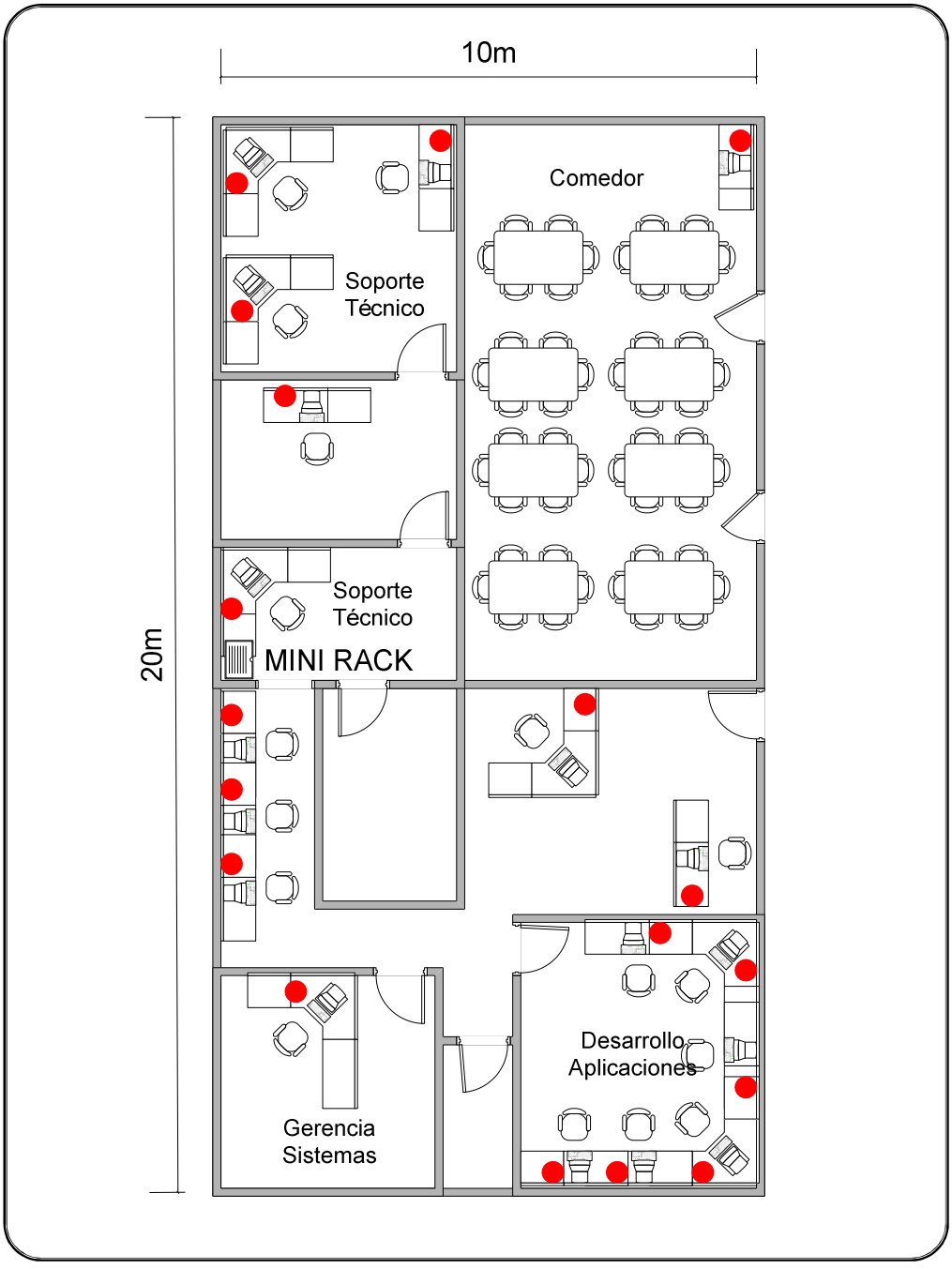


Ilustración 1:6 LAN Edificio Farmaenlace Sistemas y Zona Comedor

4) Bodega

La bodega de Farmaenlace tiene varias áreas, la principal donde se encuentran las oficinas de administración, la zona de certificación de despachos, al costado derecho se ubica la zona de devoluciones, picking de productos y bodega de proveeduría.

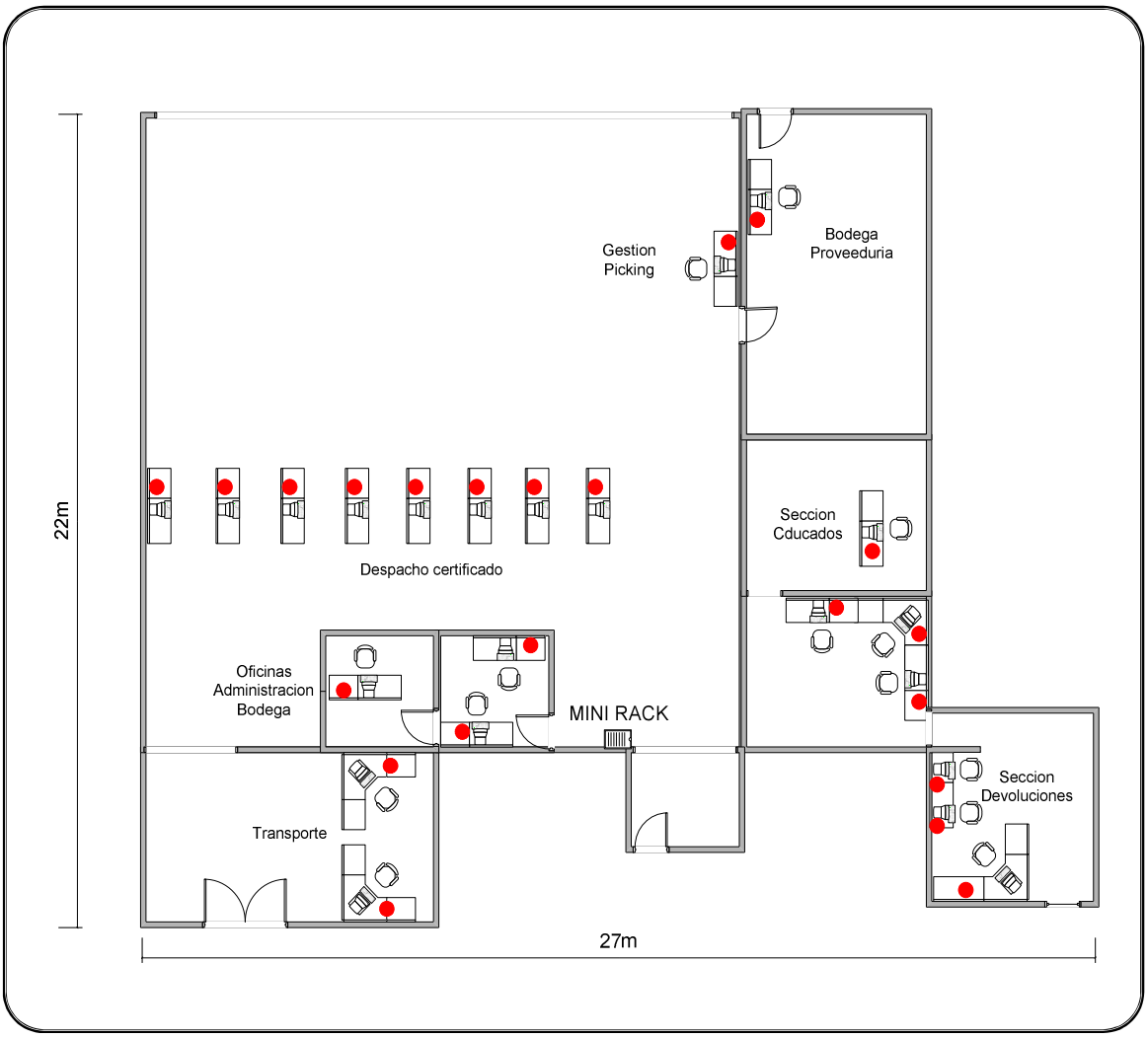


Ilustración 1:7 LAN Bodega Farmaenlace

Detrás de bodega se ubica recepción de mercadería de proveedores.

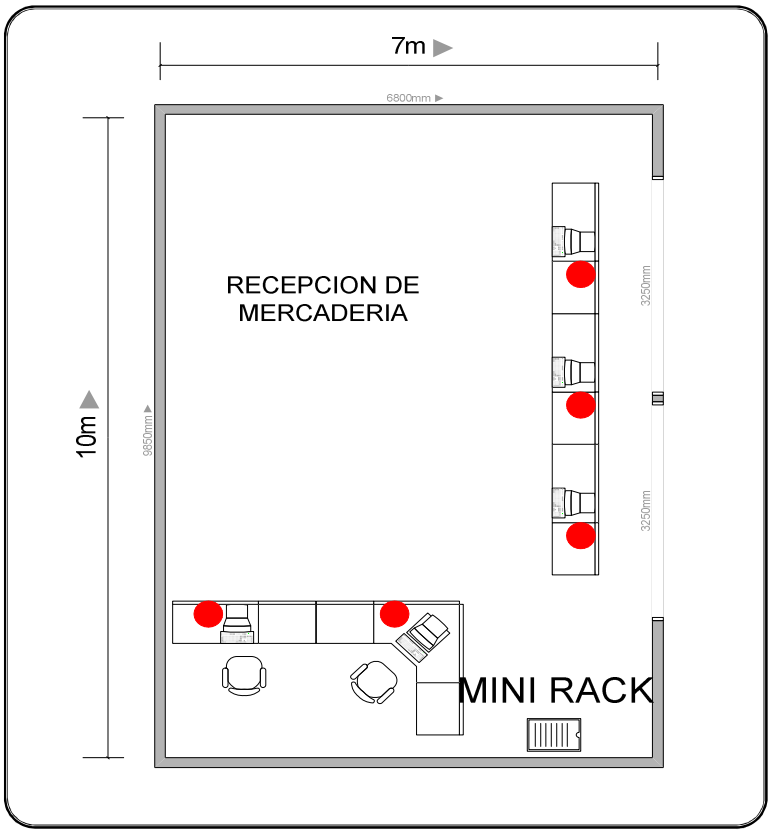


Ilustración 1:8 LAN Bodega Farmaenlace 2

5. Sala de capacitación

Detrás del edificio principal, se ubica la sala de capacitación a empleados con un espacio aproximado de 13m X 5m.

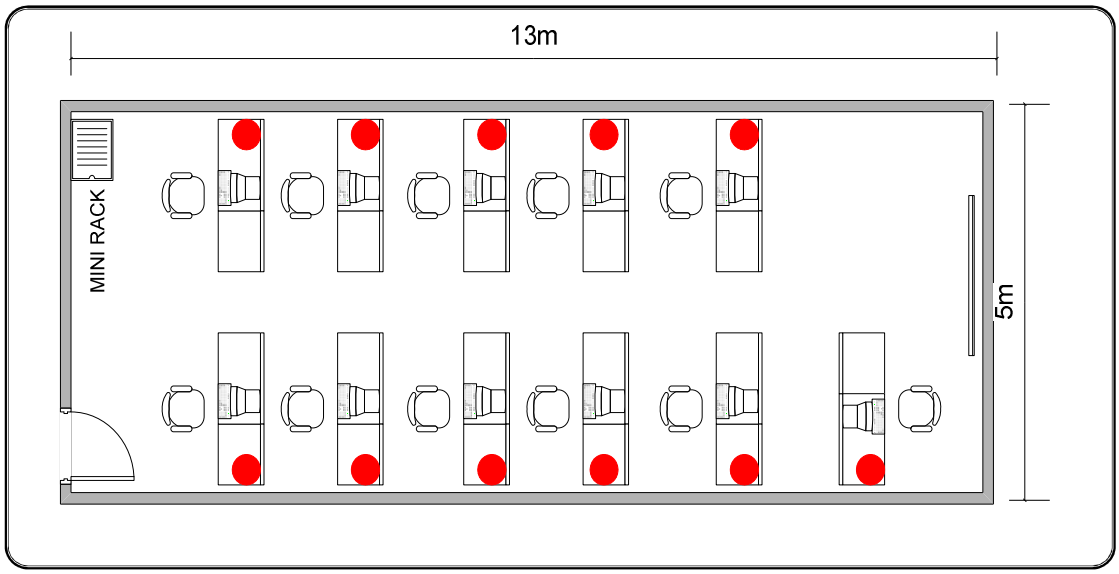


Ilustración 1:9 LAN Sala de Capacitación

1.3 Distribución de red WAN

En este enunciado, se muestran los diagramas de enlaces dedicados de datos, que interconectan las oficinas de matriz con los puntos de venta y oficinas remotas, los enlaces de datos son contratados con proveedores especializados en brindar estos servicios a nivel nacional.

1.3.1 Diagrama de distribución red WAN Farmaenlace

Farmaenlace cuenta con dos enlaces para internet, principal y secundario, con dos proveedores distintos, y enlaces dedicados de datos con todas las agencias y puntos de venta:

1. Un enlace de Fibra 2Mbps con oficinas Farmaenlace Ibarra
2. Enlaces ADSL 512Kbps con Distribuidora Difarmes y dos farmacias que ofrecen servicio de entrega a domicilio y necesitan facturación remota entre estos dos puntos.
3. 98 Enlaces ADSL 128 Kbps para farmacias ubicadas en todo el país.

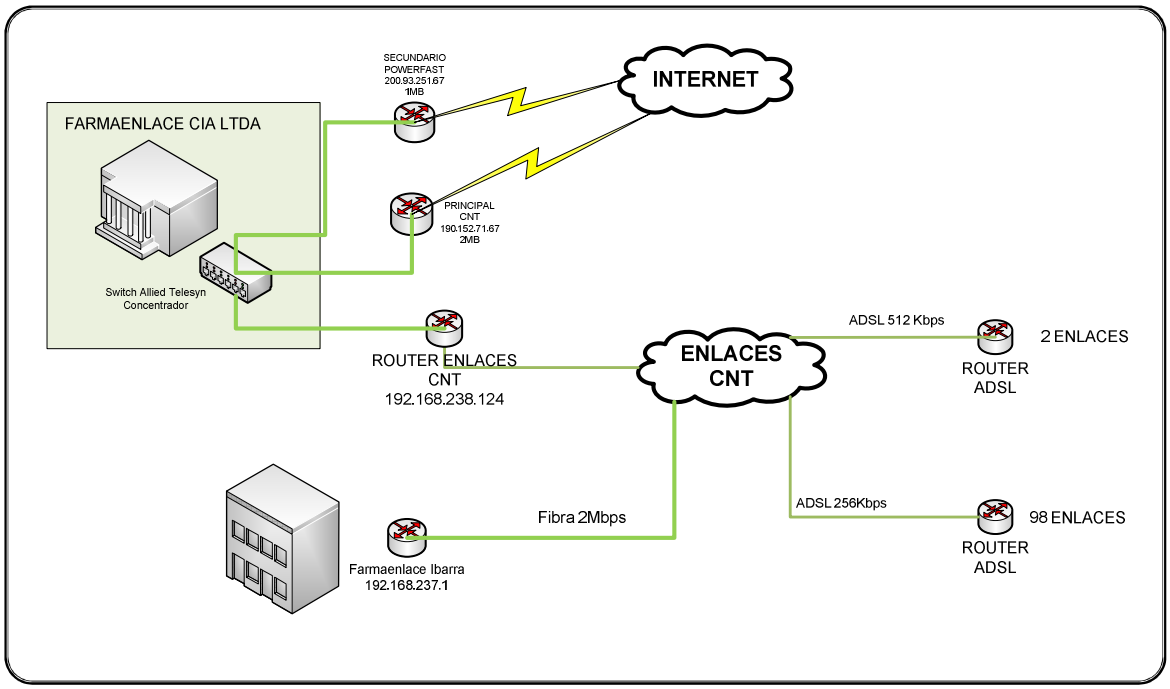


Ilustración 1:10 Distribución WAN enlaces de Farmaenlace

Partiendo de los antecedentes detallados en este capítulo y la evaluación realizada por el área administrativa junto al Departamento de Sistemas, se decide realizar los siguientes cambios:

a) Adecuación del DataCenter en infraestructura, servicios y telecomunicaciones, en un lugar con las dimensiones y facilidades necesarias para soportar los equipos destinados al DataCenter

b) Instalar una solución de telefonía IP e implementarla en Farmaenlace Cía. Ltda. para oficinas y sucursales.

c) Definición de procedimientos y políticas para el correcto uso de los recursos y culturalización del personal de Farmaenlace Cía. Ltda.

En este momento, se sugiere consultar con expertos y con las normas estándar, para tener un lineamiento guía de implementación de un DataCenter y seguir las recomendaciones posibles dependiendo del presupuesto que asigne el área administrativo-financiera, para implementar la mayor cantidad de características que permitan tener un DataCenter acorde a las necesidades de Farmaenlace y soporte la demanda de trabajo, además de tener miras de crecimiento.

1.4 Levantamiento de Necesidades Técnicas

Los Requerimientos técnicos están divididos en varios puntos detallados a continuación, tomando en cuenta que no se iniciará a partir de cero en esta implementación, sino que se utilizarán materiales y equipos ya previamente instalados y agregar nuevos, es necesario conocer ciertos lineamientos de cada uno de los aspectos a continuación.

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, climatización, seguridad de acceso, sistema de detección de incendios; todos estos elementos juegan un papel importante en el rendimiento final.

En la implementación del DataCenter, la característica principal es tratar de eliminar en lo posible los puntos de falla y aumentar la redundancia y confiabilidad de los servicios y la disponibilidad de la información que maneja la empresa.

Como guía de las características de un DataCenter, se recomienda seguir la norma TIA[8]-942 publicada en Abril del 2005, 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.

1.4.1.1 Aspecto Arquitectónico

Es necesario que exista un espacio adecuado para albergar a los dispositivos con comodidad y con miras de crecimiento, en cuanto a tecnología se refiere, el área requerida para el DataCenter no es demasiado amplia, según la recomendación de la norma (TIA-942, 2005, págs. 24-25), que dice: "diseñadores de DataCenter pueden consolidar la conexión cruzada principal, y conexión cruzada horizontal en un sola área de distribución principal, posiblemente tan pequeño como un solo gabinete o rack. La sala de telecomunicaciones para el cableado de las áreas de soporte y la sala de entrada también puede ser consolidado en el área de distribución principal en una topología de DataCenter reducido." Se va a diseñar una topología de DataCenter Reducido, como muestra el grafico a continuación:

[8] TIA: **Telecommunications Industry Association** (Asociación de la Industria de Telecomunicaciones)

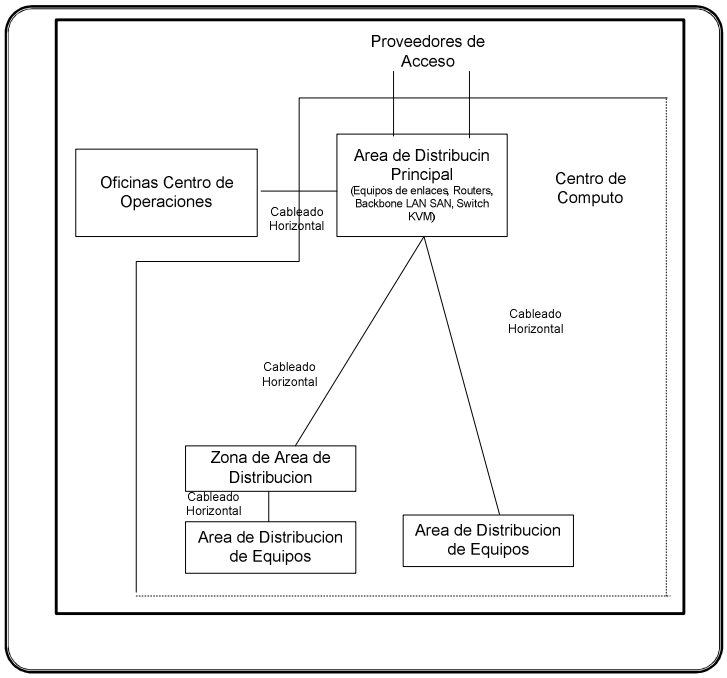


Ilustración 1:11 Diagrama de estructura de un DataCenter Reducido

Se decide ubicar el DataCenter en las oficinas de sistemas de Farmaenlace en el segundo piso del edificio principal, como se mostró anteriormente, el espacio actual de DataCenter no es suficiente para colocar todos los dispositivos que ingresarán; la primera necesidad es modificar el espacio físico del DataCenter de Farmaenlace.

Utilizando como guía el diagrama de las oficinas presentado anteriormente, es necesario aprovechar el espacio de una parte de la oficina para ampliar el espacio del nuevo DataCenter, como muestra el diagrama a continuación:

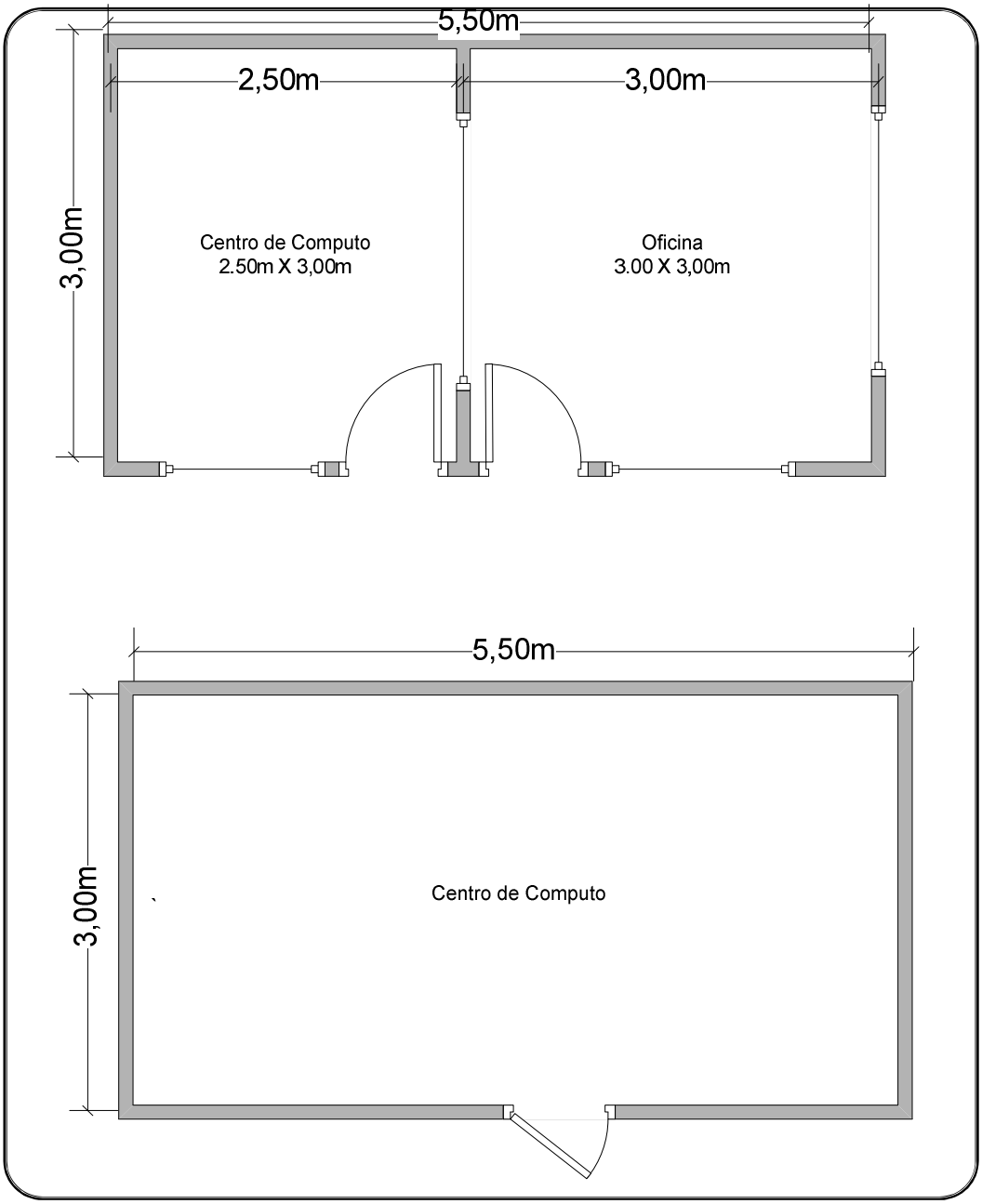


Ilustración 1:12 Diagrama de Espacio de DataCenter

Para solventar este requerimiento, es necesario derribar la pared intermedia de separación, para formar un solo habitáculo que será el DataCenter. Además de hermetizar el área, colocando paneles de fibra de vidrio en lugar de ventanas, ya que estos paneles poseen la propiedad de conservar de mejor manera la temperatura adecuada dentro del lugar.

La norma (TIA-942, 2005) sugiere para Tier Nivel 2, la implementación de un piso falso o piso elevado de al menos 18 pulgadas de elevación, para mejorar la organización del cableado estructurado eléctrico y de datos, y favorecer la circulación de aire dentro del

DataCenter, lamentablemente, debido a la falta de espacio en altitud, no se puede realizar una instalación de piso técnico para el DataCenter, el limitante es la parte superior, aproximadamente a 10 centímetros del techo falso se encuentran las vigas metálicas del edificio.

1.4.1.2 Aspecto Ventilación

Con respecto al Flujo de Aire para ventilación y enfriamiento del DataCenter, se debe seguir la recomendación de la Norma (TIA-942, 2005, pág. 38) que dice: "Los Racks y gabinetes estarán dispuestos en un patrón alternativo, con frentes de racks / bastidores entre sí en una fila para crear pasillos "calientes" y "fríos". Los Pasillos "fríos" están al frente de los racks y gabinetes. Si hay un piso de acceso, distribución de energía, los cables deben ser instalados bajo la planta de acceso a la losa. Los pasillos "Calientes" están detrás de racks y gabinetes. Si hay una planta de acceso, las bandejas de cables para cableado de telecomunicaciones debe estar ubicado en la planta de acceso en los pasillos "calientes". " (TIA-942, 2005, pág. 131) dice: "Las filas del rack y gabinete van paralelas a la dirección de flujo de aire creado por las unidades de Aire Acondicionado de la sala de computo (CRAC). Cada CRAC se encuentra frente a los "pasillos calientes" para permitir que el retorno de aire sea más eficiente para cada unidad CRAC. Los Gabinetes de Servidores están organizados para formar pasillos "Calientes" y "Fríos""; la implementación de un pasillo caliente y un pasillo frío es necesario, porque los racks soportan mayor densidad de equipos, y un mayor consumo de energía de los dispositivos y por ende mayor generación de calor, esto provoca la necesidad de proporcionar un sistema de enfriamiento con flujo de aire preciso y eficiente, que ayudará a reducir el consumo energético del DataCenter, al mantener el ambiente en una temperatura óptima.

Se debe colocar los equipos de manera que el dispositivo de Aire acondicionado de descarga frontal superior sea colocado en la parte alta posterior a los racks, así la emisión de aire frío es emitida por sobre los racks hacia la parte frontal, donde se concentra la salida de aire refrigerado (Pasillo Frío), para que los equipos la tomen desde la parte frontal y despidan aire caliente hacia la parte posterior donde se encuentran las salidas traseras de los equipos (Pasillo Caliente) y el aire caliente sea absorbido por las tomas inferiores del aire acondicionado, como muestra la imagen a continuación:

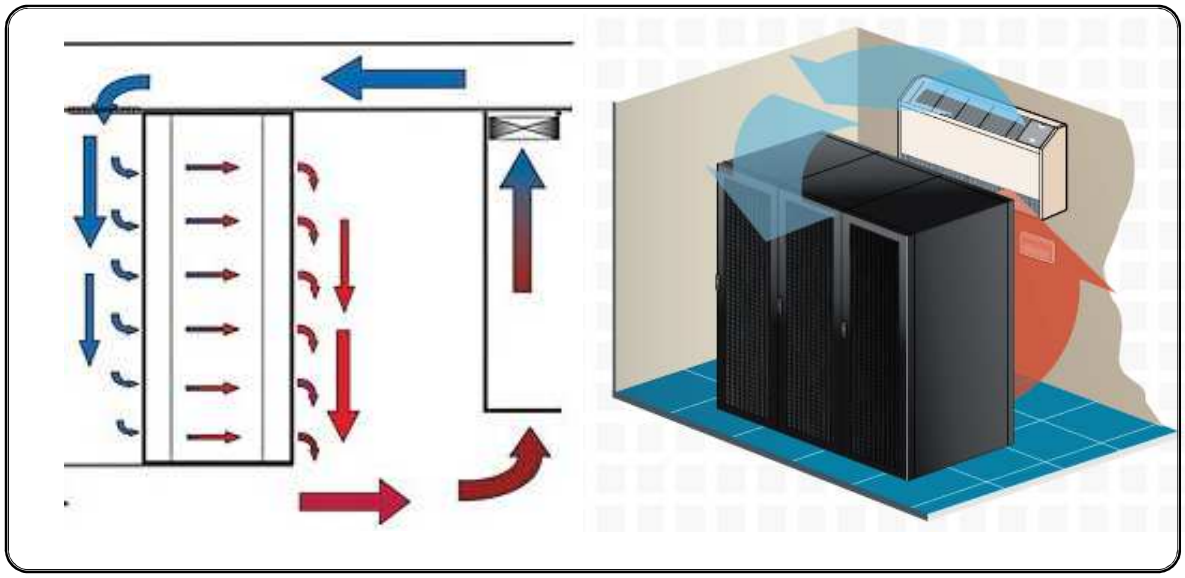


Ilustración 1:13 Pasillo frío y Pasillo Caliente

Se recomienda para TIER (nivel) 1, mínimo un equipo de ventilación, que garantice la mantención de la temperatura y un cierto grado de humedad relativo, la norma (TIA-942, 2005) (Anexo G Mechanical Tiering Tier 1) indica que el TIER 1 permite que no se tenga redundancia en los equipos de acondicionamiento de aire HVAC[9].

1.4.1.3 Aspecto Eléctrico

Dentro del aspecto eléctrico, es necesario destacar que el DataCenter de Farmaenlace tiene una acometida realizada a 110 Voltios con dos tipos de tomas, una regulada a la que se deben conectar los dispositivos que tienen el respaldo del UPS y una acometida no regulada a la que se pueden conectar equipos que no necesiten respaldo de energía, para el nuevo DataCenter se presenta el requerimiento de realizar una acometida a 220 Voltios, para varios dispositivos que trabajan a este voltaje.

El respaldo de energía es por medio de UPS[10], la empresa mantiene sistemas de respaldo de energía para todo el edificio, la carga actual de UPS de 30 KVA[11] que posee Farmaenlace está sobre el 85% y según las normas de consumo eléctrico para un desempeño óptimo de un UPS debería estar a un máximo del 70 %, por lo que es

[9] HVAC: *Heating, Ventilating and Air Conditioning* (Calefacción, Ventilación y Aire acondicionado) conjunto de métodos y técnicas que estudian y analizan el tratamiento del aire en cuanto a su enfriamiento, calentamiento, (des)humidificación, calidad, movimiento, etc.
[10] UPS: (*Uninterruptible Power Supply*) **sistema de alimentación ininterrumpida**, **SAI**, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica a demás de regular la calidad de la misma.
[11] KVA: (kilo voltampere) designa la potencia aparente de un aparato eléctrico de caracteristicas principalmente inductivas cuando funciona con corriente alterna.

necesario incluir otro sistema de respaldo eléctrico UPS de igual característica y mejorar la tecnología del generador eléctrico de backup, porque el equipo generador actual no soporta más carga y es de cambio de fase manual.

La norma (TIA-942, 2005, pág. 35) dice: "Si el área de distribución principal se encuentra en una habitación cerrada, considere dedicados HVAC, PDU, UPS y paneles de energía alimentados para esta área." Sugiere se implemente un UPS dedicado, que soporte la carga operativa únicamente del DataCenter, pero por decisión Administrativa los dos UPS serán colocados en el edificio principal de Farmaenlace, con la finalidad de brindar el respaldo eléctrico de todo el edificio incluido el DataCenter.

Para esto se colocará dos UPS para que soporten la carga del DataCenter, de oficinas y de Bodega; tanto en carga 110V como a 220V, manejando un balanceo de carga conjunto y se reemplazará el generador eléctrico actual de Farmaenlace, por un generador de mayor potencia con un sistema de encendido y cambio de fase automático si se presenta una falla eléctrica, en caso de darse fallas de alimentación eléctrica, los UPS soportan el consumo de carga eléctrica del DataCenter y las oficinas, mientras se active el generador que reemplaza la alimentación eléctrica convencional, hasta el momento que se restablezca, cuando sucede esto, el generador deja de funcionar y cambia nuevamente de fase a alimentación normal.

NOTA: La parte del aspecto arquitectónico, de ventilación y eléctrico, dependen del departamento de infraestructura de la empresa, por lo que en el presente proyecto únicamente se hará mención de los trabajos realizados, tomando en cuenta y recalcando las recomendaciones de las normas para implementación de DataCenter.

1.4.1.4 Referente a Seguridad física.

El DataCenter de Farmaenlace necesita en su infraestructura arquitectónica niveles de seguridad física, dentro de los cuales se describen varios aspectos recomendados que son:

1. **Seguridad de acceso**

El DataCenter es un área altamente crítica, por lo que el acceso del personal debe ser limitado únicamente a quienes posean la autorización debida. Actualmente y debido a que el DataCenter de Farmaenlace se encuentra junto a oficinas donde labora el personal de Servicios y Redes, se mantiene un sistema de control de acceso por medio de tarjetas magnéticas, entregadas únicamente al personal del área y al Gerente de Sistemas, lo que

limita el acceso al área de oficinas y por ende al DataCenter, cuya puerta de acceso se encuentra dentro de las oficinas de sistemas del segundo piso como muestra el diagrama.

También se sugiere la instalación de una puerta de seguridad de acceso al DataCenter que debe tener las siguientes características:

a. Plancha de acero de 2mm de espesor
b. Refuerzos de tubo estructural en el interior
c. Resistencia al calor
d. Brazo de cierre de puerta
e. Barra anti pánico.
f. Mirilla de vidrio de seguridad
g. Cierre hermético

Con el aprovechamiento del control de acceso y la instalación de la puerta de seguridad se mantendrá un mejor nivel de seguridad para el acceso físico, se garantiza un cierre hermético del DataCenter conservando la temperatura interna del mismo.

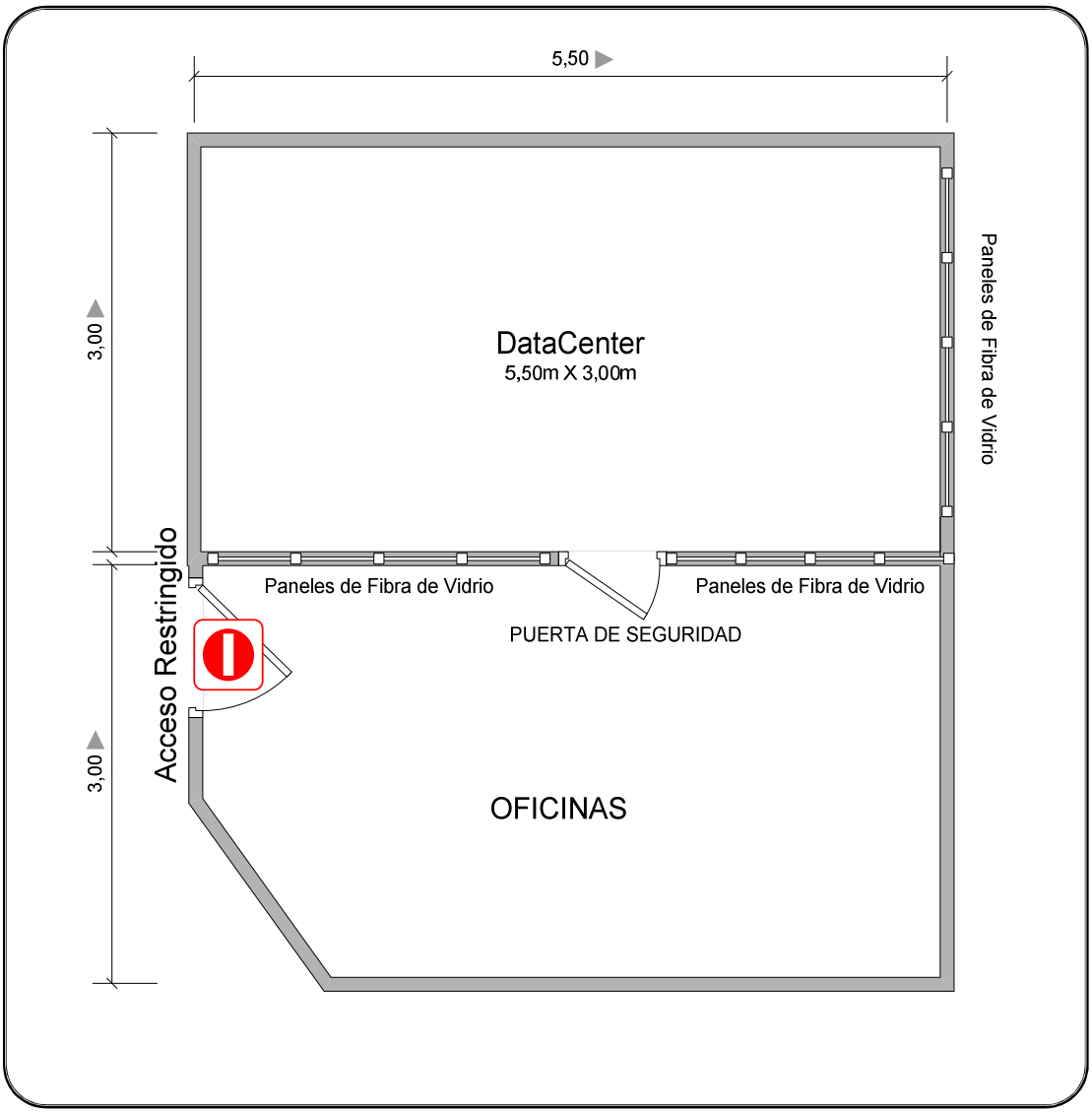


Ilustración 1:14 Diagrama de espacio DataCenter y oficinas de sistemas

2. Seguridad contra incendios

Debido a la criticidad del espacio destinado al DataCenter, a la alta concentración de equipamiento electrónico y por ende a la posibilidad de producirse un atentado al mismo, es necesario colocar un sistema de detección de incendios, que alerte al personal de un evento de esta naturaleza para que se tomen las medidas del caso, la sugerencia más básica es colocar sensores de detección de humo y colocar dispositivos extintores manuales de gas CO_2[12] que sofoquen un conato de incendio de manera manual.

La solución recomendada, por rapidez de mitigación de un conato de incendio y seguridad tanto de los equipos como del personal, es colocar un sistema de detección y además de extinción de incendios, que conste de detectores foto electrónicos y un sistema

[12] CO_2: **dióxido de carbono**

de tuberías de distribución de gas agente de extinción de incendios limpio; que se emite y llena toda la superficie y tiene la propiedad de ingresar al interior de los dispositivos electrónicos para extinguir el fuego que pueda ubicarse dentro de los equipos, no deja residuos luego de su expulsión y no es tóxico según (NFPA, 2001). Este sistema de extinción de incendios garantiza una rápida recuperación ante desastres y limita la afectación de equipos que se encuentren junto al origen del incendio por su rápida acción.

3. **Seguridad contra desastres**

Además de un posible conato de incendio, pueden presentarse diferentes eventos considerados como desastres naturales, por ejemplo inundaciones o terremotos, para el caso de inundaciones se recomienda revisar las instalaciones cercanas al DataCenter y proceder a impermeabilizar la zona, para evitar el filtrado de agua al interior del DataCenter desde el techo y evaluar si se encuentran cerca al DataCenter tuberías de agua que pudieran afectar en caso de una ruptura o corrosión de las mismas.

Para el caso de terremotos, depende estrictamente de la estructura del edificio en general, que se encuentra construido con estructuras metálicas altamente resistentes y paredes de bloque y ladrillo que brindan estabilidad al edificio.

De estos temas se encarga el Departamento de Infraestructura de Farmaenlace Cía. Ltda., para la revisión y aseguramiento del perímetro del DataCenter en caso de posibles desastres de este tipo.

1.4.2 Referente a Cableado Estructurado y Comunicaciones

1. **Adecuación de Áreas Nuevas**

El cableado de Farmaenlace Cía. Ltda. fue realizado en el año 2005 bajo categoría 5E, por presupuestos y decisión administrativa no se considera cambios en el cableado actual del edificio, exceptuando la adecuación de las nuevas oficinas, que serán las áreas de capacitación, auditorio de Farmaenlace y edificio posterior, donde se instalará un cableado estructurado de forma segmentada y se colocaran concentradores por cada área y desde estos se conectará hacia el DataCenter; se calcula alrededor de 60 puntos de red nuevos que se deberán implementar.

Siguiendo las normativas, se recomienda la instalación de cableado estructurado mínimo de categoría 6, en las áreas que requieran instalaciones de red nuevas, se debe tener miras

de crecimiento en cuanto al cableado estructurado y conforme avance el tiempo se plantearán nuevos proyectos de mejoramiento de cableado estructurado del edificio para reemplazar el cableado considerado como obsoleto y resulta una mejor inversión si ciertas alas del edificio tienen instalado un cableado estructurado que no necesite ser reemplazado a corto plazo.

Adicional, se requiere inhabilitar los puntos de voz de las oficinas de Farmaenlace, ya que con la implementación de la telefonía Ip, tanto voz como datos se transmiten por el mismo punto de red y por consiguiente los puntos de voz no serán utilizados.

2. 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, que según (TIA-942, 2005, págs. 24-25) que dice: "Los espacios de los DataCenter de telecomunicaciones incluyen la sala de entrada, área de distribución principal (MDA), el área de distribución horizontal (HDA), área de la zona de distribución (ZDA) y el área de distribución de equipos (EDA)… El área de distribución principal incluye la conexión cruzada principal (MC), que es el punto central de distribución para el sistema de cableado estructurado del DataCenter y puede incluir conexión cruzada horizontal (HC) cuando las áreas de equipos se sirven directamente de la zona de distribución principal." Recomienda mantener una zona para cableado estructurado, donde se encuentren los puntos de red en patch panel de todo el edificio y los switches que interconecten la red (Cableado Horizontal). Un Área de Distribución Principal MDA (Main Distribution Area) donde se encontrarán los equipos de telecomunicaciones, como enlaces de datos hacia puntos de venta o proveedores de servicios de la empresa, switches y routers principales.

Por consideraciones de espacio y presupuesto en el desarrollo del proyecto se mostrará la adecuación definitiva y organización de los racks.

El DataCenter Ebook (Siemon, 2008) indica que de acuerdo a las consideraciones de cableado de DataCenter, no se recomienda un cableado punto a punto desde los concentradores o switches hacia los equipos servidores, sino que se recomienda el concepto de cableado estructurado, es decir que se coloque en cableado ordenado entre los racks de comunicaciones y racks de servidores mejorando la modularidad, administración, funcionalidad y escalabilidad, manejando patch panels en cada rack y desde cada patch panel alimentar los puertos de red de cada servidor.

La Categoría de cableado reconocida por la norma (TIA-942, 2005, pág. 60) dice: "El uso de cable de par trenzado 100-Ohm (4 pares categoría 6 se recomienda)… El uso de la actual fibra multimodo de 62.5/125 micras (160/500 MHz • km)… El uso de la actual fibra multimodo de 50/125 micras (500/500 MHz • km)…" para el cableado interno o cableado horizontal del DataCenter y cableado de backbone es mínimo UTP Cat 6 basado en las normas ANSI/TIA/EIA-568-B, para fibra óptica debe ser de tipo multimodo de 62.5/125 micrones o 50/125 micrones y también la fibra monomodo.

Adicional, se debe establecer una comunicación por fibra óptica desde el DataCenter de Farmaenlace hacia la zona de bodega, para mantener una comunicación constante y minimizar el riesgo de pérdida de comunicación, debido a la distancia entre el Datacenter y esta zona que supera los 300 metros.

3. 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.

Se plantea también el requerimiento de eliminar la infraestructura de comunicación telefónica actual de Farmaenlace y remplazarla con la telefonía IP, lo que a mediano y largo plazo repercutirá en un ahorro en costos de consumo telefónico.

Con respecto a la red interna se considera la mejor opción mantener la red de tipo C (192.168.238.0 /24) que maneja Farmaenlace, asignarla para dispositivos servidores y equipos enlaces de datos y agregar una red de tipo B (172.30.0.0) donde se incluirá a los equipos de todos los usuarios (Host) de Farmaenlace.

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, sea cobre o fibra, racks, tomas eléctricas, patch panels, patch cords[13], tomas, canaletas, etc., considerados en el punto anterior como cableado estructurado.

Adicional están los equipos computacionales que se destinarán al DataCenter sean estos CPU, servidores, dispositivos de almacenamiento (Storage), elementos de central telefónica.

El requerimiento que se recoge concerniente a este aspecto es ya contando con el inventario de dispositivos recopilado previamente, considerar cuáles equipos se conservan, cuáles se reutilizan para agregar nuevos servicios, cuáles se desechan y que equipos nuevos se deben adquirir para el correcto desempeño del nuevo DataCenter.

De la evaluación realizada se detalla los siguientes requerimientos.

a) Conservar los servidores de los sistemas LISA
b) Conservar los servidores del sistema EasyFarma
c) Conservar el servidor de TINI de Farmaenlace
d) Conservar los servidores de correo electrónico y navegación de Farmaenlace
e) Implementar un storage[14] para almacenamiento de base de datos.
f) Desactivar la central telefónica de Farmaenlace incluyendo los teléfonos convencionales.
g) Implementar un servicio de central telefónica IP para que provea el servicio a Farmaenlace incluyendo teléfonos IP para distribuirlos en oficinas y puntos de venta.
h) Adquirir nuevos equipos activos de red para soportar el paso de datos y voz Ip y reemplazar los equipos actuales.
i) Reutilizar los equipos activos de red en los sectores que se requiera.
j) Reemplazar los rack de torre por racks tipo armario en el nuevo DataCenter.
k) Adquirir nuevos servidores para manejo de dominio y servicios adicionales.

[13] **Patch Cord:** cable (UTP) se usa en la red para conectar un dispositivo electrónico con otro.
[14] Storage: repositorio de discos independiente de servidores que contienen gran tamaño y alta disponibilidad, se accede desde los servidores por medio de una red SAN (Storage Area Network)

1.4.4 Referente a servicios, actualización o implementación

Revisando los servicios que se encuentran funcionando, es necesario evaluar los sistemas que se encuentran trabajando, se detalla a continuación:

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 Farmaenlace.

c) Servicios adicionales para áreas especificas de la empresa incluidos los de desarrollo interno Farmaenlace

d) Cubos (Información financiera)

e) PL (Logística y Certificación de despacho)

f) TINI Central

g) Aplicaciones Web de manejo de requerimientos y procesos internos de la empresa.

h) Servicios de Administración de transacciones para servicios de proveedores externos, como ventas con tarjetas de crédito, recargas celulares y facturación electrónica

i) Es necesario incorporar un nuevo servicio de control de dominio y directorio activo bajo el nombre ***farmaenlace.com*** y asociar a todos los equipos computacionales a este nuevo dominio para mejor control de usuarios y políticas de seguridad.

j) Se debe implementar un servicio de actualizaciones automáticas de aplicaciones Windows al que tengan acceso todos los equipos computacionales de la empresa que se encuentren atados al dominio ***Farmaenlace.com***

k) 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.

l) 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 redes y telecomunicaciones así como también de los usuarios, se planea mejorar con estas recomendaciones la manera de administrar personal y del comportamiento de los usuarios con respecto a su trabajo, a la utilización de servicios y aprovechamiento de recursos, estos requerimientos se detallan a continuación.

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 tres personas. Al principio, cada uno seguirá con el trabajo que ha venido desempeñando en la empresa y paulatinamente sus conocimientos deberán ser compartidos entre sí hasta alcanzar un nivel homogéneo de tal manera que las funciones puedan ser compartidas y suplidas en caso de que uno de ellos no se encontrare en el momento de ser requerido.

Se deberá realizar la implementación de los servicios anteriormente detallados garantizando continuidad en el servicio para los usuarios finales y tratando de no suspenderlos durante la migración a menos que sea estrictamente necesario; para lo cual se deberá trabajar durante horarios fuera de oficina para tareas críticas que incluyan suspensión temporal de los sistemas o servicios y en horario normal para tareas que no sean invasivas en el desempeño laboral diario de la empresa.

1.5.2 Referente a procedimientos

Los procedimientos que se elaborarán son guías documentales de los pasos a seguir para la realización de tareas específicas de la administración de sistemas redes y telecomunicaciones. Varios de estos procedimientos deben establecerse claramente y servirán como parte de la información y conocimiento que debe ser compartido por ambas empresas para conformar un solo y nuevo grupo de documentación que facilite las funciones y sea ampliamente comprensible.

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 debidamente documentados y publicados para conocimiento del personal que los vaya a utilizar dentro de los cuales están los siguientes:

a) Configuración de equipos Cliente
b) Creación de Usuarios y asignación de permisos de acceso
c) Creación de Cuentas de Correo y Listas de Distribución
d) Asignación de permisos para servicios web
e) Creación y modificación de directivas de seguridad
f) Respaldo de información y backups de bases de datos
g) Mantenimiento de sistemas y bases de datos
h) Solicitud de nuevos enlaces de datos
i) Reporte a proveedores de fallas en enlaces de datos

Adicional se deberán establecer planes de contingencia que también deberán estar debidamente documentados y disponibles para el personal en caso de ser requeridos estos planes son:

a) Caídas de Servicios
b) Enlaces de Datos caída y configuración para acceso por enlace backup
c) Correo Electrónico
d) Navegación Web
e) Fallas de Servidores
f) Fallas en 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.

Se requiere establecer políticas 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.

CAPÍTULO 2

2 FUNDAMENTO TEÓRICO DEL PROYECTO

Para el desarrollo del proyecto, conociendo los antecedentes y requerimientos de todo el trabajo que se deberá realizar, es necesario conocer los fundamentos teóricos que nos ayudarán en la realización del mismo, para esto necesitamos conocer fundamentos de redes y administración de sistemas, puntos que los describimos a continuación.

2.1 Redes LAN y WAN

Según (Tanenbaum, 2003) una red de computadores o red informática se refiere al conjunto de equipos computacionales interconectados entre sí por diversos medios físicos

o dispositivos, que se encargan de la transmisión de datos con la finalidad de recoger, compartir, procesar información y recursos garantizando fiabilidad en los datos y disponibilidad la información, sin importar la locación física del recurso y del usuario, mismo que podría ubicarse de manera local dentro del mismo edificio o de manera remota en otra ciudad u oficina distante y poder acceder a la información que necesite de manera inmediata.

Las redes hoy se están utilizando para diversas aplicaciones, las más tradicionales son el uso empresarial o para aplicaciones de negocios como el desarrollo del presente proyecto, una empresa relativamente grande con diversas sucursales y un stock de equipos computacionales que en todo el país fácilmente supera los quinientos dispositivos, mismos que necesitan estar conectados hacia un servidor principal que está ubicado en la oficina matriz, compartiendo, obteniendo información y aprovechando recursos constantemente, convirtiéndose en el activo intangible más importante de la empresa.

El modelo que se utiliza en esta empresa se conoce como Modelo Cliente Servidor, donde existen varios clientes en oficina o en puntos lejanos, que requieren acceso a la información que primordialmente está contenida en las oficinas principales de la empresa y que es replicada a los diversos puntos de venta y oficinas en todo el país.

El modelo cliente servidor se comporta de la siguiente manera (Oramas Bustillos, 2010):

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.

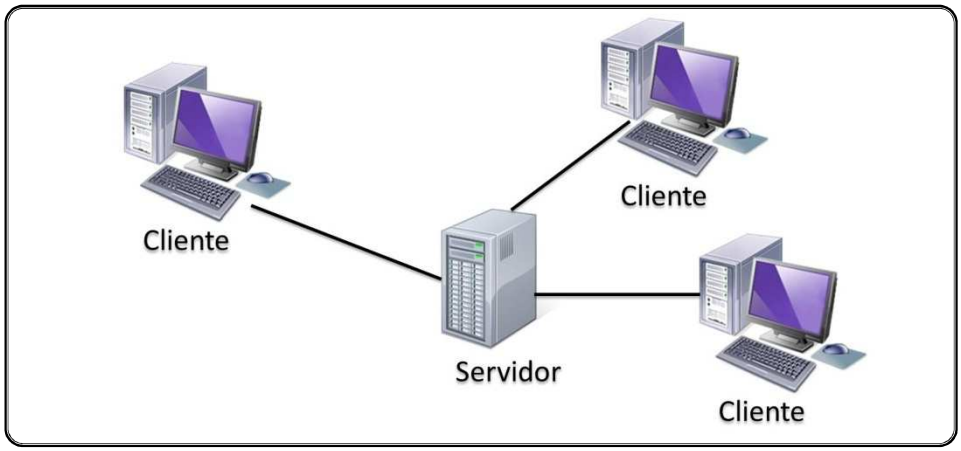


Ilustración 2:1 Figura del Modelo Cliente Servidor

Además de la información también se cuenta con los métodos de comunicación entre los usuarios, tales como el correo electrónico, la telefonía IP, videoconferencias, mensajería instantánea, navegación web, etc. que son servicios que funcionan a través de las redes informáticas; mejorando de manera sustancial la comunicación, optimizando recursos y fomentando el ahorro de los mismos.

Para (Tanenbaum, 2003) las redes de computadores se pueden clasificar de acuerdo a la tecnología de transmisión en:

Enlaces de difusión: Tienen un solo canal de comunicación donde todos los equipos de la red lo comparten, de tal manera que si un equipo envía un paquete todos los equipos lo reciben y verifican si el paquete les corresponde a ellos, de ser así lo procesan, caso contrario lo descartan; en el caso de que se desee enviar un paquete a todos los equipos para que lo reciban y lo procesen se utiliza un código especial llamado broadcasting, también si se desea que un paquete llegue a un subconjunto de dispositivos específicos, esta forma de difusión se la conoce como multicasting.

Enlaces de punto a punto: Constan de varias conexiones entre pares de equipos, de tal manera que para llegar un paquete de su emisor hasta su destinatario, debe pasar por uno o varios dispositivos intermedios, encaminándose a través de rutas que pueden variar en medios y velocidad de transmisión.

Se puede mencionar que las redes de difusión se utilizan en las redes pequeñas en una misma área geográfica y las redes punto a punto se utilizan en redes grandes o de áreas extensas.

Otro tipo de clasificación de las redes es en base a la distancia o alcance, como se describe a continuación:

a) Redes de Área Personal PAN
b) Redes de Área Local LAN
c) Redes de Área de Campus CAN
d) Redes de Área Metropolitana MAN
e) Redes de Área Amplia WAN
f) Redes de Almacenamiento SAN
g) Redes de Área Local Virtual VLAN

Para fines del proyecto se describen los tres tipos de redes que guiarán en lo posterior, estas son las redes de Área Local LAN, las redes de Área Extensa WAN y redes de Área Local Virtual VLAN.

2.1.1 Fundamentos de Redes LAN

Las **redes de área local (LAN)** (Tanenbaum, 2003) son redes de propiedad privada que se encuentran dentro de un solo edificio o en un área de pocos kilómetros de longitud, se utilizan para conectar computadoras personales, estaciones de trabajo y dispositivos de acceso en oficinas de una empresa para compartir recursos e información.

Las LANs se limitan de acuerdo a los siguientes aspectos:

Tamaño: Las LANs están restringidas por tamaño, es decir, no pueden extenderse más allá de donde su medio físico lo permite, en el caso de cable de cobre según la norma EIA/TIA 568 se permite una distancia máxima de 90 metros, en el caso de una red LAN inalámbrica se depende del radio de señal que emiten los dispositivos de conexión (access point), también el tiempo de transmisión de los paquetes es limitado y conocido de antemano.

Tecnología de transmisión: Las LANs podrían utilizar una tecnología de transmisión que consiste en un cable al cual están unidas todas las máquinas, también existe la disponibilidad de acceso a la red LAN para dispositivos inalámbricos, como laptops o dispositivos móviles, conectando a la red alámbrica dispositivos de acceso para formar así una red inalámbrica, conocida como Wireless LAN (WLAN). Existe un estándar para las LANs inalámbricas llamado **IEEE 802.11,** que la mayoría de los sistemas implementa y que se ha extendido ampliamente.

Velocidad de transmisión: Depende en este caso del medio físico, sea este cable o inalámbrico, los dispositivos de conmutación (switches) y las tarjetas de conexión de los equipos, las más comunes son las velocidades de 10, 100 y 1000 Mbps[15], pero con las nuevas tecnologías en medios de transmisión sobre cobre se puede permitir la transmisión de hasta 10 Gbps[16].

[15] Mbps: **megabit por segundo** (**Mb/s** o **Mbit/s**) unidad que se usa para cuantificar un caudal de datos equivalente a 1 000 kb/s.
[16] Gbps: **gigabit por segundo** (**Gb/s** o **Gbit/s**) unidad que se usa para cuantificar un caudal de datos equivalente a 1 000 Mb/s

Topología: El tipo de topología más utilizado en las redes en la actualidad es una red de bus, es decir todos los dispositivos están lógicamente interconectados a una sola línea de transmisión, en cualquier instante al menos una máquina es la maestra y puede transmitir información, todas las demás máquinas se abstienen de enviar, en el momento que se presenta un conflicto de que dos o más máquinas desean transmitir al mismo tiempo (Colisión), se requiere un mecanismo de control de la transmisión para administrar este evento, tal mecanismo podría ser centralizado o distribuido. La norma mas estandarizada es la IEEE 802.3, también conocida como **Ethernet,** es una red de difusión basada en bus con control descentralizado, funciona de 10 Mbps a 10 Gbps, de tal manera que las computadoras que están en una Ethernet pueden transmitir siempre que lo deseen; si dos o más paquetes entran en colisión, cada computadora espera un tiempo aleatorio y lo intenta de nuevo más tarde.

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "intranet". Los servidores Web de red interna son distintos de los servidores de Web públicos, ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas para acceder a la red interna de una organización. Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización; dentro de una red interna, los servidores de Web se instalan en la red, la tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.

Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna y utilizan un acceso extendido y seguro a usuarios o empresas externas, este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios y seguridad a nivel de las aplicaciones; por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

2.1.2 Fundamentos de Redes WAN

Una **red de área amplia** (**WAN**) (Tanenbaum, 2003)**,** abarca una gran área geográfica, con frecuencia una ciudad (también se considera una red de área metropolitana MAN), un país o un continente; los *hosts (Equipos cliente)* están conectados por una subred de comunicación; los clientes son quienes poseen a los *hosts* (es decir las computadoras personales de los usuarios), mientras que los proveedores de servicios de Internet o

enlaces dedicados poseen y operan la subred de comunicación. La función de una subred es llevar mensajes de un *host* a otro a través de una gran distancia, se sugiere mantener por separado los host de la subred de transmisión en el diseño para una mejor comprensión y simplicidad.

En la mayoría de las redes de área amplia la subred consta de dos componentes distintos: líneas de transmisión y elementos de conmutación; las líneas de transmisión, como su nombre lo indica se encargan de movilizar los pulsos eléctricos conocidos como bits entre dispositivos, pueden estar hechas de cable de cobre, fibra óptica o incluso radioenlaces. Los elementos de conmutación son computadoras especializadas que conectan varias líneas de transmisión, de tal manera que cuando los datos llegan a una línea de entrada, el elemento de conmutación debe elegir una línea de salida por la cual reenviarlos para que lleguen a su destino.

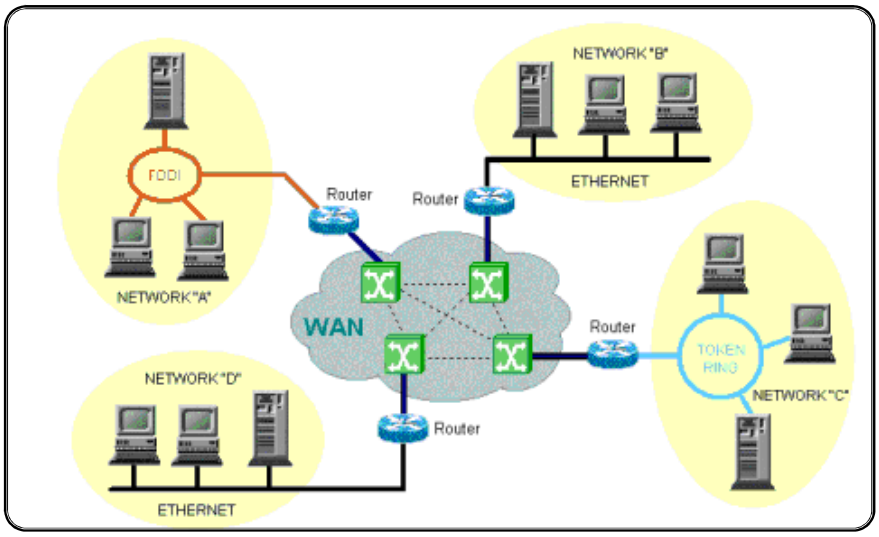


Ilustración 2:2 Ejemplo red WAN

En este modelo, mostrado en la figura anterior cada *host* está conectado a una LAN en la que existe un enrutador. El conjunto de líneas de comunicación y enrutadores (sin incluir las de los *hosts*) forma la subred de comunicación.

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 servicios directamente al

usuario también conocidos como Host y los dispositivos de red que son los que conectan entre sí a los dispositivos de usuario final.

Cada host posee una interfaz de comunicación con la red denominada NIC (Network Interface Card) con lo que se pueden conectar a los dispositivos de red, cada NIC posee una dirección individual que posee un código único denominado Dirección de Control de Acceso al Medio (MAC), misma que es utilizada para control de comunicación para el host de la red.

Los dispositivos de red se encargan de transportar los datos que necesitan ser transferidos entre los Host, dentro de las características de los dispositivos de red se destacan que proveen las conexiones de cable, concentración de conexiones, conversión de formatos de datos y administración de transferencia de datos.

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. La norma (IEEE-803.3, 2002) sugiere la regla 5-4-3 que divide la red en dos tipos de segmentos físicos: segmentos poblados (usuarios) y segmentos no poblados (enlaces); la regla indica que debe haber un máximo de 5 segmentos conectados por 4 repetidores o concentradores y solamente 3 de los cinco segmentos pueden tener usuarios conectados a los mismos.

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. Cuando el puente recibe una trama, busca la dirección MAC destino en la tabla de puenteo para determinar qué proceso debe seguir: si el dispositivo esta en el mismo segmento que la trama, el puente impide el paso hacia otros segmentos (filtrado); si el dispositivo de destino está en un segmento distinto, el puente envía la

trama al segmento correspondiente; si no se conoce la dirección de destino, se envía la trama a todos los segmentos de la red excepto al origen (inundación).

Switches.- Estos dispositivos concentran múltiples conexiones, además agregan mas 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. La comunicación de datos maneja dos operaciones básicas: Conmutación de tramas de datos, mediante el cual una trama se recibe por un medio de entrada y se transmite a un medio de salida; y el mantenimiento de operaciones de conmutación, donde se crean y mantienen las tablas de 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 una ruta 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. Una subred organizada a partir de este principio se conoce como subred de **almacenamiento y reenvío** (*store and forward)* o de **conmutación de paquetes;** casi todas las redes de área amplia (excepto las que utilizan satélites) tienen subredes de almacenamiento y reenvío; cuando los paquetes son pequeños y tienen el mismo tamaño, se les llama **celdas.** En general, cuando un proceso de cualquier *host* tiene un mensaje que se va a enviar a un proceso de algún otro *host*, el *host* emisor divide primero el mensaje en paquetes, los cuales tienen un número de secuencia; estos paquetes se envían entonces por la red de uno en uno en una rápida sucesión, los paquetes se transportan de forma individual a través de la red y se depositan en el *host* receptor, donde se re-ensamblan en el mensaje original y se entregan al proceso

receptor. En la figura se muestra un flujo de paquetes correspondiente a algún mensaje inicial, todos los paquetes siguen la ruta *A-C-E* en vez de la *A-B-D-E* o *A-C-D-E*. En algunas redes todos los paquetes de un mensaje determinado *deben* seguir la misma ruta; en otras, cada paquete se enruta por separado; desde luego, si *A-C-E* es la mejor ruta, todos los paquetes se podrían enviar a través de ella, incluso si cada paquete se enruta de manera individual. Las decisiones de enrutamiento se hacen de manera local, cuando un paquete llega al enrutador *A*, éste debe decidir si el paquete se enviará hacia *B* o hacia *C*. La manera en que el enrutador *A* toma esa decisión se conoce como **algoritmo de enrutamiento**

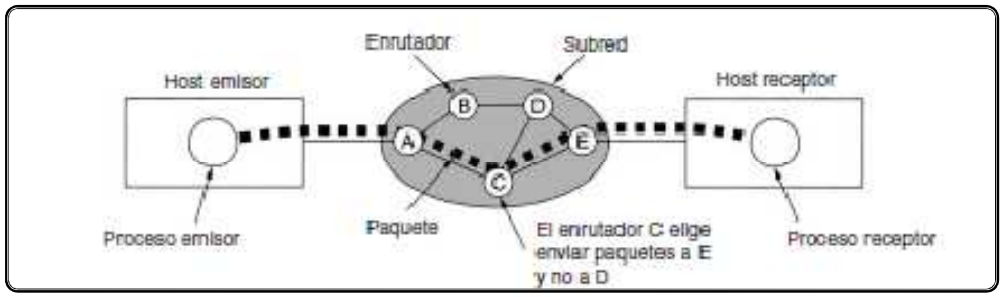


Ilustración 2:3 Enrutamiento de Redes

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: La topología Física y la topología Lógica (Cisco, 2005).

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[17] que debe terminarse en ambos extremos, todos los hosts se conectan directamente a este backbone.
b) **ANILLO.-** La topología de anillo conecta un host con el siguiente y al último host con el primero, esto crea un anillo físico de cable.
c) **ESTRELLA.-**La topología en estrella conecta todos los cables con un punto central de concentración.

[17] Backbone: se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.

d) **ESTRELLA EXTENDIDA.-**Una topología en 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) **JERÁRQUICA.-** Una topología jerárquica 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.-** La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio generando redundancia en las conexiones.

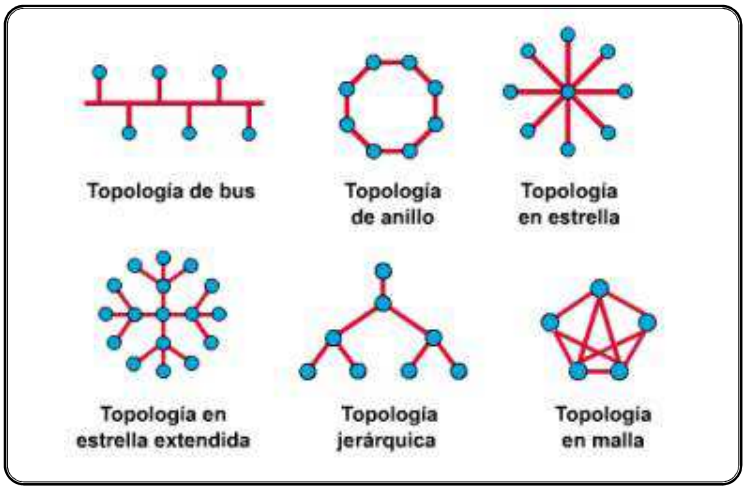


Ilustración 2:4 Topologías físicas de Red

La topología Lógica es la forma de comunicarse los hosts a través del medio físico; las topologías Lógicas más conocidas son:

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 quien no, aprovechando el canal de red; el ejemplo más común es Ethernet.

TRANSMISIÓN 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 tiene datos para transmitir, pasa el token al siguiente host hasta llegar al último host de la red, esta topología se utiliza en la topología Física de Token Ring o Anillo.

2.1.5 Protocolos De Transmisión

Para (Tanenbaum, 2003) un protocolo es un conjunto de reglas para controlar que la comunicación en una red sea más eficiente; para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red de manera correcta, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo; es decir, un protocolo de comunicaciones de datos es un conjunto de normas, o un acuerdo que determina el formato y la transmisión de datos.

Para lograr la comunicación y transmisión de datos se considera una estructura basada en capas; el protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos, al prepararlos para ser enviados a través de la red; los datos luego pasan a la siguiente capa, donde otro protocolo realiza otro conjunto diferente de operaciones.

Cuando el paquete llega a su destino, los protocolos deshacen la construcción del paquete armada en el origen, esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original, para que la aplicación pueda leer los datos correctamente.

2.1.5.1 Modelo OSI

Al inicio del desarrollo de las redes, el crecimiento fue desordenado por el enorme aumento en la cantidad y el tamaño de las redes, debido a que se introducían nuevas tecnologías de red de tipo propietario, redes que utilizaban diferentes especificaciones e implementaciones; lo que provocaba que se tengan dificultades para intercambiar información con tecnologías de red diferentes. Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) desarrolló un modelo de red, que ayuda a los fabricantes a crear redes que sean compatibles unas con otras, se publicó en 1984 el modelo de referencia de Interconexión de Sistemas Abiertos (OSI), siendo un modelo de red descriptivo (Cisco, 2005).

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI.

Dentro de las ventajas que ofrece el modelo OSI están:

a) Reduce la complejidad

b) Estandariza las interfaces
c) Facilita el diseño modular
d) Asegura la interoperabilidad de la tecnología

El modelo de referencia OSI se puede utilizar para comprender cómo viaja la información a través de una red, explica de qué manera los paquetes de datos viajan a través de varias capas a otro dispositivo de una red, aun cuando el remitente y el destinatario poseen diferentes tipos de medios de red; en el modelo de referencia OSI hay siete capas numeradas, cada una de las cuales ilustra una función de red específica.

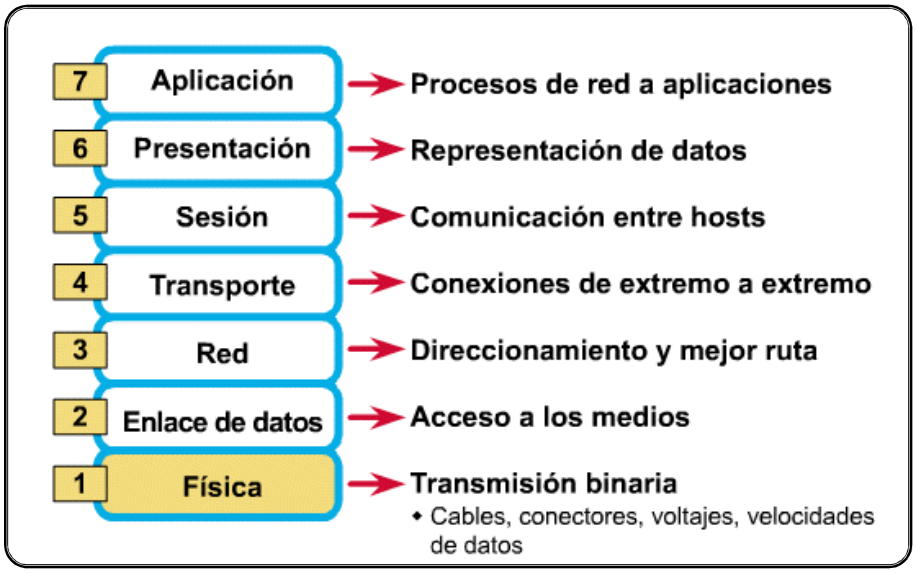


Ilustración 2:5 Capas del Modelo OSI

Capa Física.- Maneja todo lo correspondiente a trasmisión de pulsos eléctricos en modo de trasmisión binaria, abarca todo lo correspondiente a cables, conectores, voltaje y velocidades de transmisión de datos.

Capa de Enlace de Datos.- Se encarga del control de los enlaces y acceso a los medios, proveyendo una transferencia confiable de los datos a través de los mismos; brinda conectividad y selección de la ruta entre sistemas de direccionamiento lógico, basándose en la entrega del mejor esfuerzo.

Capa de Red.- Permite la asignación de la dirección de red y la determinación de la mejor ruta para llegar al destino, también provee la transferencia confiable de los datos.

Capa de Transporte.- Se encarga de las conexiones de extremo a extremo, establece, mantiene y termina circuitos virtuales, brindando adicionalmente un método de detección de fallas y control de flujo de la información.

Capa de Sesión.- Controla la comunicación de host mediante sesiones entre aplicaciones, desde su establecimiento, administración y cierre.

Capa de Presentación.- Se encarga de garantizar que los datos sean legibles para el sistema receptor, maneja el formato y la estructura de los datos, también negocia la sintaxis de transferencia de datos para las aplicaciones.

Capa de Aplicación.-Suministra servicios de red a los servicios de aplicaciones, por ejemplo transferencia de archivos, correo electrónico, etc.

El modelo OSI indica que las comunicaciones deben ser de par a par, es decir, que la capa del modelo OSI del origen debe comunicarse con su correspondiente capa en el destino; esto se logra mediante el intercambio de unidades de datos del protocolo (PDU), mismas que son específicos de cada capa, para que puedan llegar los PDU correspondientes a cada capa en el momento de la transmisión de datos, el PDU encapsula el PDU de la capa superior en el campo de datos de la siguiente capa. Cada PDU en su capa correspondiente recibe un nombre; para las capas de Aplicación, Presentación y Sesión se denominan **Datos**, cuando son encapsulados en la capa de transporte reciben el nombre de **Segmentos**, en el momento de encapsular en la capa de Red la PDU recibe el nombre de **Paquetes**, al pasar a capa 2 se encapsula en la PDU denominada **Trama** y al llegar al nivel de capa física se codifica la trama de enlace de datos en un patrón de **Bits** (Cisco, 2005)

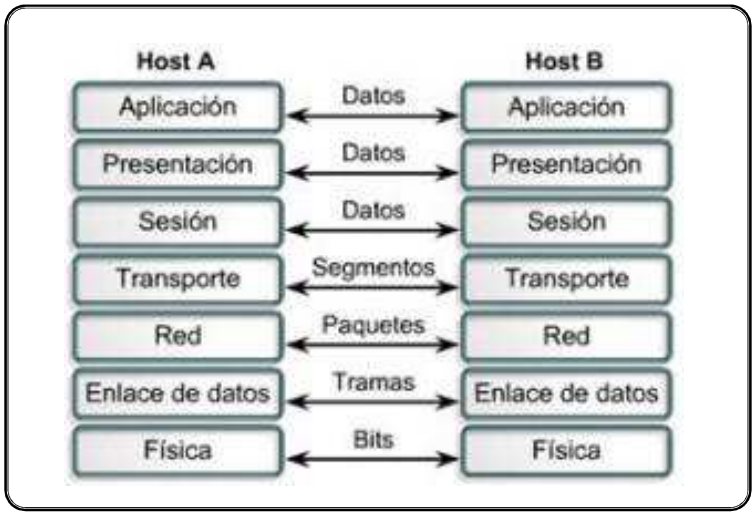


Ilustración 2:6 PDU de las Capas del Modelo OSI

2.1.5.2 Modelo TCP/IP

El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP, porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier circunstancia, y trabajar sobre cualquier medio físico. El TCP/IP se desarrolló como un estándar abierto, esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar. (Cisco, 2005)

El modelo TCP/IP tiene cuatro capas:

a) Capa de aplicación
b) Capa de transporte
c) Capa de Internet
d) Capa de acceso a la red

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. La capa de aplicación incluye los detalles de las capas de sesión y presentación OSI (Cisco, 2005).

La capa de transporte se encarga de los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores; uno de sus protocolos, el protocolo para el control de la transmisión (TCP) es un protocolo orientado a conexión, mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos; orientado a conexión significa que segmentos de la Capa 4(Aplicación) viajan de un lado a otro entre dos hosts, para comprobar que la conexión exista lógicamente en un determinado período de tiempo (Cisco, 2005).

La capa Internet divide los segmentos TCP en paquetes y los envía hacia la red de destino independientemente de la ruta que utilice; el protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes (Cisco, 2005).

La relación entre IP y TCP es importante; se puede pensar en el IP como el que indica el camino a los paquetes, en tanto que el TCP brinda un transporte seguro. El nombre de la capa de acceso de red, también se conoce como la capa de host a red, esta capa guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un

enlace físico; incluye los detalles de tecnología de networking y todos los detalles de la capa física y de enlace de datos del modelo OSI (Cisco, 2005).

2.2 Estándar TIA – 942 (Resumen)

2.2.1 Generalidades.

La Asociación de Industrias de Telecomunicaciones (TIA por sus siglas en ingles) 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 ingles), 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, 2005) con respecto al propósito dice: “Está elaborado para ser utilizado por los diseñadores, que necesitan una comprensión integral del diseño del DataCenter; incluyendo la planificación de la instalación, el sistema de cableado y el diseño de la red. La norma permitirá el diseño de centros de datos a ser considerado desde el inicio del proceso de construcción, contribuyendo a las consideraciones arquitecturales al proporcionar información que va a través de los esfuerzos de diseño multidisciplinarios; promover la cooperación en el diseño y las fases de construcción. Una planificación adecuada durante la construcción o renovación, es significativamente menos costosa y menos perjudicial que implementar luego que las facilidades están operativas. Los DataCenter en particular, pueden beneficiarse de la infraestructura que ha sido planeada con antelación para apoyar el crecimiento y los cambios en los sistemas informáticos que el DataCenter está diseñado para soportar.

Este documento, en particular, presenta una topología de infraestructura para el acceso y conexión de elementos respectivos en varias configuraciones de sistemas de cableado encontrados actualmente en el medio, con el fin de determinar los requisitos de

rendimiento de un cableado genérico, varios servicios de telecomunicaciones y aplicaciones fueron consideradas."

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; más de sesenta (60) organizaciones fueron las que contribuyeron con el desarrollo de este estándar, además guarda relación y contiene referencias con varios estándares y documentos publicados previamente por ANSI-TIA-EIA y entidades similares como: IEEE, NFPA y ASHRAE.

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

1. Alcance
2. Definición de términos, acrónimos, Unidades de Medida
3. Descripción del diseño del DataCenter
4. Infraestructura de Sistema de cableado de DataCenter
5. DataCenter Telecomunicaciones, espacios y topologías relacionadas
6. Sistemas de cableado de DataCenter
7. Vías de Cableado para DataCenter
8. 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

La norma recomienda varios pasos a seguir para el diseño de un nuevo DataCenter o para la expansión de un DataCenter existente, los pasos recomendados son:

Estimar equipamiento de telecomunicaciones, espacio, alimentación eléctrica y requerimientos de enfriamiento del DataCenter cuando esté a toda su capacidad, anticipando futuras implementaciones en el ciclo de vida del DataCenter.

Proveer espacio, alimentación eléctrica, enfriamiento, seguridad, carga de piso, aterrizaje, protección eléctrica y otros requerimientos para arquitectos e ingenieros. Proveer requerimientos para el centro de operaciones, área de carga, sala de almacenamiento, áreas de colocacion y otras áreas de soporte.

Coordinar preliminarmente los planos del DataCenter y sugerir cambios según lo requerido

Crear un plan de equipamiento de piso incluyendo la locación de cuartos principales y espacios para salas de ingreso, área de distribución principal, áreas de distribución horizontal, áreas de distribución de zonas y áreas de distribución de equipamiento.

Obtener y actualizar los planos de ingeniería con vías de acceso de telecomunicaciones, equipamiento eléctrico y equipamiento mecánico que se agregará al plan de piso del DataCenter a toda su capacidad.

Diseñar el sistema de cableado basado en las necesidades del equipamiento a ser colocado en el DataCenter.

A continuación se describirá los temas más relevantes de esta norma y que apoyan a la realización de este proyecto.

2.2.2 Diseño de DataCenter

Un DataCenter considerado típico posee una distribución de varios espacios, que son requeridos para soportar toda una infraestructura dedicada para almacenar cableado, telecomunicaciones y equipamiento. 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 (MC) que es el punto central de distribución del cableado estructurado, se

encuentra dentro de la sala de cómputo, cada DataCenter debe tener por lo menos una MDA conteniendo Routers principales, Switches de LAN core, Switches de SAN y PBX[18].

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, Swicthes KVM para manejo de equipos ubicados en dicho sitio. Un DataCenter pequeño no requiere un HDA necesariamente.

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, estas áreas no sirven al propósito de una sala de acceso un MDA o un HDA.

Dependiendo del tamaño del DataCenter no todos estos espacios son usados dentro de una estructura.

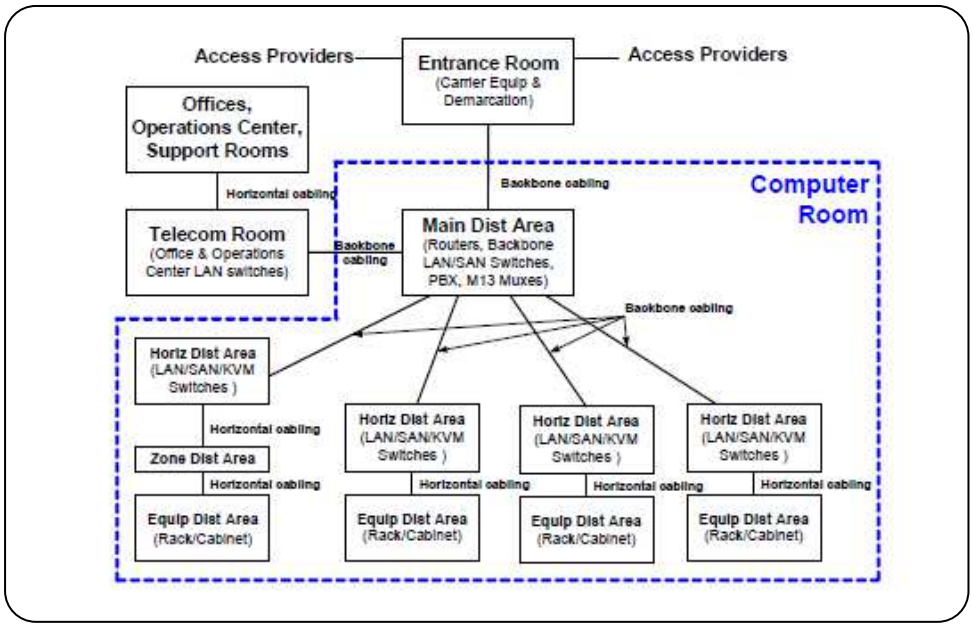


Ilustración 2:7 Ejemplo de topología básica de un DatCenter (TIA-942, 2005)

Se puede consolidar en el DataCenter el Main Cross-Conect y el Horizontal Cross-connect en una sola MDA, posiblemente en un solo gabinete o rack, el área de acceso y la

[18] PBX: ***P**rivate **B**ranch E**x**change. Central Telefonica Privada que gestiona llamadas internas y salida a llamadas externas.*

sala de telecomunicaciones pueden ser consolidadas dentro del MDA en una topología denominada DataCenter Reducido.

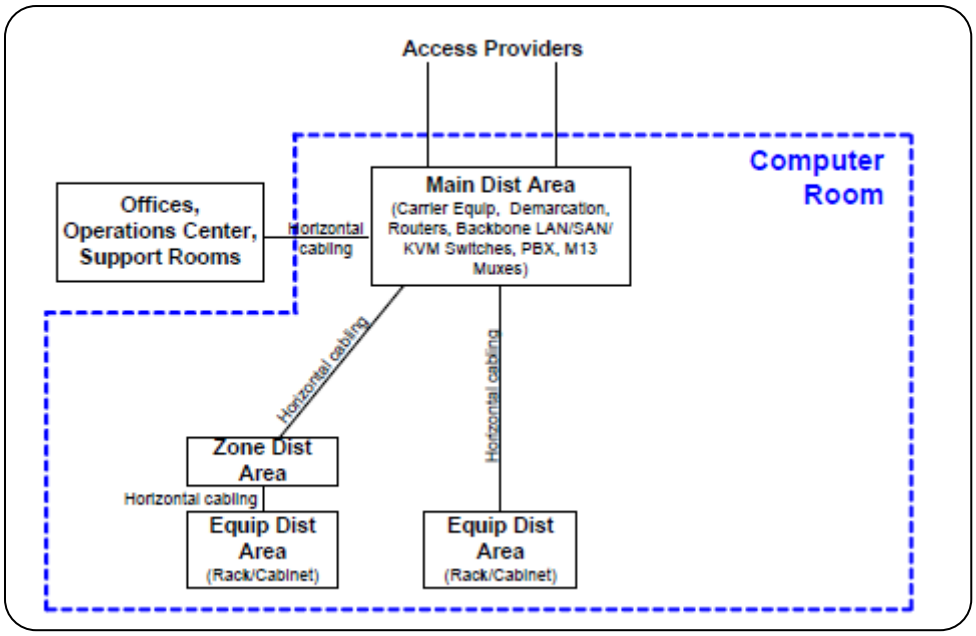


Ilustración 2:8 Ejemplo de topología de un DataCenter reducido (TIA-942, 2005)

Luego de la definición de distribución del DataCenter se debe revisar varios requerimientos como:

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

La norma (TIA-942, 2005) detalla varios aspectos para los requerimientos de un centro de cómputo como: locación, acceso, diseño arquitectónico; donde detalla las principales características que debe tener el espacio destinado a un DataCenter, como el tamaño que debe ser acorde a los requerimientos del equipamiento a ser instalado, la altura mínima de un centro de cómputo debe ser 2.6 metros desde el piso finalizado hasta el nivel donde se encuentren los elementos del techo, como luminarias o sensores. Las paredes y pisos deben ser sellados y pintados o construidos con material que minimice el polvo y debe tener un color que ayude a aumentar la iluminación de la habitación. Los pisos deben tener propiedades antiestáticas de acuerdo a la norma IEC 61000-4-2. Las puertas deben

ser de mínimo 1.0 metros de ancho y 2.13 metros de altura sin bisagras que brinden posibilidad de abrirse a ambos lados o ser desmontable. La carga de piso debe ser suficiente para soportar tanto la carga distribuida y concentrada de los equipos instalados con el cableado y los medios de comunicación, la mínima carga distribuida debe ser 7,2 kPa[19] (150 lbf[20]/m^2) y la carga recomendada es 12Kpa (250 lbf/m^2).

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 conexión en 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 cableado de cobre como para fibra óptica así como también las distancias entre terminaciones.

La norma (TIA-942, 2005) en el capítulo 6, describe detalladamente cada una de las características que debe tener todo el cableado como topología, y elección de medios, así como también hace referencia a normas asociadas como la TIA-568B; el capítulo 7 se destina para los canalizaciones de cableado donde se destaca la ubicación, separación entre cables y entre cableado eléctrico y de datos.

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

[19] kPa: KiloPascal
[20] Lbf: Fuerza en libras

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.

Se debe tomar en cuenta recomendaciones arquitecturales de construcción con materiales adecuados y no combustibles, con espacio abierto apropiado entre columnas, que maximice el espacio utilizable. Con respeto a consideraciones mecánicas, de telecomunicaciones y de seguridad y de permisos de acceso; se recomienda espacios alejados de instalaciones militares, laboratorios, aeropuertos y otras áreas dedicadas.

2.2.5 Flujo de Aire

"Se recomienda el uso de un sistema de enfriamiento o aire acondicionado dedicado para el DataCenter; sin embargo, si la sala de cómputo no tiene un HVAC dedicado, por lo menos debe estar ubicado con acceso listo para el HVAC principal del edificio. El servicio de HVAC debe ser provisto 24 horas al día 365 días al año" (TIA-942, 2005).

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° por hora
e) Equipamiento de humidificación se requiere.

En cuanto al flujo de aire y la ubicación de gabinetes, es necesario definir zonas especificas 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, 2005).

2.2.6 Instalaciones eléctricas

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.

La conexión a tierra esta normada por el estándar ANSI/TIA/EIA-J-STD-607-A que recomienda que debe haber una red de unión común para todo el Centro de Cómputo.

2.2.7 Tiers o niveles de infraestructura de DataCenter

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.

Tipo de construcción	**TIER 1** **DEPENDEINTE**	**TIER 2** **DEPENDEINTE**	**TIER 3** **INDEPENDEINTE**	**TIER 4** **INDEPENDEINTE**
Personal	No	1 turno	1 + turnos	siempre
Uso en Carga Máxima	100%	100%	90%	90%
Inicial bruto Watts por pie cuadrado (W/ft^2)	20-30	40-50	40-60	50-80
Final W/Ft^2	20-30	40-50	100-150[1,2,3]	150+[1,2]
Enfriamiento continuo	No	No	Puede ser	Si
Relación Espacio soportado a Piso elevado	20%	30%	80-90%[2]	100+%
Altura Piso elevado	12''	18''	30-36''[2]	30-36''[2]
Carga de piso $Lbs./Ft^2$	85	100	150	150
Utilidad de tensión	208-480	208-480	12-15 kV^2	12-15 kV^2
Puntos únicos de falla	varios+error humano	varios+error humano	pocos+error humano	ninguno+error humano

IT Downtime provocado Anual	28.8 h	22.0h	1.6h	0.4h
Disponibilidad	99.671%	99.749%	99.982%	99.995%
Meses para implementar	3	3-6	15-20	15-20
Año de primera implementación	1965	1970	1985	1995

Tabla 2:1 Cuadro descriptivo de características TIER para DataCenter

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 aun 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%

Una vez detallados los niveles de disponibilidad según las normativas, en el caso de Farmaenlace se espera acoplar el DataCenter en Tier 1 como mínimo, tratando de acoplar el presupuesto a lo que recomiendan las normas, en lo posible habrán temas que puedan apuntar a un nivel 2 de tier; pero si un solo aspecto no cumple con un nivel 2 el DataCenter no podrá ser considerado en este nivel.

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. Basándose principalmente en la arquitectura de red y en la filosofía de compartir recursos entre varios equipos computacionales y dispositivos conectados a la misma; las redes implementadas con equipos cuyo sistema operativo es Microsoft Windows soportan dos modelos de servicios de directorio: el grupo de trabajo (workgroup) y el dominio. El modelo dominio es el más utilizado en organizaciones que implementan servidores con Windows Server, está caracterizado por un solo directorio de recursos de la empresa (Active Directory), que confían en todos los sistemas de seguridad a lo largo del dominio; estos sistemas usan las directivas de seguridad para garantizar recursos como: usuarios, grupos y cuentas de computadoras, proveyendo una lista única que indica quién es quién en el dominio.

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. (Holem & Thomas, 2006).

Active Directory no puede existir sin un dominio y viceversa, un dominio es la principal unidad administrativa del servicio de directory de Windows Server. Una empresa podría tener más de un dominio en su Active Directory, la creación de varios dominios crean diversas estructuras lógicas llamadas árboles, que comparten nombres DNS contiguos, por ejemplo: farmaenlace.com, ibarra.farmaenlace.com y quito.farmaenlace.com; y pueden ser referenciados como un árbol. Si los dominios de Active Directory no comparten una raíz de dominio común se crean múltiples árboles, lo que lleva a una estructura más grande en un Active Directory, el bosque. Un bosque de active directory incluye todos los dominios de Active Directory, un bosque puede contener múltiples dominios en múltiples arboles o solo un dominio, cuando más de un dominio existe interviene un componente llamado catálogo global, quien provee la información sobre los objetos que están localizados en otros dominios en el bosque.

Adicional a la estructura del Active Directory, toda red necesita un mecanismo para resolver los nombres de computadores a direcciones IP, este requerimiento nace porque las personas y aplicaciones tratan de conectarse a la red de computadores especificando un nombre. DNS[21] es el sistema de nombramiento preferido en Windows Server, ofreciendo escalabilidad, seguridad y compatibilidad. Este servicio requiere una configuración previa para funcionar y se convierte en un elemento esencial en los dominios de Active Directory; en las redes de Windows Server la resolución de nombres DNS tiene la prioridad de nombres sobre NetBIOS, esta priorización es manejada por el servicio cliente DNS, el cual es responsable de direccionar la resolución de nombres, primero llamando a una resolución de nombres a través de DNS; si esta falla, el cliente DNS reenvía la solicitud del nombre a NetBIOS (Holem & Thomas, 2006).

[21] DNS: **Domain Name System** o **DNS** (**sistema de nombres de dominio**) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada

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 (Group Policy Object). (Holem & Thomas, 2006)

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 (Polchowski, 2003).

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.

En la configuración de DHCP se pueden incluir rangos de direcciones para ser repartidos en la red y también rangos de exclusión con direcciones que no necesitan ser entregadas a un host, también se puede reservar una dirección especifica asociada a la dirección física (MAC address) de tal manera que cada vez que el equipo que mantiene la reserva se conecte a la red, reciba siempre la misma dirección IP, esto con la finalidad de mantener una configuración especifica de acceso por ejemplo navegación por internet.

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. Por último se encuentran los documentos denominados planes de contingencia, que son manuales que detallan lo que se debe hacer para prevenir o enfrentar un posible desastre que incluya la caída de los servicios y pérdida de información; de tal manera que se pueda garantizar la recuperación de los mismos en el menor tiempo posible y con el menor impacto en tiempo y disponibilidad al usuario final.

CAPÍTULO 3

3 IMPLEMENTACIÓN DEL PROYECTO (Datacenter, Equipos y Redes)

En los capítulos anteriores se señaló los antecedentes y el levantamiento correspondiente de los datos necesarios para la implementación del proyecto en todos sus ámbitos, se da inicio a todos los trabajos para llevar a cabo la implementación del DataCenter de Farmaenlace Cía. Ltda. Este capítulo detalla todo el trabajo realizado conjuntamente el área de Redes Servicios y Telecomunicaciones del Departamento de Sistemas con el Departamento de Infraestructura, para la adecuación física o arquitectónica, instalación de cableado estructurado y migración de equipos con su respectiva ubicación en el nuevo DataCenter.

3.1 Adecuación Arquitectónica de DataCenter de Farmaenlace Cía. Ltda.

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) Requerimientos 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

Como se menciona en el capítulo 1 de levantamiento de requerimientos, el espacio físico de la instalación del centro de cómputo de Farmaenlace no es suficiente para albergar todos los dispositivos, tampoco es suficiente el sistema de ventilación y enfriamiento; además de las instalaciones eléctricas y el soporte de UPS. Todos estos aspectos son fundamentales para proceder con la implementación del proyecto; siendo los cambios en el área de sistemas los que a continuación se detallan:

3.1.1 Cambios arquitectónicos

La norma (TIA-942, 2005, pág. 27) 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 Data Center, la norma (TIA-942, 2005, pág. 27) 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

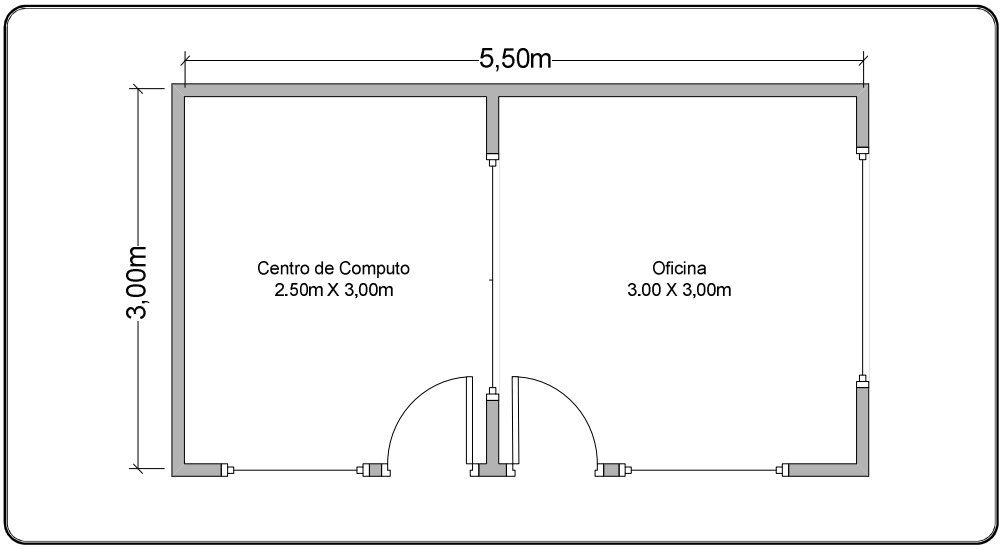


Ilustración 3:1 Diagrama de DataCenter antes del cambio

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, 2005, pág. 28), las puertas deben tener un mínimo de 1 m de ancho y 2.13 m 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.

Al realizar estas adecuaciones de obra civil el área del DataCenter queda de la siguiente manera:

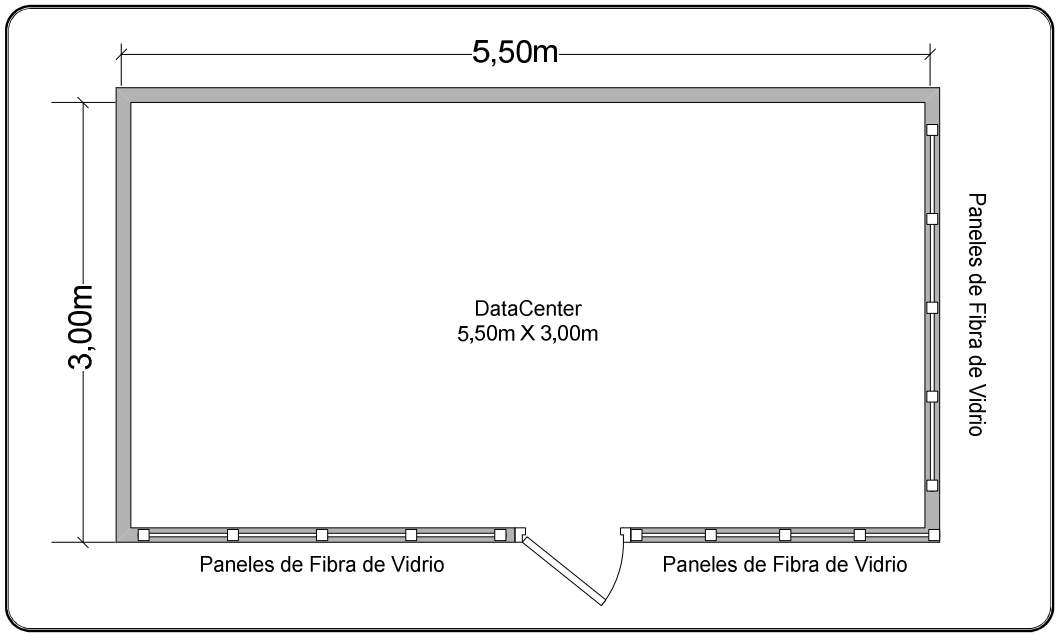


Ilustración 3:2 Diagrama de espacio de DataCenter luego del cambio

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, 2005, pág. 27) 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 Farmaenlace poseía un sistema de enfriamiento de confort que resultaba suficiente en el área en que se encontraban ubicados, 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; decisión que no se apega a las normas establecidas.

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, 2005, pág. 29) 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 de Farmaenlace 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.

Se realiza la instalación de un aire acondicionado marca Liebert DATAMATE, de 30700 BTU/H de precisión diseñado para operar 24 horas 365 días, controlando de manera automática cinco parámetros críticos (Liebert Corporation, 2010):

a) Temperatura, graduable en mínimo + /- 1C
b) Humedad Relativa en rangos de 45% + /- 5%, con lo que se controla los efectos de corrosión y corrientes electroestáticas.
c) Velocidad de Movimiento de Aire desde 600 a 15200 CFM (Cooling Flow Movemement)
d) Filtración de Aire que circula en el área, lo que garantiza que partículas unidas con la humedad se conviertan en caminos conductivos en las tarjetas electrónicas.
e) Manejo de Disipación que brinda mayor circulación de aire frío y absorción rápida y efectiva del calor.

Está compuesto de dos elementos:

Evaporador.- diseñado para el control de temperatura en aplicaciones de equipos electrónicos, es capaz de enfriar, calentar, humidificar, deshumidificar y filtrar el aire dentro del DataCenter. Posee un control de procesamiento de temperatura y humedad con operación programable, una pantalla de control que muestra las condiciones ambientales y el estado de operación del sistema HVAC, botones de mando e indicación para programación y alarmas.

Condensador.- es la unidad exterior que debe ubicarse fuera del DataCenter a una distancia no mayor de 20 metros.

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 frío 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 frío por la parte superior paralelo al techo del DataCenter, de tal manera que el flujo de aire frío llegue al pasillo en la parte frontal de los racks; es decir el pasillo frío.

Ilustración 3:3 Imágenes del aire acondicionado Liebert Datamate

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 Servicios y Telecomunicaciones podrá ingresar también al DataCenter. La puerta de acceso al área posee un lector magnético que detecta la proximidad de la tarjeta y si la identifica, libera el magneto electrónico que bloquea la puerta no permitiendo el acceso o salida a menos que la tarjeta sea identificada.

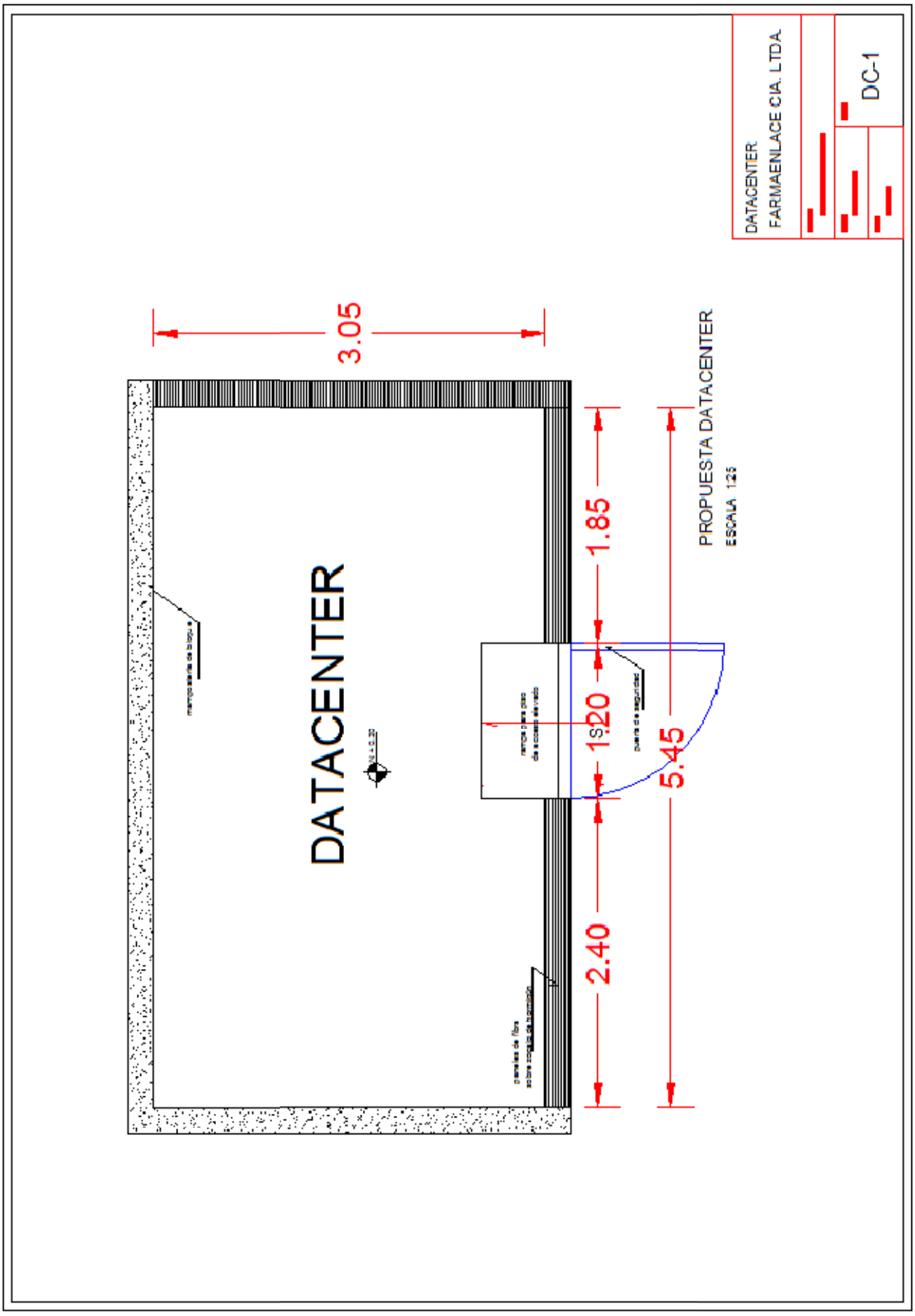
Ilustración 3:4 Imágenes acceso por tarjeta magnética

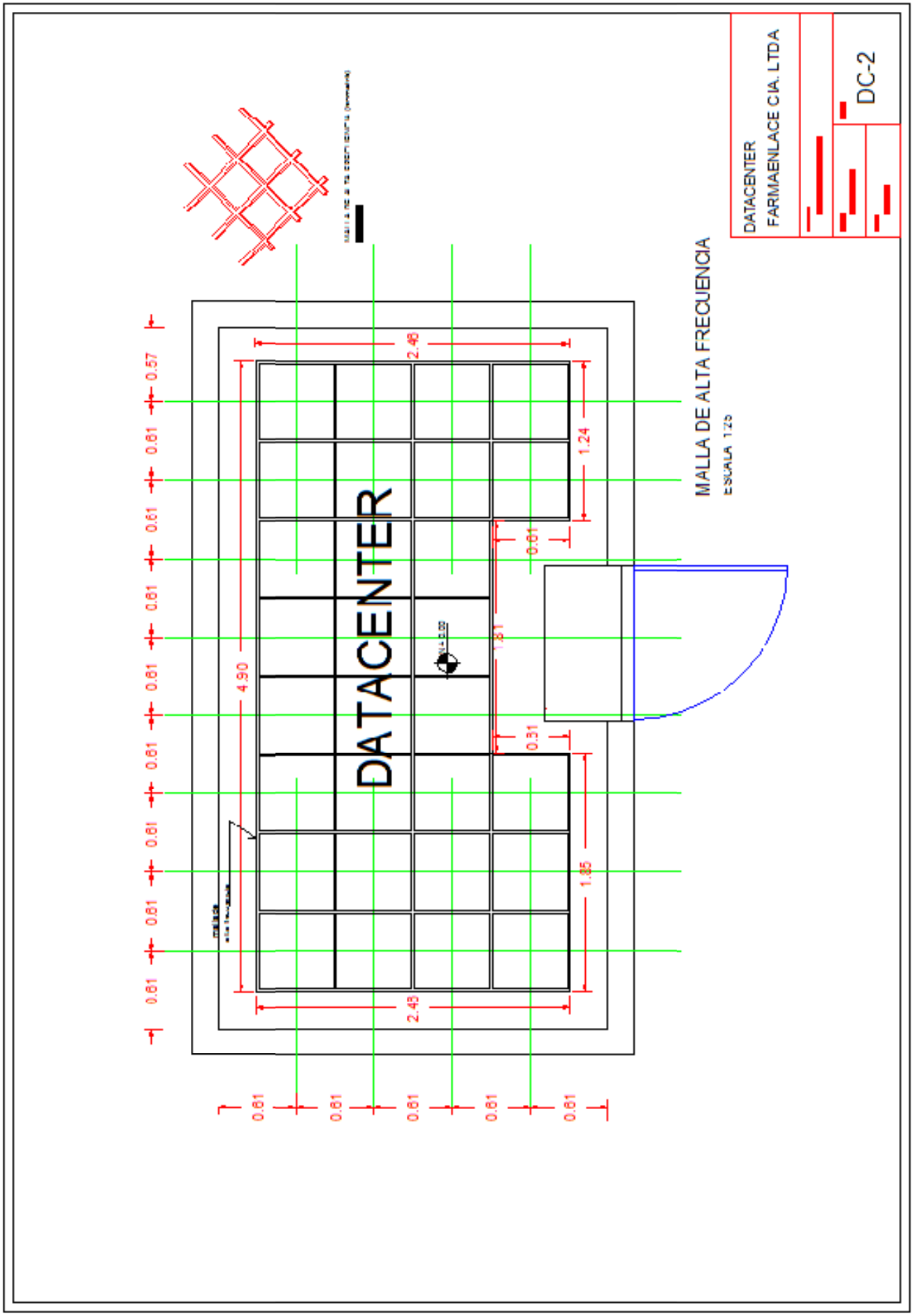
Se ha realizado un estudio de factibilidad para la instalación de un sistema de extinción de incendios, considerando la recomendación de la norma (TIA-942, 2005, pág. 109) que dice: "Un sistema de extinción de incendios de agente limpio proporciona el más alto nivel de protección para la sala de cómputo 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.

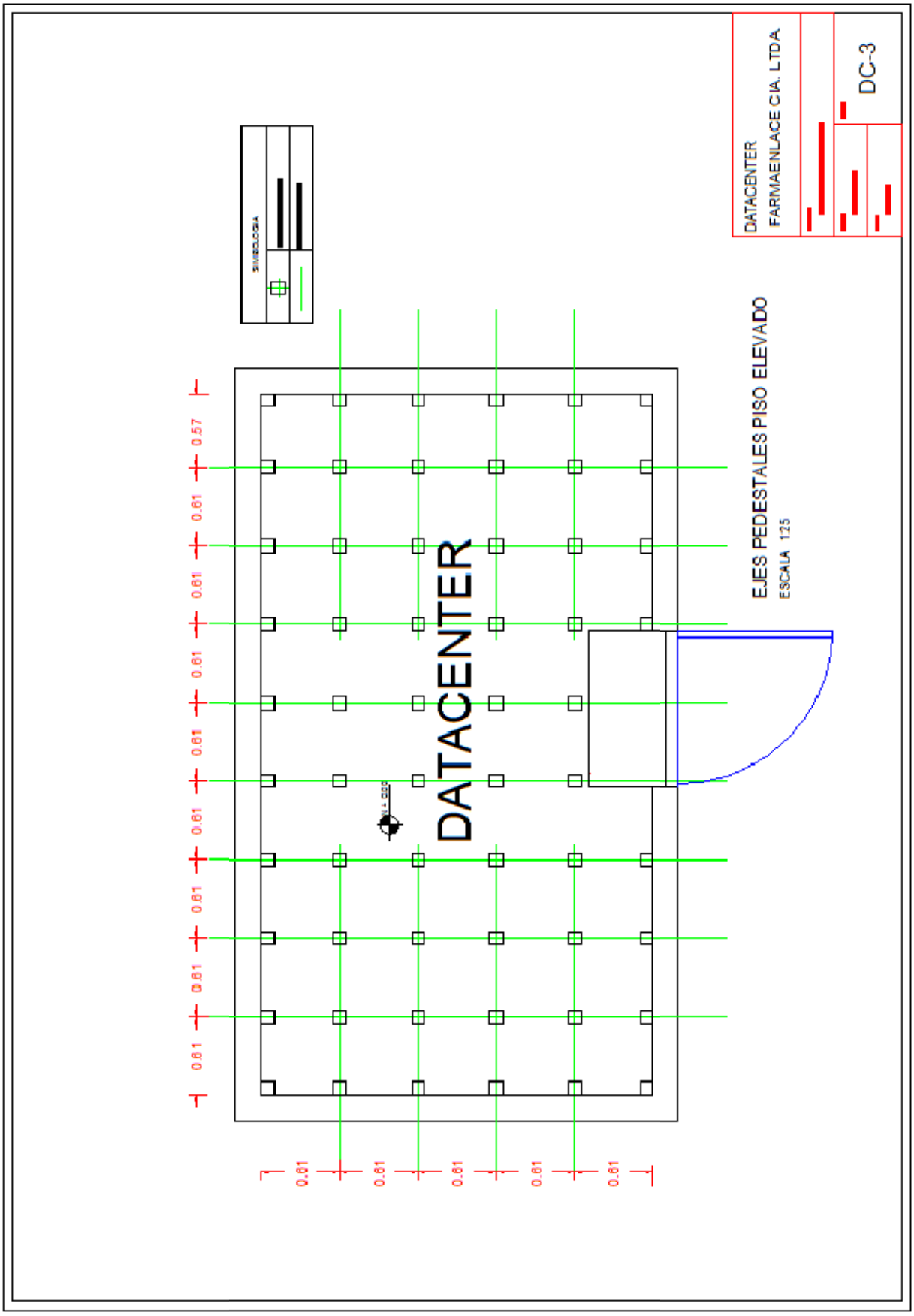
Con respecto a la posibilidad de inundación o infiltración de agua al DataCenter, se ha realizado la impermeabilización completa de todo el techo del edificio principal de Farmaenlace; garantizando que no se producirán infiltraciones de agua debido a las lluvias y en vista que el DataCenter se encuentra ubicado en el segundo piso, no tiene posibilidad de ser víctima de una inundación.

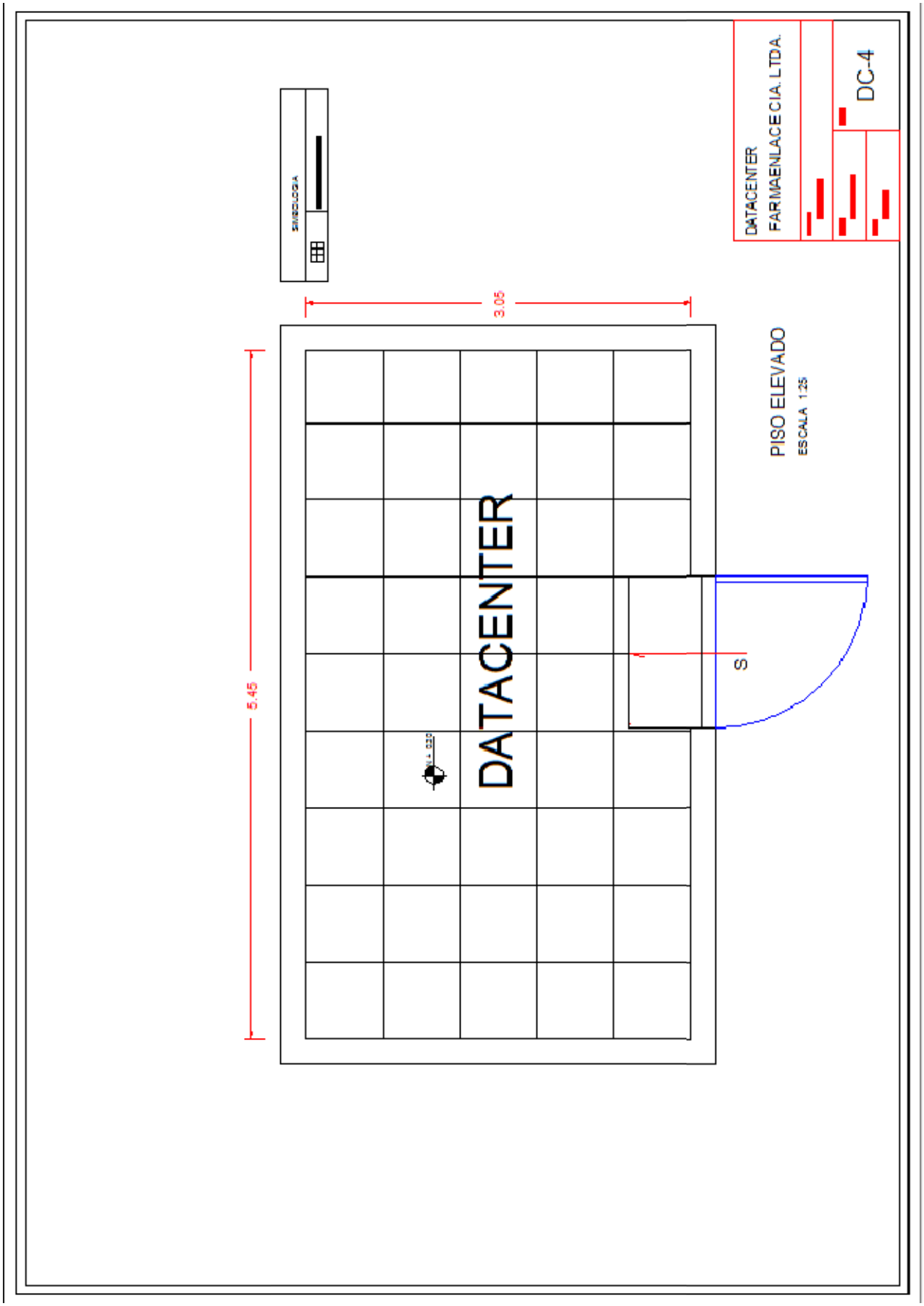
Se sugirió en el levantamiento de requerimientos la posibilidad de implementación de piso elevado para el DataCenter, como complemento a este proyecto se ha realizado el diseño de implementación de piso elevado para el DataCenter de Farmaenlace, lamentablemente por el limitante de altitud en la estructura del edificio de Farmaenlace 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.

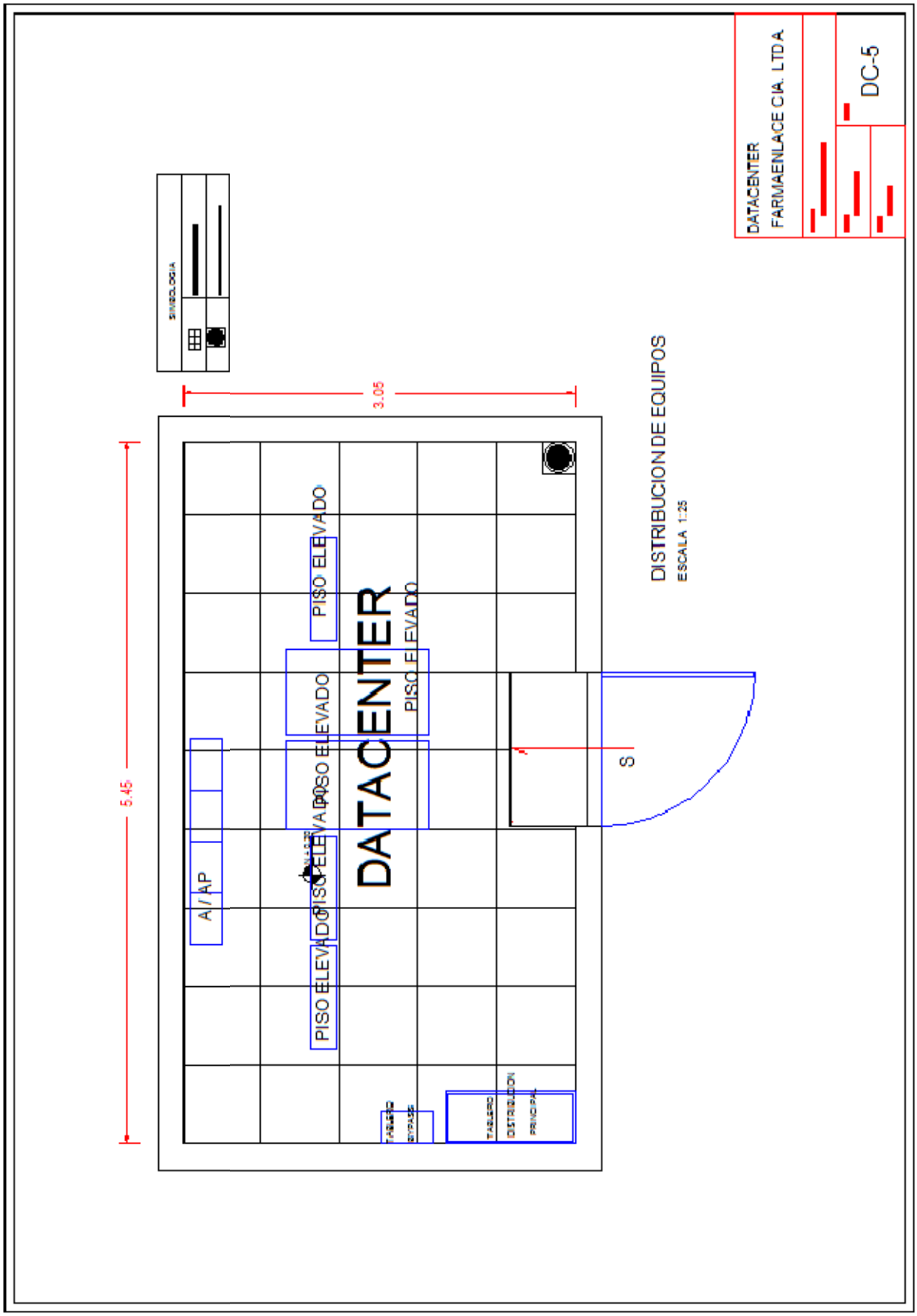
A continuación se incluyen los gráficos arquitectónicos de la colocación de piso elevado para el DataCenter de Farmaenlace, en el caso de que fuera posible su implementación.


DATACENTER
FARMAENLACE CIA. LTDA.
DC-1
3.05
DATACENTER
1.85
1.20
2.40
5.45
PROPUESTA DATACENTER
ESCALA 1:25


DATACENTER
FARMAENLACE CIA. LTDA
DC-2
MALLA DE ALTA FRECUENCIA
ESCALA 1:25
2.46
2.43
4.90
1.24
1.85
1.81
0.61
0.31
0.57


DATACENTER FARMAENLACE CIA. LTDA.
DC-3
SIMBOLOGIA
EJES PEDESTALES PISO ELEVADO
ESCALA 1:25
DATACENTER
0.57
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61
0.61


DATACENTER
FARMAENLACE CIA. LTDA.
DC-4
SIMBOLOGIA
3.05
5.45
DATACENTER
PISO ELEVADO
ESCALA 1:25
S


DATACENTER
FARMAENLACE CIA. LTDA.
DC-5
SIMBOLOGIA
3.05
5.45
DISTRIBUCION DE EQUIPOS
ESCALA 1:25
DATACENTER
PISO ELEVADO
PISO ELEVADO
PISO ELEVADO
PISO ELEVADO
A/A
S
TABLERO
DISTRIBUCION
PRINCIPAL

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). (DataCenter Consultores, 2011).

1. Clase:

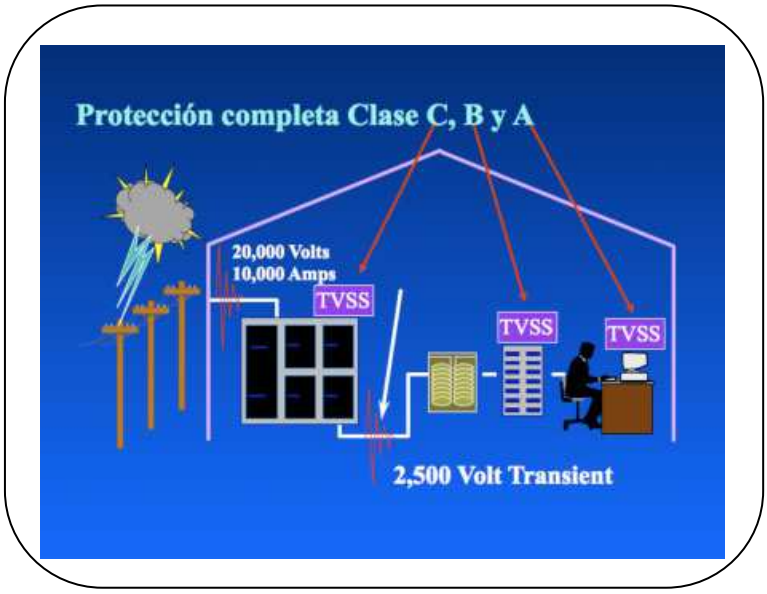


Ilustración 3:7 Diagrama de protección completa Clase C,B y A

- Clase A
- Clase B
- Clase C

2. Capacidad de amperios en barras:

- ☐ Más de 3001
- ☐ 3000 – 2001
- ☐ 2000 – 1201
- ☐ 1200 – 601
- ☐ 600 – 226
- ◉ 225 – 126
- ☐ 125 – 60

3. Nivel de exposición

a. Tipo de actividad

- ☐ Médica – Industria – Telecomunicaciones
- ☐ Banca
- ◉ Comercial
- ☐ Instituciones – PYMES
- ☐ Residencial

b. Nivel de incidencia de rayos

- ☐ Extrema incidencia de rayos

- ☐ Severa incidencia de rayos
- ☐ Moderada incidencia de rayos
- ◉ Leve incidencia de rayos
- ☐ Nula incidencia de rayos

c. Distancia a fuentes de generación eléctrica

- ◉ 50 KM o menos
- ☐ 51 a 75 KM
- ☐ 75 a 125 KM
- ☐ 126 a 180 KM
- ☐ 181 KM o más

d. Cercanía a industrias y subestaciones

- ☐ Menos de 1 KM
- ◉ 1 a 5 KM
- ☐ 5 a 10 KM
- ☐ 15 a 20 KM
- ☐ 21 KM o más

RESULTADO

- Capacidad en Amp Filtro Clase A: 225
- Capacidad en KA TVSS Clase B: 130
- Capacidad en KA TVSS Clase C: 160

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.

1. KW de salida del sistema de UPS:

10

2. KW de iluminación

5

3. KW de aire acondicionado:

6

4. KW de otras cargas:

5

5. Eficiencia del sistema UPS:

0.94

Valor de eficiencia mínimo recomendado 0.94 a plena carga

- ***6. Coeficiente de recarga de barterías(CRB):***
- ○ 1.25
- ○ 1.15
- ◉ 1.00

  Entre menor sea, más tiempo demora el cargador del UPS en restablecer la capacidad máxima de las baterías.

RESULTADO

Capacidad del generador (KW): 28

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.

1. Cantidad de gabinetes de servidores y telecomunicaciones (0 – ∞):

5

2. KW por gabinete(1 – 30 KW):

1

- Colocar un valor entre 1 y 30
- Promedio mundial 3.5 KW/ Gabinete

3. Carga de diseño estimado en KW (CD):

5

4. Factor de seguridad (CD):

- ◉ 1.2
- ○ 1.3

1.2: Margen de seguridad para crecimiento y operación del 20%

1.3: Margen de seguridad para crecimiento y operación del 30%

5. Fases:

- ○ Monofásico
- ◉ Trifásico

6. Voltaje:

- ○ 120 V
- ◉ 240 V / 120 V
- ○ 208 V / 120Y V
- ○ 480 V / 277/120 V

RESULTADO:

Capacidad del UPS: KW: 6 KVA: 9

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 Farmaenlace garantizando un continuo flujo eléctrico; se traslada el UPS que se encuentra en el centro de cómputo de Farmaenlace 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 Farmaenlace 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 de Farmaenlace 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:

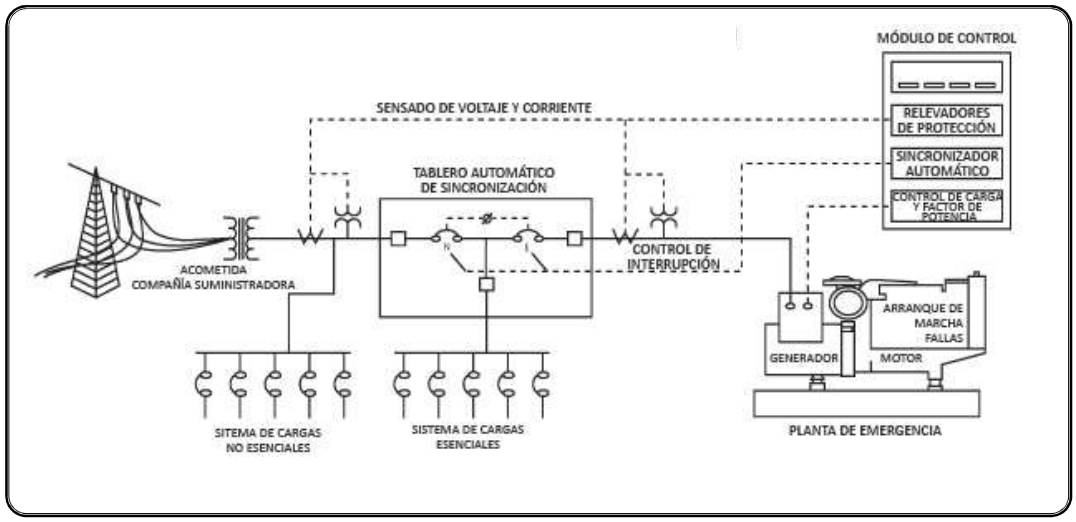


Ilustración 3:8 Esquema de conexión de instalaciones eléctricas con generador

La norma (TIA-942, 2005)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 equipo no adecuado para enchufar en lineas 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"

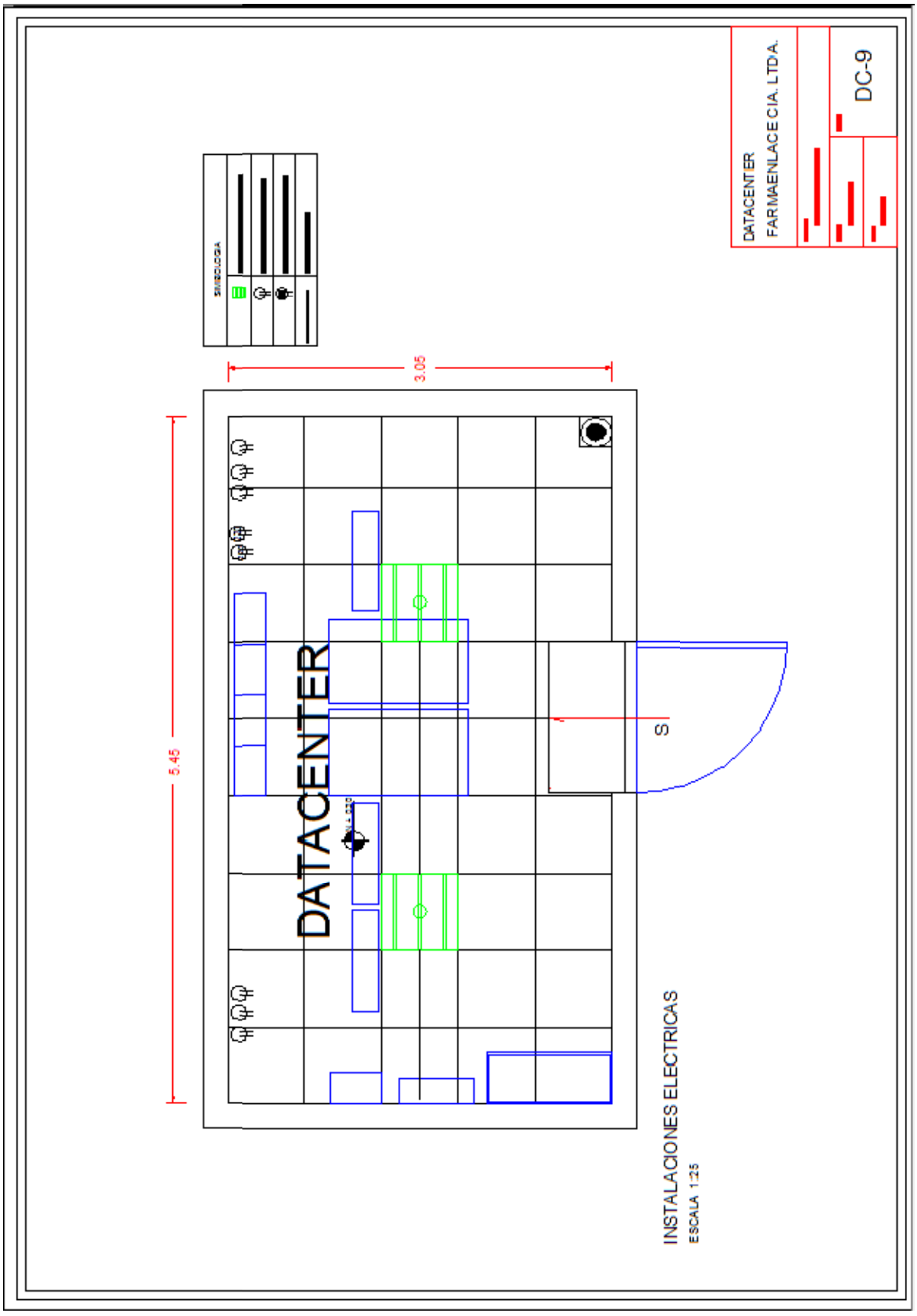
En el DataCenter se procede hacer dos circuitos de acometida de energía eléctrica a 220 voltios para alimentación eléctrica a los equipos servidores, con la finalidad de garantizar el balanceo de carga de alimentación a 220 v. También se realiza una acometida adicional a 110v, manejando el mismo principio de continuidad para alimentar a los equipos que trabajan a este voltaje.

En todo el edificio de Farmaenlace se manejan dos circuitos eléctricos, uno de energía regulada mismo que trabaja con el respaldo de los UPS y el generador eléctrico, principalmente diseñado para la conectividad de equipos que necesiten regulación de voltaje y alimentación continua; y un circuito de alimentación no regulada al que se pueden conectar todo tipo de artefactos eléctricos y al que también está interconectado el sistema de iluminación de todo el edificio; esto aplicado al Data Center ayuda a cumplir el enunciado anterior de la norma TIA 942 para diseño eléctrico.

La norma (TIA-942, 2005) 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 que # 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 de Farmaenlace poseen conexión a tierra, por el mismo sistema de tendido eléctrico que se encuentra instalado en el edificio.

A continuación se encuentra el diagrama de las instalaciones eléctricas del DataCenter de Farmaenlace Cía. Ltda.


DATACENTER
FARMAENLACE CIA. LTDA.
DC-9
3.05
5.45
DATACENTER
S
INSTALACIONES ELECTRICAS
ESCALA 1:25

3.1.3 Cableado Estructurado de Oficinas

Debido al crecimiento en las oficinas de Farmaenlace se torna necesaria la adecuación de los espacios, para distribuirlos de manera ordenada con la correspondiente reubicación de personal.

El departamento de contabilidad fue ubicado en la zona que antes era el auditorio de Farmaenlace, 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).

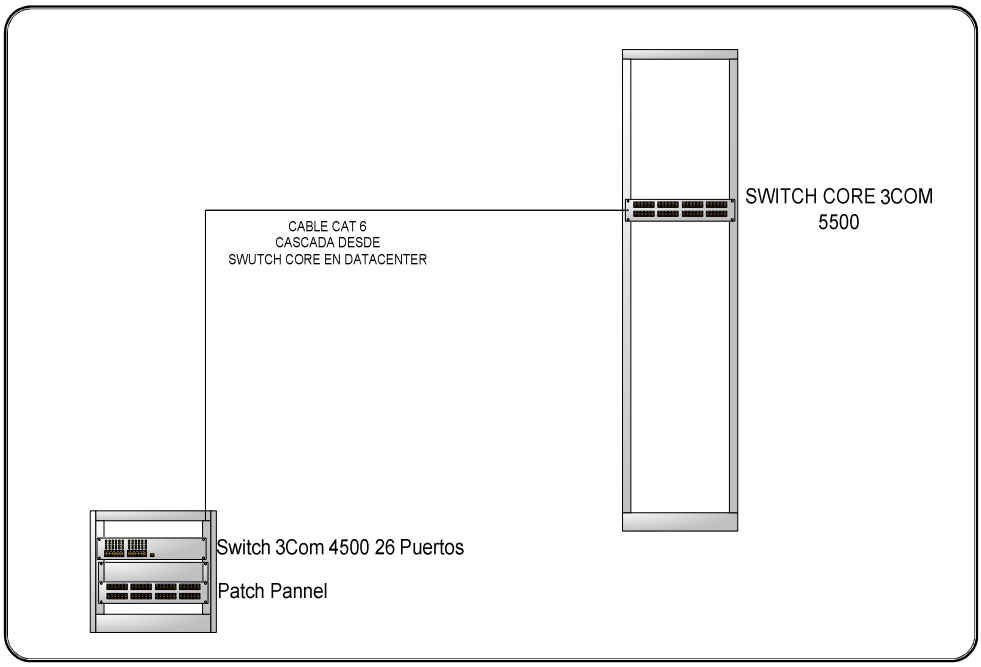
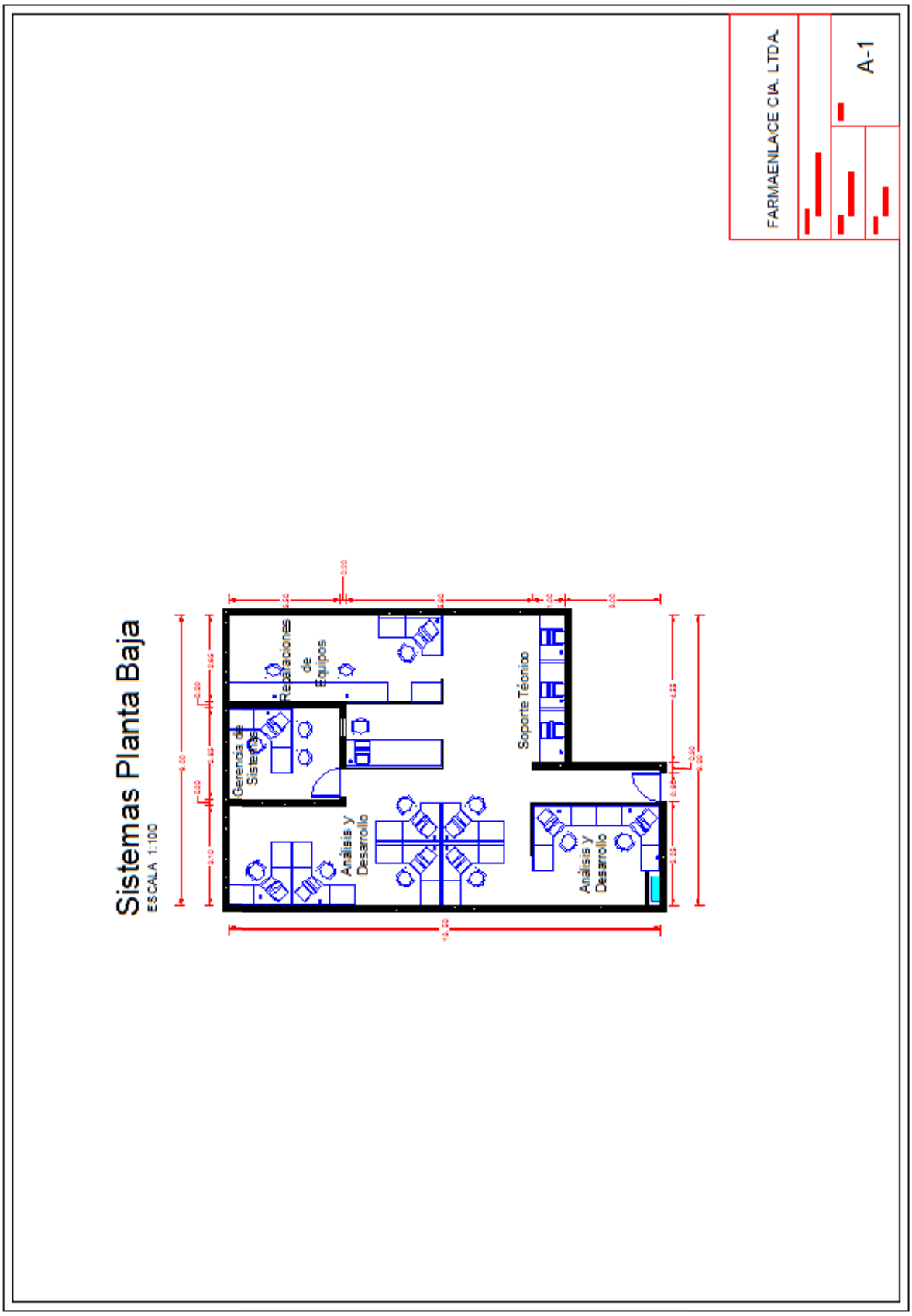


Ilustración 3:10 Diagrama de Conexión de Switch en Cascada

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.

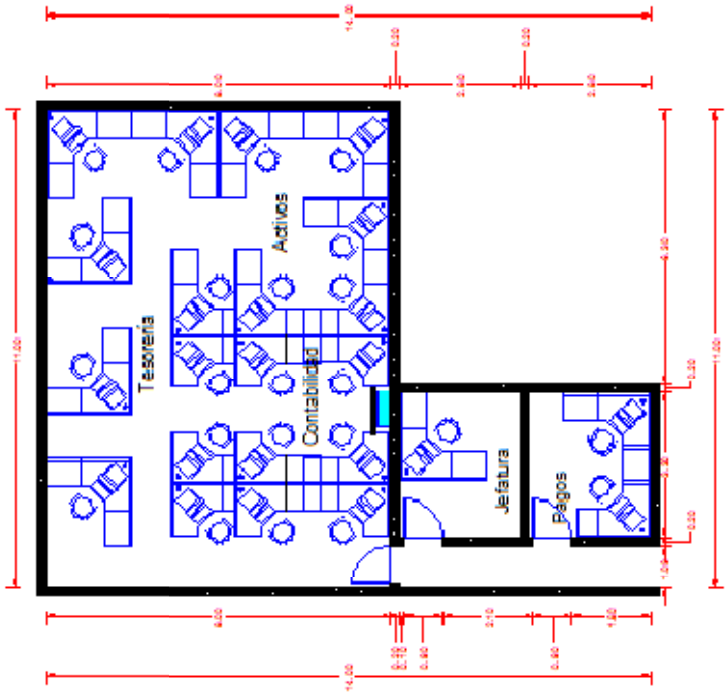
En esta área se tenía instalado previamente un rack de pared donde llegaba el cableado estructurado, se aprovecha este rack para aterrizar todos los puntos resultantes en la adecuación de esta zona. Este rack tiene conexión directa con el Data Center.

Para la ubicación del departamento de recursos humanos se construyó la segunda planta en las instalaciones que se encuentran en la parte posterior del edificio de Farmaenlace, se efectuó la implementación del cableado estructurado en categoría 6. En esta nueva ala se realiza la instalación de 53 puntos incluyendo oficinas, auditorio, sala de capacitación informática y sala de pruebas computarizadas.


FARMAENLACE CIA. LTDA.
A-1
Sistemas Planta Baja
ESCALA 1:100
Reparaciones de Equipos
Gerencia de Sistemas
Análisis y Desarrollo
Soporte Técnico
Análisis y Desarrollo

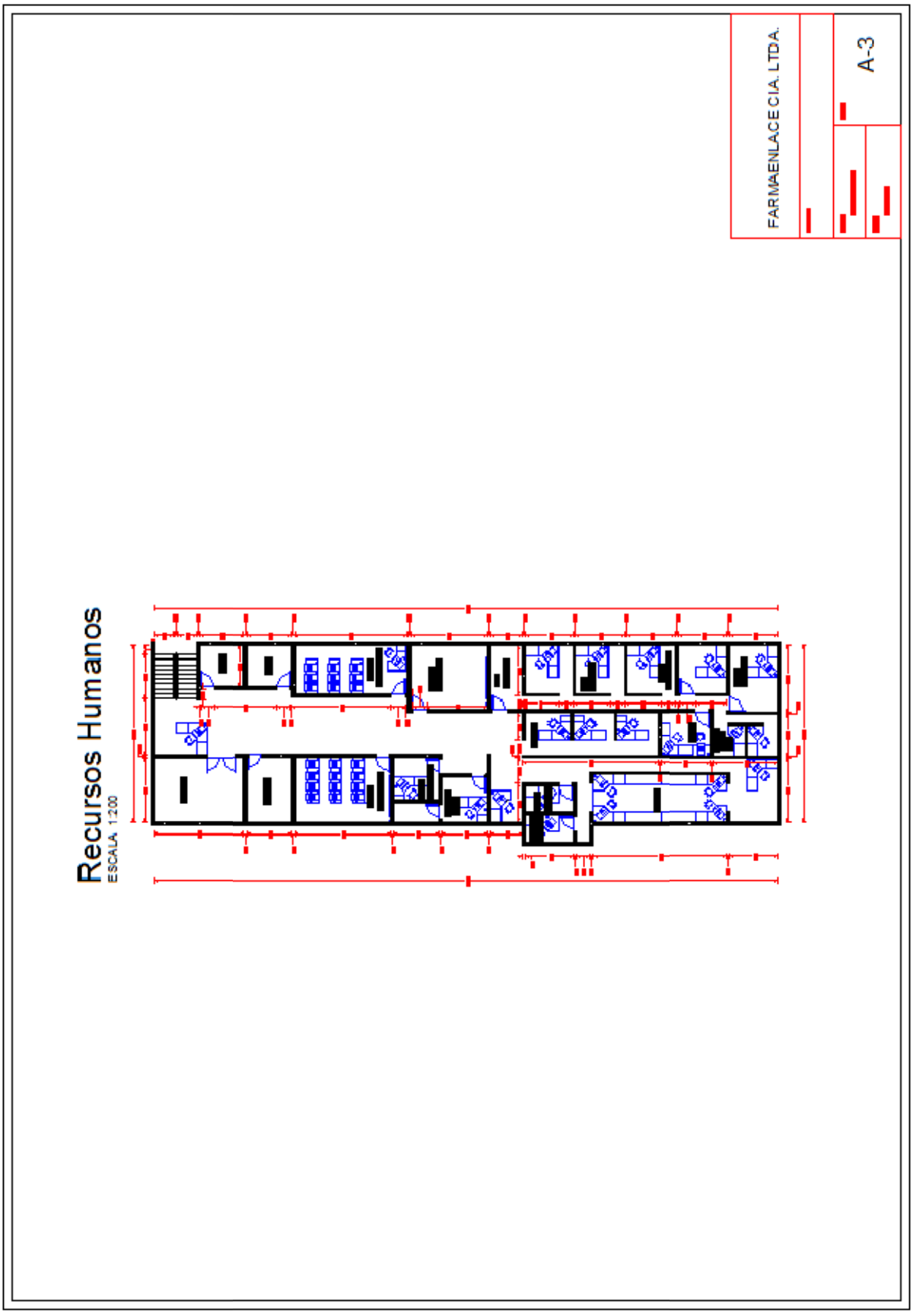
FARMAENLACE CIA. LTDA.

A-2



Contabilidad

ESCALA 1:100


FARMAENLACE CIA. LTDA.
A-3
Recursos Humanos
ESCALA 1:200

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 Farmaenlace manejará en lo posterior, así como también la adquisición y puesta en marcha de servidores de mejores características para la implementación de nuevos servicios.

Contando con ayuda de un equipo de colaboradores y proveedores externos se procede a evaluar y definir el tipo de equipamiento de networking que necesita la empresa. A continuación se describe las características de los equipos y la configuración que deben tener los mismos.

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 Farmaenlace, 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 Farmaenlace (192.168.238.0 /24)
- **VLAN 2 :** Red LAN Farmacia Medi Magda La Luz (192.168.101.0 /24)
- **VLAN 3 :** Red de telefonía IP (192.168.110.252 /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 de Farmaenlace y el edificio de Magda supermercados donde se ubica la farmacia, el diagrama de conectividad con los modelos de switches seria de la siguiente manera:

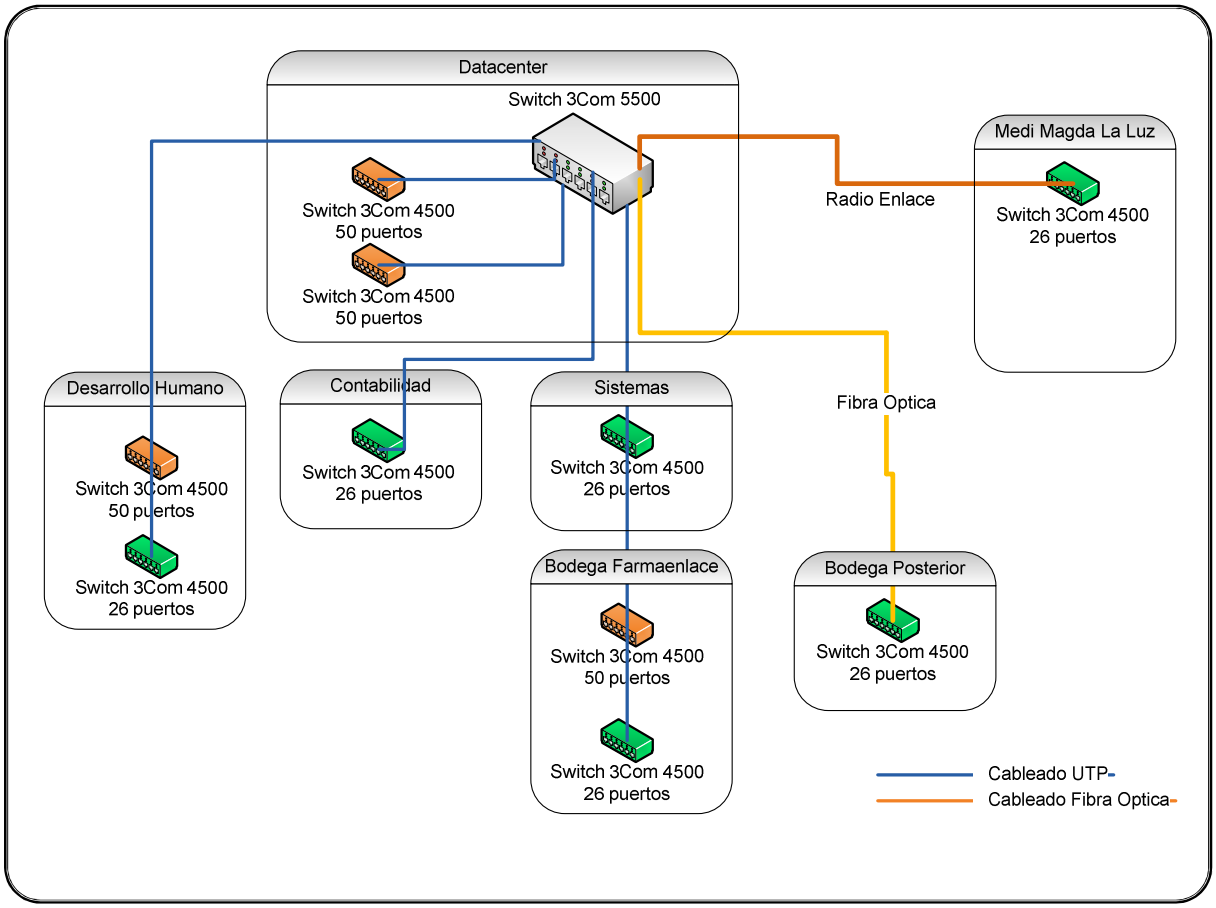


Ilustración 3:14 Distribución de Switches en Farmaenlace Cía. Ltda.

Las características de los dispositivos son las siguientes:

SWITCH 3COM 5500G

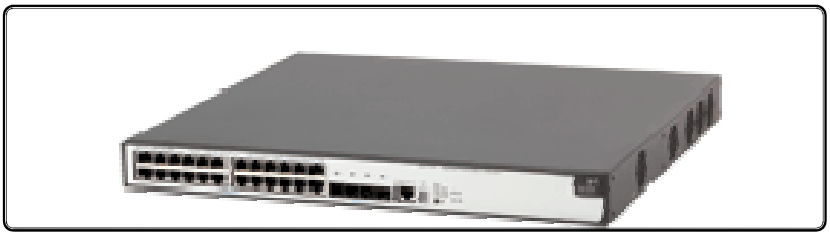


Ilustración 3:15 Switch 3Com 5500G 28 puertos

(3Com, 2010) 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.

El Switch 5500G-EI soporta tecnología de apilamiento 3Com XRN® distribuido y resistente ante fallos, con ancho de banda de apilamiento de 48 Gbps (96 Gbps full-duplex) y routing avanzado de Capa 3 (RIP / OSPF), QoS de Capa 2-4 y funcionalidades de limitación de velocidades.

Ofrece funcionalidades de seguridad - SNMP v3, SSH, login de red - y apilamiento resistente ante fallos y hot-swappable, para una administración y monitorización simplificadas.

Dimensiones: Altura: 43,6 mm; anchura: 440 mm, fondo: 450 mm

SWITCH 3COM 4500G

Ilustración 3:16 Switch 3Com 4500 26 y 50 puertos

(3Com, 2010) 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 4500 ofrece 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.

Se pueden apilar hasta ocho switches mediante puertos Gigabit Ethernet, por lo que toda una pila puede administrarse como una única entidad de administración IP.

24 o 48 puertos 10/100 y dos puertos Gigabit de uso dual permiten al Switch 4500 proporcionar una conectividad de LAN segura y fiable para redes

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 Farmaenlace.

Se decidió la adquisición de un sistema de servidores Blade de marca HP modelo C3000 con 6 servidores de cuchilla. Además de dos servidores apilables tipo rack de marca HP. Cuyas características se describen a continuación:

3.2.2.1 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 16 servidores 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 Area 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 o Chasis.
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 Farmaenlace se optó por un sistema de servidores Blade en un Enclosure marca HP modelo C3000, este sistema de Blade tiene dos presentaciones tipo torre o tipo Rack, soporta hasta un máximo de 8 servidores como muestra el grafico a continuación:

Ilustración 3:17 HP BladeSystem C3000 vista frontal (HP, 2011)

El chasis del C3000 tiene 8 subdivisiones donde se pueden insertar los servidores blade, cada subdivisión es una unidad del chasis, existen servidores que ocupan 2 unidades del chasis, en estas unidades además de servidores también pueden ser instalados módulos de discos para que sean asignados a un servidor como una unidad de almacenamiento de mayor tamaño en caso de que sea necesario. Adicional posee una pantalla de configuración y administración, donde se puede observar el estado del BladeSystem y realizar operaciones de configuración que sean requeridas, como por ejemplo asignar la unidad de CD a un servidor en específico o determinar si un servidor está alarmado y las posibles causas de problema. (HP, 2011).

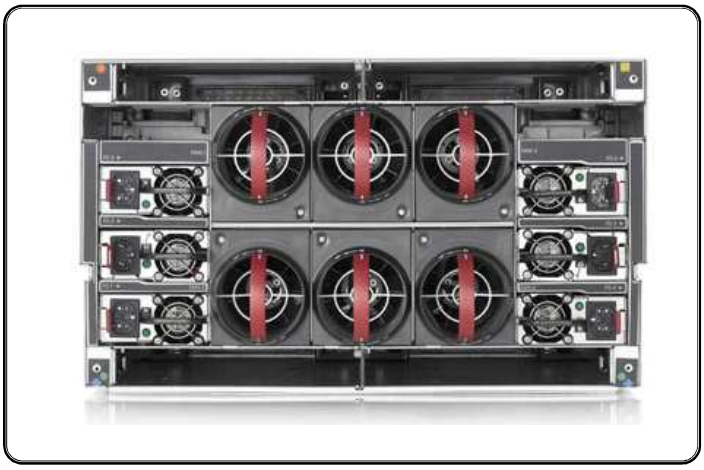


Ilustración 3:18 HP BladeSystem C3000 vista posterior (HP, 2011)

En la parte posterior se ubican las fuentes de poder redundante tres a cada costado y en la parte central hasta 6 ventiladores del sistema de enfriamiento que soporta todo el chasis c3000.

Las partes que componen al chasis C3000 son las siguientes:

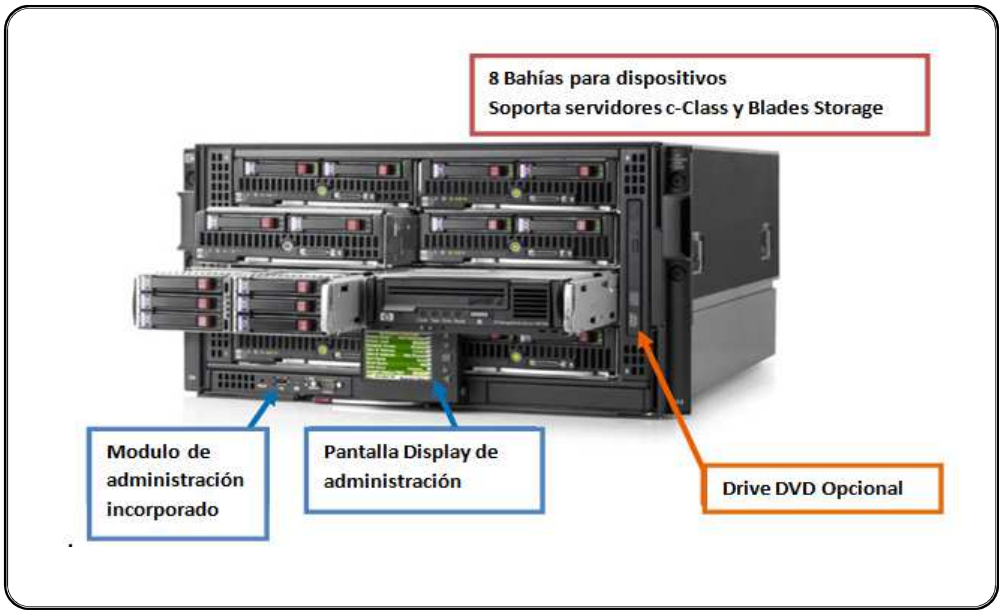


Ilustración 3:19 Componentes de HP BladeSystem C3000 (HP, 2011)

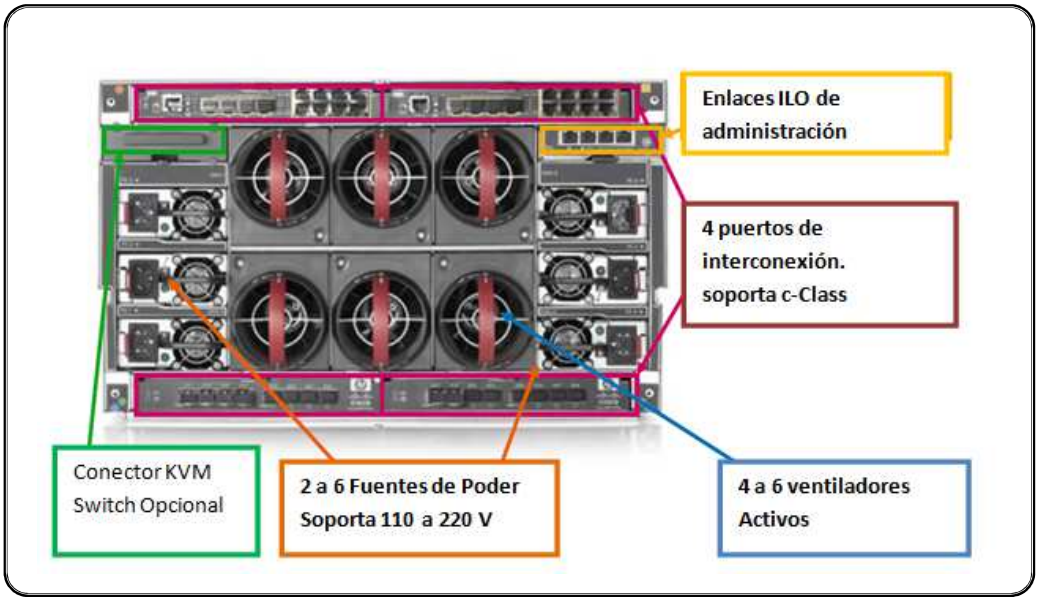


Ilustración 3:20 Elementos de HP BladeSystem C3000 vista posterior (HP, 2011)

En el enclosure BladeSystem C3000 se proceden a instalar dos servidores HP BL480c que ocupan 2 unidades del chasis.

Ilustración 3:21 Servidor HP Bl480c

Características:

a) Modelo: Hp Proliant Bl480c
b) Procesador: Intel Xeon 2.66Ghz
c) Memoria: 8 GB
d) Disco: 4 Discos Sata 146GB
    1. Servidor 192.168.238.2: dos discos Raid 1+0 146GB
    2. Servidor 192.168.238.19: 1 disco Raid 5 450GB
e) Sistema Operativo: Windows 2003 Enterprise

Se instalan también cuatro servidores Bl 460c que ocupan una unidad del chasis

Ilustración 3:22 Servidor HP Bl 460c

Características:

a) Modelo: Hp Proliant Bl480c

b) Procesador: Intel Xeon 2.50Ghz
c) Memoria:
    1. Servidor 192.168.238.1: 4 GB
    2. Servidor 192.168.238.6: 8 GB
    3. Servidor 192.168.238.26: 16GB
d) Disco: 2 Discos Sata 146GB
    1. Servidor 192.168.238.1: 1 disco Raid 1+0 146GB
    2. Servidor 192.168.238.6: 1 disco Raid 1+0 146GB
    3. Servidor 192.168.238.26: 1 disco Raid 0 290GB
e) Sistema Operativo:
    1. Servidor 192.168.238.1: Windows 2003 Enterprise
    2. Servidor 192.168.238.6: Windows 2003 Enterprise
    3. Servidor 192.168.238.26: Windows 2008 Standard

Adicional de los servidores incluidos en el BladeSystem se adquirió dos servidores con las siguientes características:

Ilustración 3:23 Servidor HP DL380 G5

a) Modelo: HP Proliant DL380 G5
b) Procesador: Intel Xeon 3.00 GHz
c) Memoria: 8GB
d) Disco: 8 discos 146GB
    1. 1 disco Raid 1+0 146GB
    2. 1 disco Raid 5 690GB
e) Sistema Operativo: Windows 2003 Enterprise
f) Interfaz de red: 2

g) Dvd ROM

Ilustración 3:25 Servidor HP DL380 G6

Ilustración 3:24 Servidor DL380 G6

a) Modelo: HP Proliant DL380 G6
b) Procesador: Intel Xeon 2.67 GHz
c) Memoria: 16GB
d) Disco: 2 discos 146GB
    1. 1 disco Raid 1+0 146GB
e) Sistema Operativo: Windows 2008 Standard 64Bits
f) Interfaz de red: 2
g) Dvd ROM

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 Farmaenlace Cía. Ltda., 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

Según (Wikipedia, 2011) 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 óptico consta de varios componentes esenciales:

a) La fuente de luz
b) El medio de transmisión
c) 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 tomar en 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.

Si se hace un corte transversal de un cable de fibra, se pueden distinguir sus componentes principales:

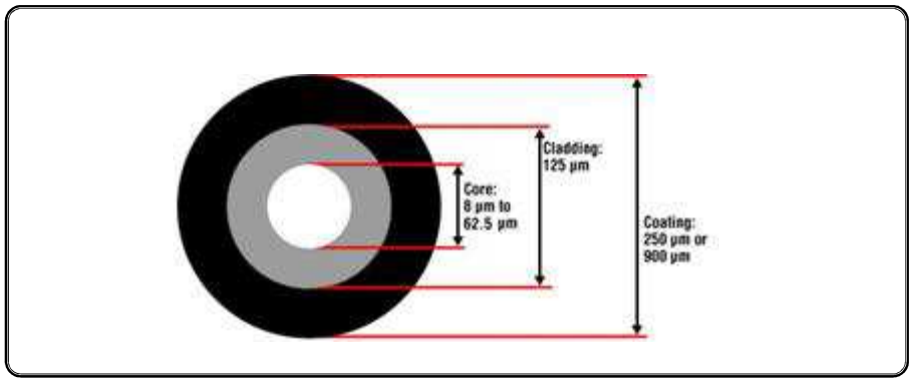


Ilustración 3:26 Componentes de Cable de Fibra Óptica

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 (SiO2) 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.

Dependiendo el tipo de índice de refracción del núcleo, tenemos dos tipos de fibra multimodo, el índice escalonado que el núcleo tiene un índice de refracción constante en toda la sección cilíndrica, tiene alta dispersión modal. Y el índice gradual en el cual el

índice de refracción no es constante, tiene menor dispersión modal y el núcleo se constituye de distintos materiales.

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).

Las fibras monomodo no sufren tanto el fenómeno de la dispersión como las multimodo ya que por la fibra sólo viaja un pulso de luz cada vez. También tiene menos atenuación (absorción parcial al ser reflejada en el revestimiento) lo que garantiza una transmisión de la señal más fidedigna. (Infiesta Saborit, 2008).

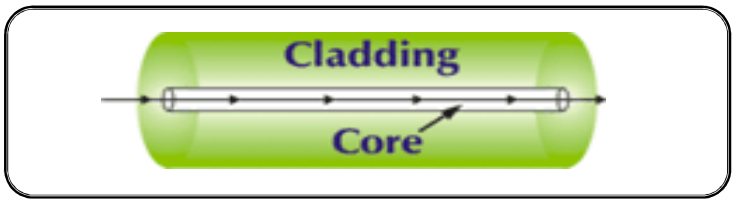


Ilustración 3:27 Transmisión de haz de luz (Infiesta Saborit, 2008)

Una de las desventajas de este tipo de fibras, es que al ser el núcleo mucho más estrecho, la conexión entre dos fibras tiene que ser mucho más precisa, encareciendo los conectores y el coste del cable en general.

Existen 3 tipos básicos de fibra monomodo: NDSF, DSF y NZ-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 (Infiesta Saborit, 2008).

Los conectores son interconexiones fibra a fibra que alinean el núcleo de ambas fibras y la principal diferencia entre ellos es el tipo de enganche mecánico 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.

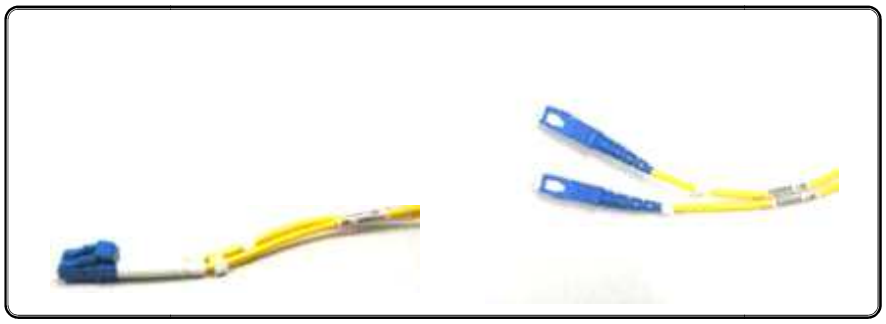


Ilustración 3:28 Conectores de Fibra Óptica

Con el conocimiento de que tipo de fibra utilizar, se decide que se instale fibra multimodo, por ser diseñada para distancias cortas y un costo menor que una fibra monomodo. Para la instalación es necesario colocar el cable de fibra desde el DataCenter de Farmaenlace ubicado en el segundo piso del edificio Farmaenlace, llevarlo hasta la zona posterior de bodega, recubriendo el cable en las partes que quedan a la intemperie con un conducto plástico para protección del cable.

Vista desde la Fachada:

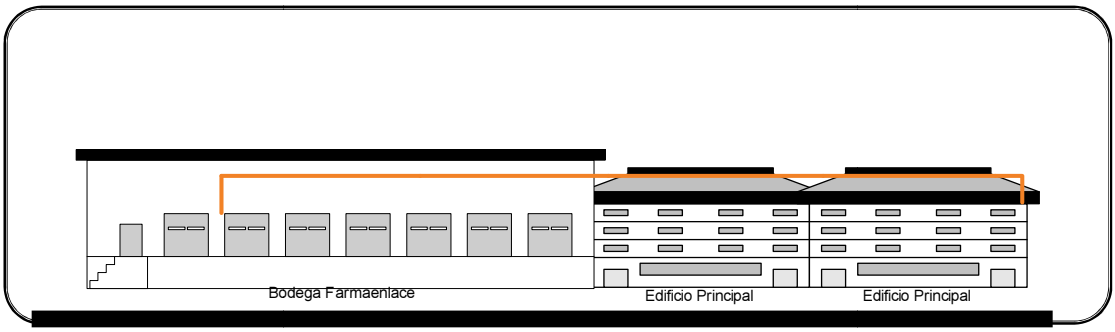


Ilustración 3:29 Diagrama de tendido de Fibra Óptica

Vista Aérea:

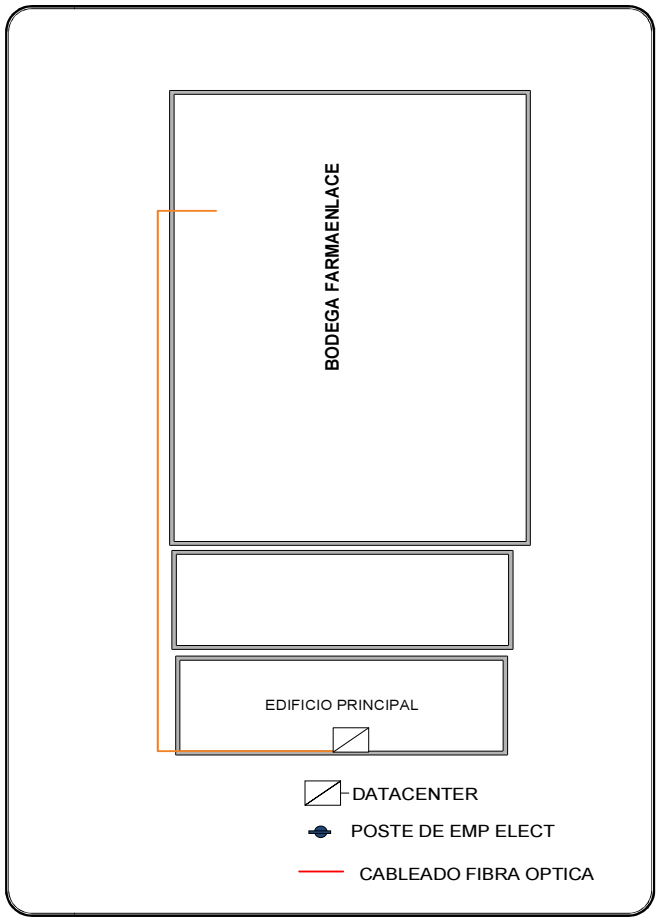


Ilustración 3:30 Diagrama de tendido de Fibra Óptica 2

Siguiendo con el diagrama se procede con la instalación del cable de fibra, tendiéndolo por el edificio hasta llegar a la bodega desde el DataCenter de Farmaenlace.

Ilustración 3:31 Colocación de Cableado en postes exteriores

Cuando se tiene listo el cable de extremo a extremo, se procede con el empalme en bandejas como la que se muestra a continuación:

Ilustración 3:32 Bandejas de Empalme de Fibra Óptica

Por un extremo ingresa el cable de fibra óptica que proviene del exterior, según el modelo de bandeja o caja de empalme, hay bandejas que tienen cable de fibra óptica interno que desemboca en dos patch cord de fibra o a dos conectores donde se colocan los patch cord de fibra, para el enlace directo que se está instalando se necesitan empalmar dos filamentos para TX (Transmisión) y RX (recepción).

Para realizar el procedimiento de empalme se debe hacerlo utilizando el método de Fusión, que es un empalme permanente y se realiza con una maquina empalmadora.

Ilustración 3:33 Empalmadora de Fibra Óptica

Realizar los siguientes pasos (yio.com.ar, 2007):

1. Con una pinza especial (125 micrones) se retira el recubrimiento del filamento de fibra aproximadamente unos 5cm.

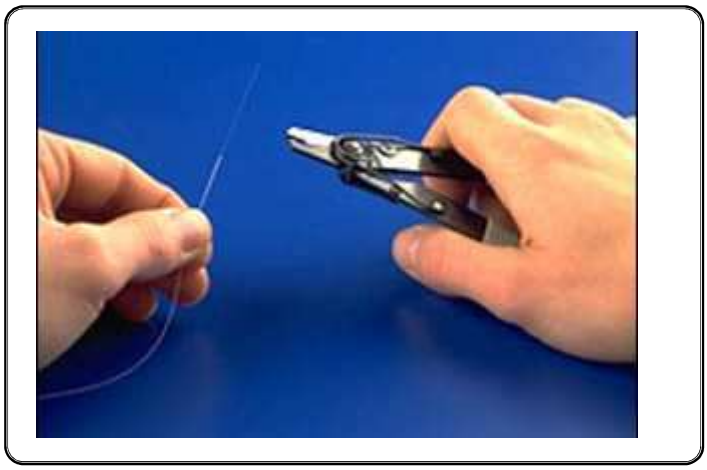


Ilustración 3:34 Fusión de F.O. paso 1

2. Se limpia la fibra con un papel suave humedecido con alcohol isopropílico.

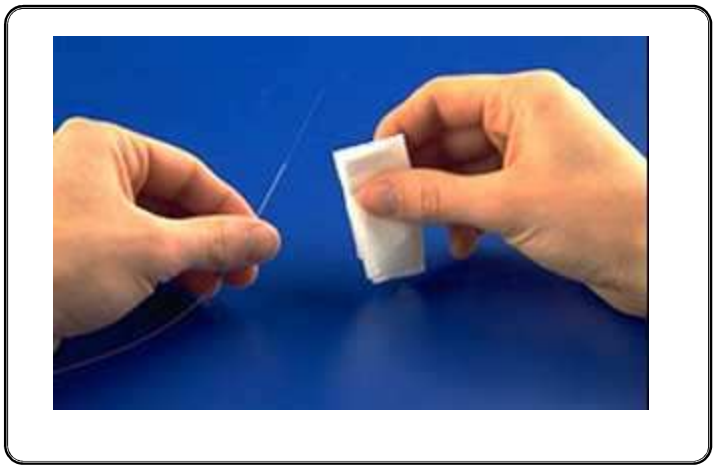


Ilustración 3:35 Fusión de F.O. paso 2

3. Se corta la fibra a unos 8 a 16 mm con una cortadora especial (cutter o cleaver) con hoja de diamante apoyando la fibra dentro del canal, haciendo coincidir el final del recubrimiento (coating) con la división correspondiente a la medida. Una vez cortada la fibra no se debe volver a limpiar ni tocar.

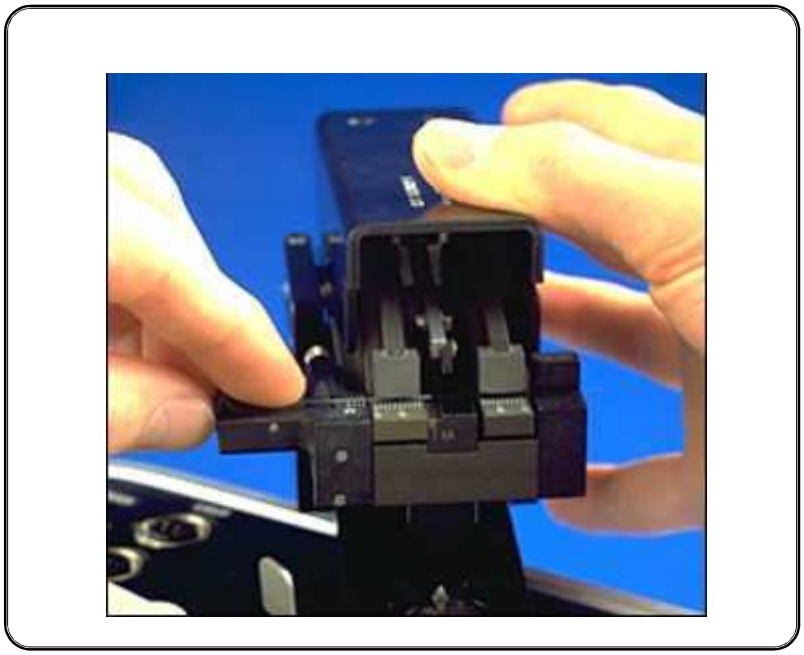


Ilustración 3:36 Fusión de F.O. paso 3

4. Se introduce la fibra en la empalmadora, procurando que la fibra no haga contacto con nada. Lo mismo se debe hacer con el otro extremo de fibra a empalmar.

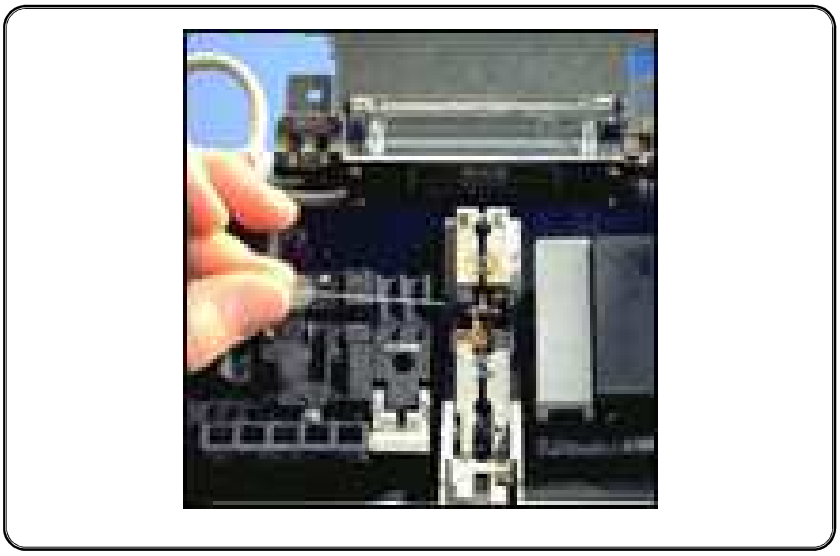


Ilustración 3:37 Fusión de F.O. paso 4

5. En la pantalla de la máquina se puede observar las dos puntas y se puede distinguir si el ángulo de corte es recto completamente (90 grados), de no ser así, la máquina no permite el empalme.

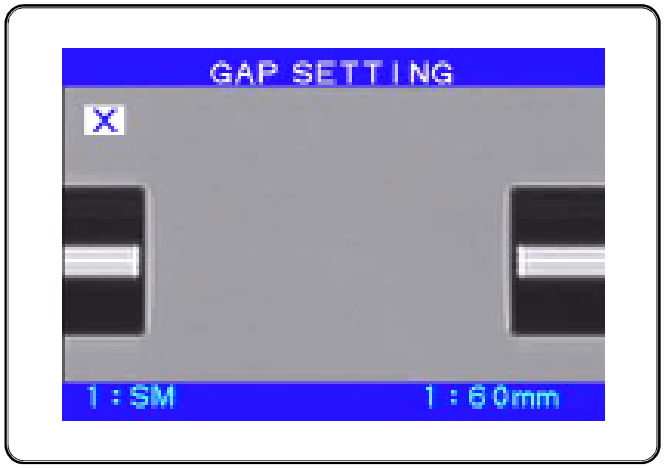


Ilustración 3:38 Fusión de F.O. paso 5

6. Se presiona el botón de empalme y la empalmadora automáticamente alinea los ejes y acerca las puntas a la distancia correcta.

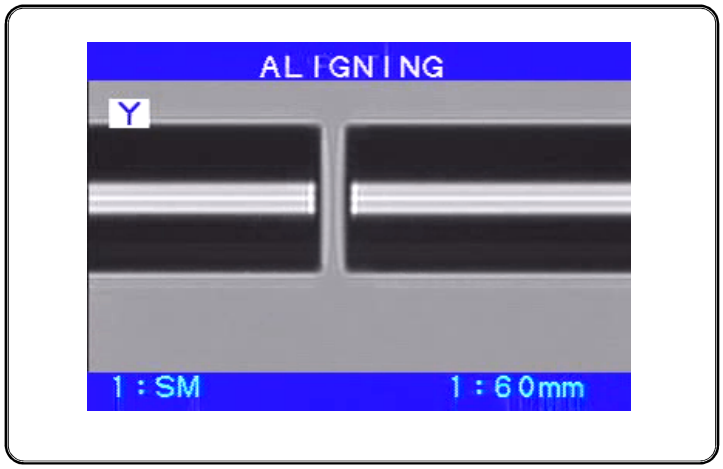


Ilustración 3:39 Fusión de F.O. paso 6

7. Cuando está listo, la máquina emite un arco eléctrico y aplica una corriente de pre fusión por un lapso de tiempo y luego emite la corriente de fusión hasta que se complete el proceso.

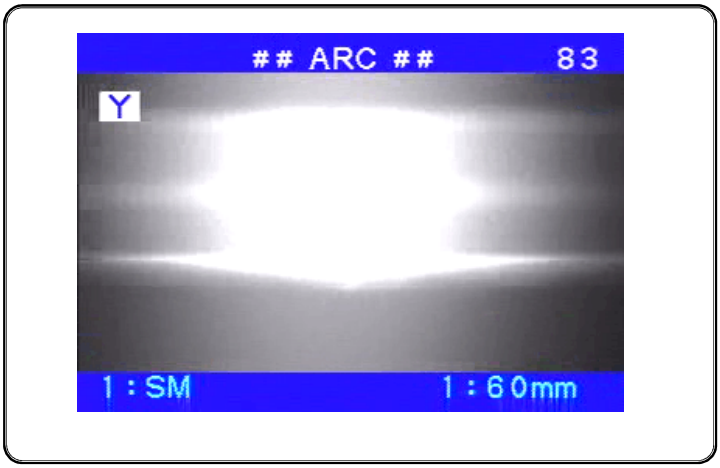


Ilustración 3:40 Fusión de F.O. paso 7

8. Una vez terminado el proceso de fusión se hace una estimación del valor de atenuación de la señal debido al empalme.

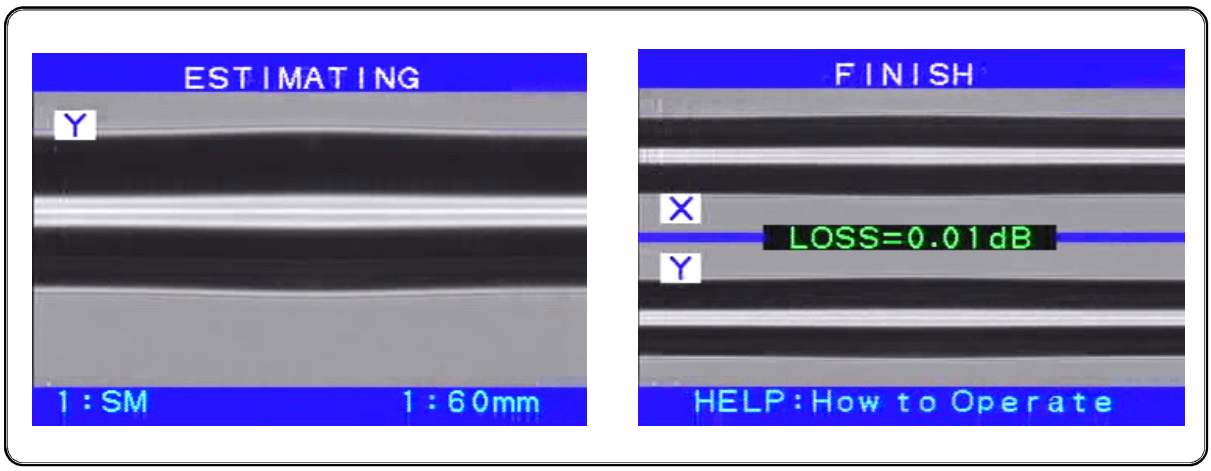


Ilustración 3:41 Fusión de F.O. paso 8

9. Por último se retira de la empalmadora la fibra ya fusionada y se le coloca un protector, un conducto de almohadilla adhesiva que generalmente viene en la caja de empalme.

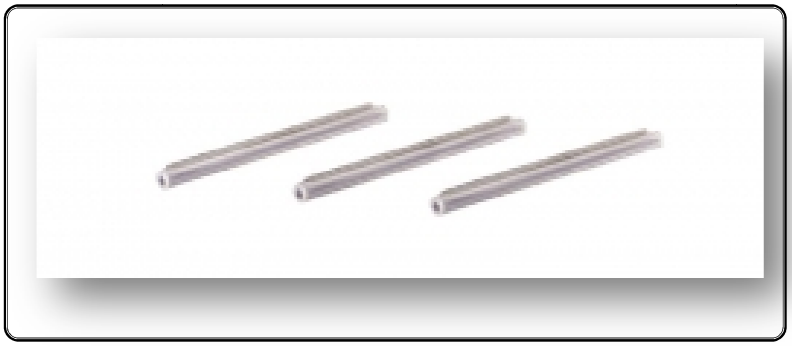


Ilustración 3:42 Fusión de F.O. paso 9

Con la fibra empalmada a los filamentos de la caja, se procede a organizar las fibras en la caja de empalme procurando no doblar los filamentos que son sumamente delicados, la fibra ordenada dentro de la caja debe quedar de la siguiente manera:

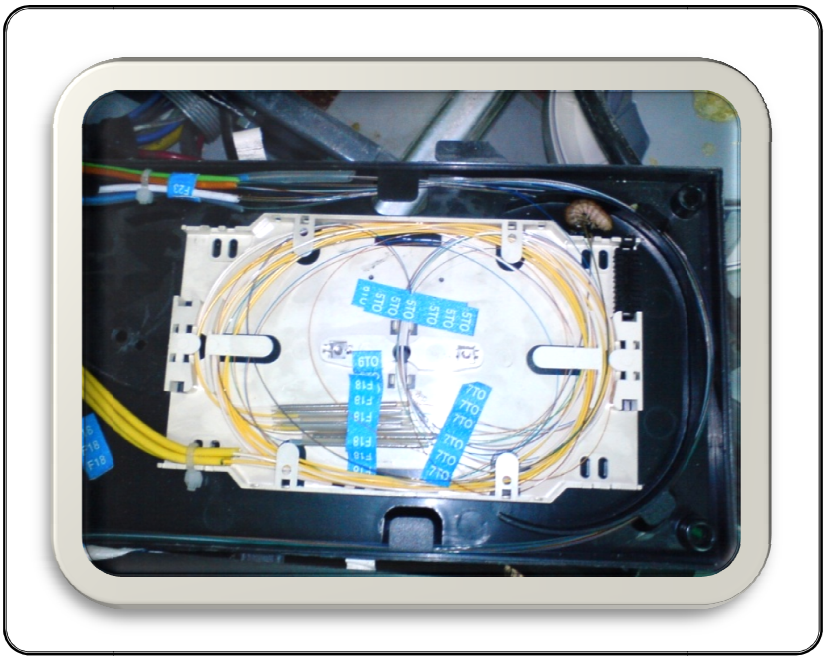


Ilustración 3:43 Caja de empalme con Fibra Óptica

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

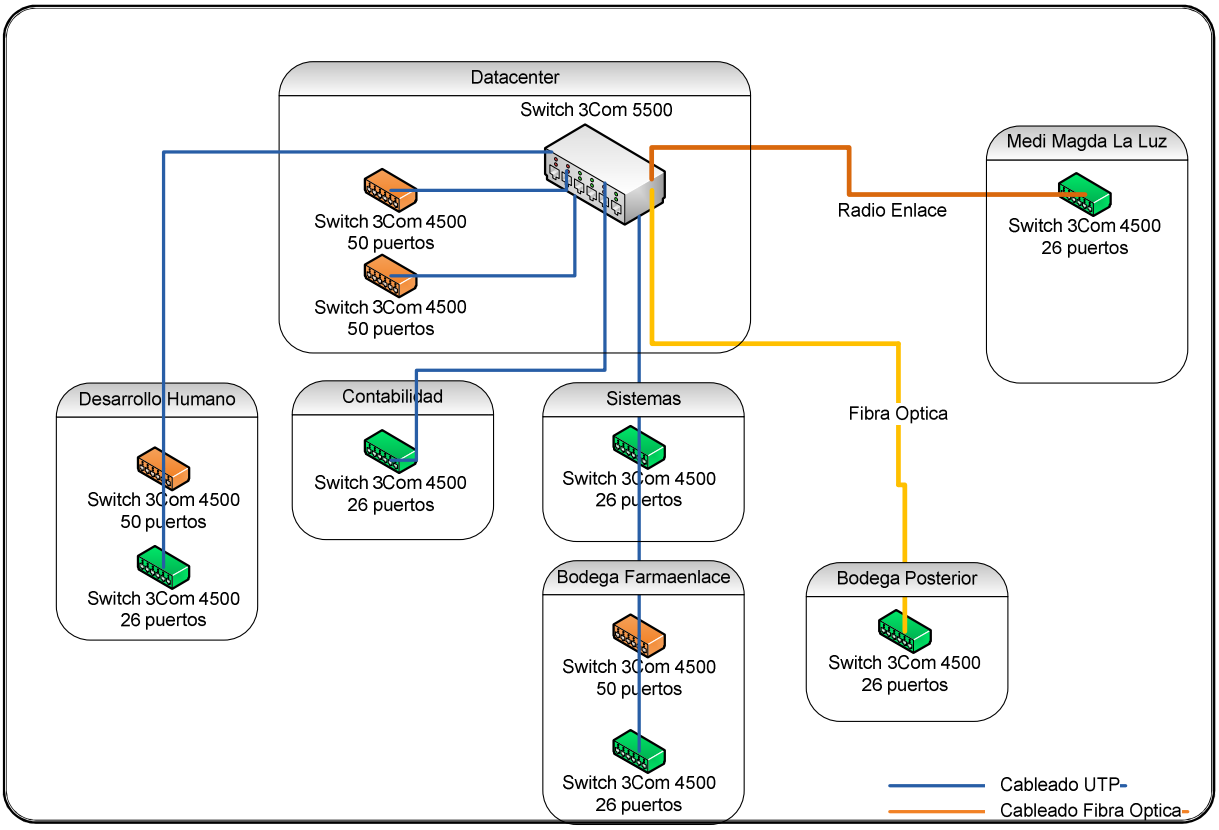


Ilustración 3:44 Distribución de Switches por Áreas

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 de Farmaenlace.

Cada uno de estos switch posee un par de aditamentos metálicos para su instalación en el rack

Ilustración 3:45 Soporte de switch para 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

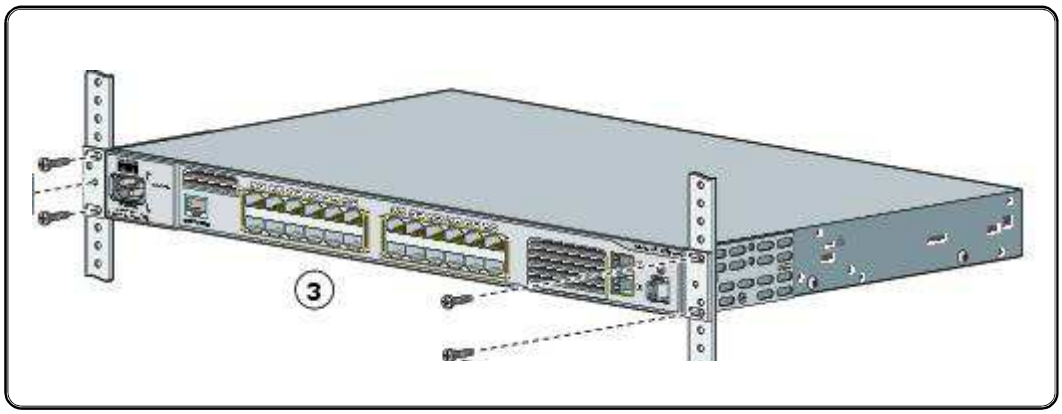


Ilustración 3:46 Instalación de Switch en Rack

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.

Ilustración 3:47 Cable de consola para administracion de switch

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.

Ilustración 3:48 Adaptador Serial - USB para cable de consola

Una vez conectado el dispositivo al computador, se procede a acceder a la información del equipo por medio de HyperTerminal. Para poder establecer comunicación con Hyperterminal se debe colocar la siguiente información:

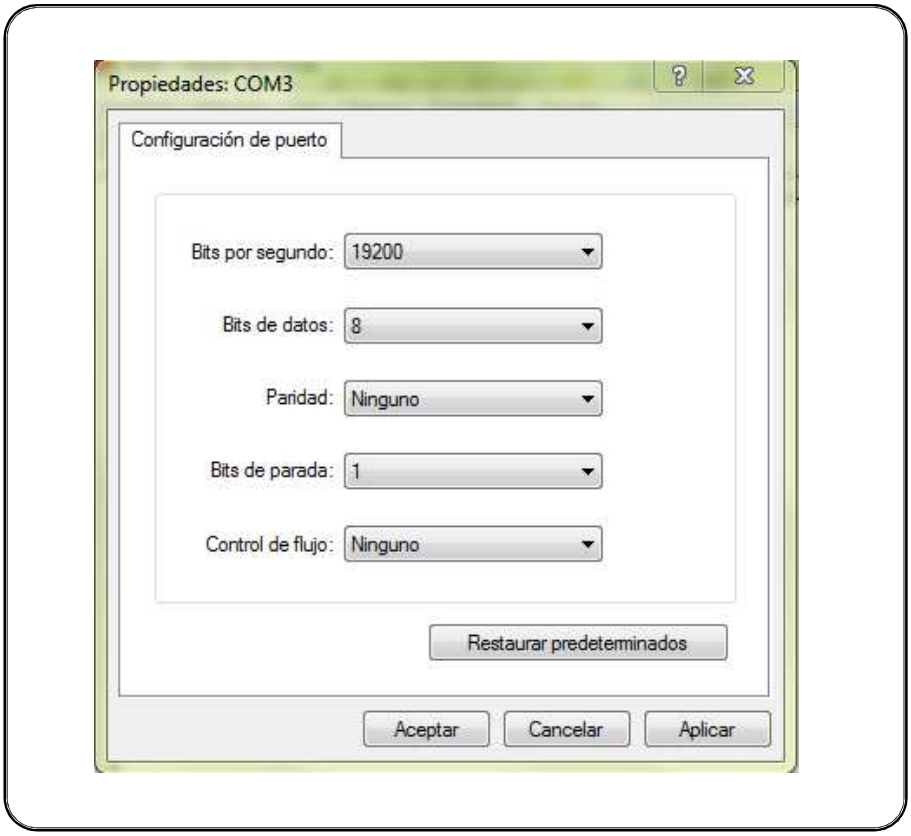


Ilustración 3:49 Configuración Hyperterminal para switches 3COM

Para configurar la infraestructura de switches de acuerdo a las necesidades de la empresa se deben utilizar comandos específicos que se usan en el lenguaje de los switches 3Com.

La configuración completa de los switches se encuentra detallada en el anexo B.

Los comandos usados son:

Sysname ***nombre del dispositivo***: comando utilizado para cambiar el nombre informativo del dispositivo.

Vlan ***número***: comando para agregar una vlan ej.: vlan 2, vlan 3. Por defecto el switch tiene configurada la Vlan 1 como principal.

Interface ***nombre de la interface***: comando para acceder a la configuración especifica de una interfaz del switch, sea una vlan o un puerto de red del dispositivo.

Description ***nombre de la interfaz***: comando para agregar un nombre a la interface que describa su propósito.

Ip address *dirección ip mascara de red*: comando para agregar una dirección ip a una interfaz, ej.: ip addres 192.168.101.253 255.255.255.0

Rip versión 2 multicast: habilitación de la interfaz para soportar protocolo de ruteo RIP versión 2.

Ejemplo completo de configuración de VLAN:
Vlan 2
Interface Vlan-interface2
description RED TELEFONIA
ip address 192.168.110.1 255.255.255.0
rip version 2 multicast

Para configuración de los puertos se utilizan los siguientes comandos.

Stp edged-port enable: habilita a los puertos para entrar en modo de transmisión más rápido cuando se reinicia el equipo o se levanta el puerto.

Port link-type trunk: comando para configurar el puerto para que permita la transmisión de datos originados en distintas VLANs.

Port trunk permit vlan número de vlan o all: comando para permitir el paso de los datos de la vlan especificando que vlan se requiere o todas.

Port link-type hybrid: comando para configuración de puertos híbridos, que permiten la transmisión de datos pertenecientes a ciertas VLANs con y sin TAG (etiqueta), de acuerdo a como se configure. El TAG es una identificación adicional que se añade a los paquetes para su asociación a una VLAN específica, cuando se recibe paquetes sin tag (untagged) se les asignan a la VLAN por defecto.

Port Hybrid vlan *número vlan to número vlan [tagged / untagged]:* complementa la configuración del comando anterior para establecer que VLANs serán agregadas etiqueta de identificación y que VLANs no lo harán.

Ej: port hybrid vlan 1 to 2 tagged port hybrid vlan 3 untagged.

Broadcast-suppression pps 3000: establece la cantidad de paquetes por segundo (pps) que el switch limitara en caso de haber trafico excesivo de broadcast.

Undo jumboframe enable: restringe el paso de paquetes de gran tamaño y limita la fragmentación/desfragmentación inesperada de paquetes.

Apply qos-profile default: aplica la configuración de calidad de servicio en modo default con las configuraciones originales.

Speed valor: comando para establecer la velocidad de transmisión por defecto en MegaBits por segundo (Mbps). Ej: speed 10

Ejemplo de configuración de puerto de red:

```
interface GigabitEthernet1/0/1

stp edged-port enable

port link-type trunk
port trunk permit vlan all
broadcast-suppression pps 3000
undo jumboframe enable
apply qos-profile default

interface GigabitEthernet1/0/23

stp edged-port enable
duplex full
speed 10
port link-type hybrid
port hybrid vlan 1 to 2 tagged
port hybrid vlan 3 untagged
broadcast-suppression pps 3000
port isolate
description chasis remoto
apply qos-profile default
```

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 (TIA-942, 2005), 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 distribución de los racks en toda el área del DataCenter, se reemplaza dos racks de torre en 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.

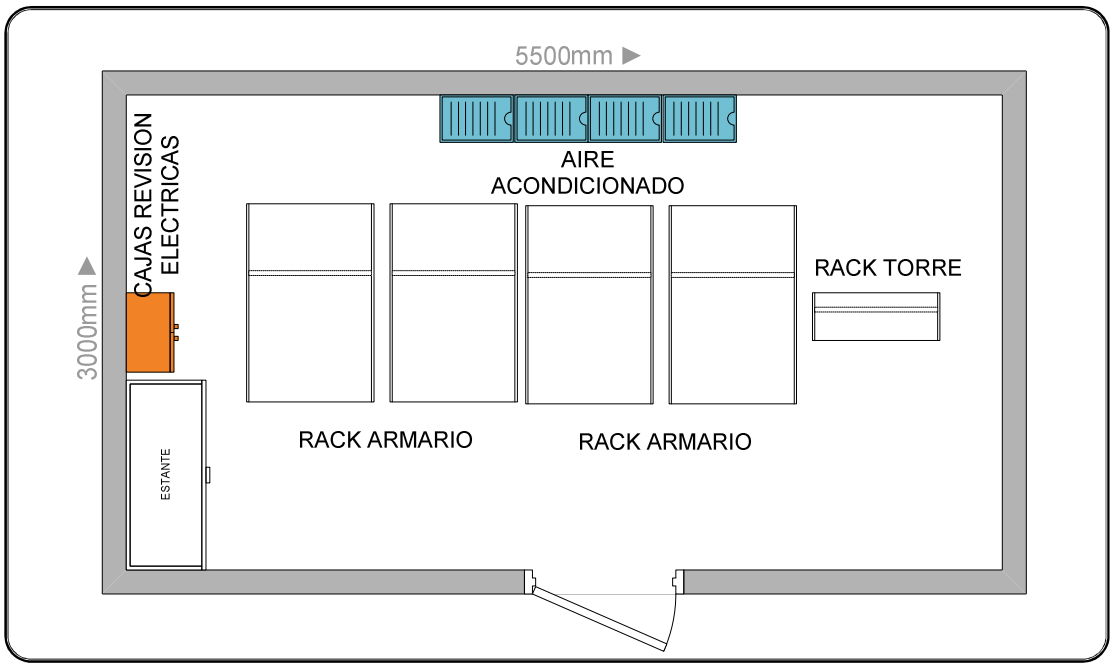


Ilustración 3:50 Diagrama de Distribución de DataCenter

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 enlaces de datos con sucursales y empresas prestadoras de servicios. En el rack 3 se encuentra un 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 administración de los equipos restantes del rack 4 y los equipos del rack 5.

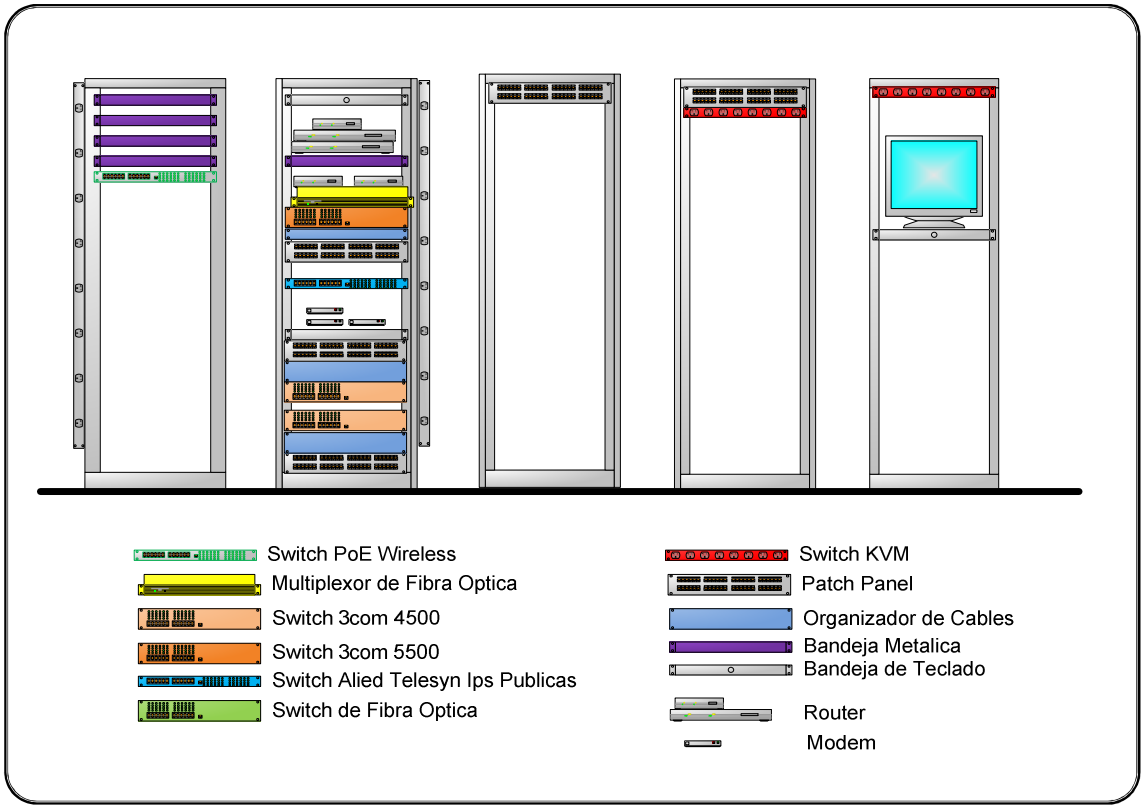


Ilustración 3:51 Ubicación de equipos de comunicaciones en DataCenter

EQUIPO	MARCA	PROPOSITO
Switch 26 puertos	3Com 5500i	Switch Core
Switch 50 Puertos	3Com 4500	Switch adicional Servidores
Switch 24 puertos	Allied Telesyn	Switch de IPs Públicas
Switch 50 puertos	3Com 4500	Red LAN
Switch 50 puertos	3Com 4500	Red LAN
Switch 25 puertos	3Com 4226	Red LAN Servidores
Router	Cisco 1800	Enlaces de datos con sucursales
Router	Cisco 2600	Internet canal principal y enlace Broadnet

Router	Cisco 2600	Enlaces Backup
Router	Cisco 800	Enlace con Empresa Salud S.A.
Router	Cisco 800	Enlace Datafast
Router	Wawuei AR18-21	Enlace Medianet
Modem	GPRS	Enlace Backup Medianet
Network Terminal	TellLabs 8110	Enlace Datafast
Modem	Zhone	ADSL Medianet
Multiplexor Fibra	Raisecom RCM 52801	Enlaces de datos con sucursales y E1 de voz

Tabla 3:1 Listado de dispositivos de Red en DataCenter Farmaenlace

De los dispositivos enumerados en la lista anterior, los que corresponden a routers y módems son para servicios de conexión con sucursales de Farmaenlace como farmacias, supermercados y oficinas remotas, así como también para servicios específicos provistos por empresas como managers de tarjetas de crédito, recargas celulares y servicios de crédito corporativo con instituciones clientes.

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 y de las sucursales de Farmaenlace, se han retirado algunos equipos por ser muy antiguos y se han reemplazado por nuevos equipos, mismos que fueron detallados en el numeral 4.2 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.

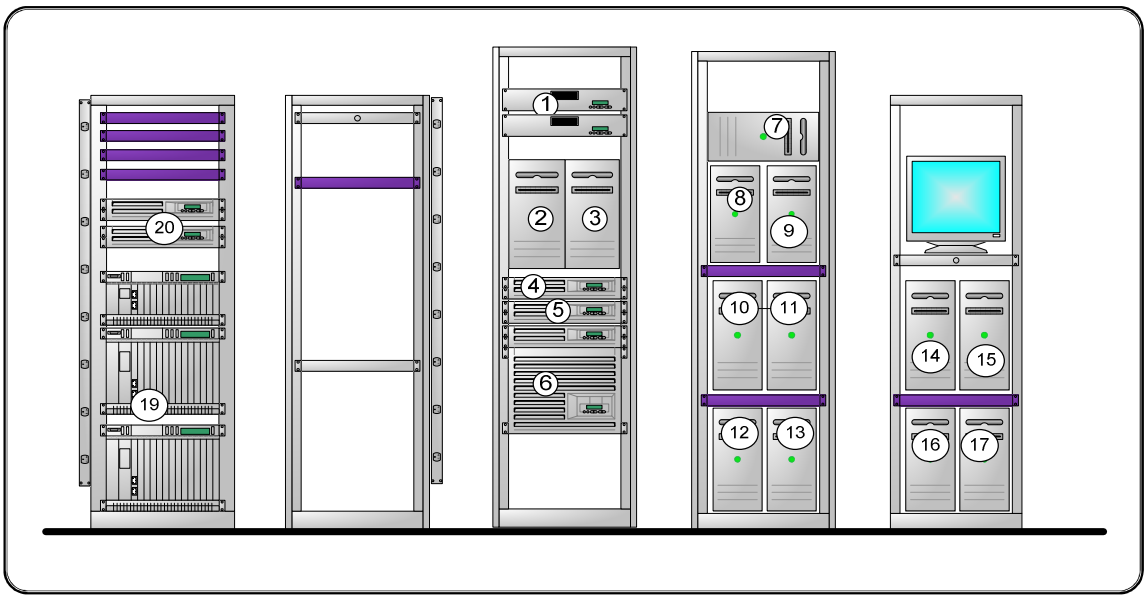


Ilustración 3:52 Distribución de Servidores en DataCenter Farmaenlace

No	MODELO	NOMBRE	DIR. IP 192.168.238	CPU	DISCO	RAM	SIST. OPERAT.
1	HP EVA 4400	Storage	123		2TB		
2	HP Proliant ML370 G5	EasyGestion Aplicaciones	158	Intel Xeon Dual Core 2.33Ghz	C:20Gb E:117Gb	8Gb	Windows 2003 Enterprise
3	HP Proliant ML370 G5	Programas de Logística y Bodega	25	Intel Xeon Dual Core 2.33Ghz	C: 273Gb	8Gb	Windows 2003 Enterprise
4	HP Proliant DL380 G6	EasyGestion Base Datos	159	Intel Xeon Cuad Core 2.67Ghz	C:140Gb D:800Gb Fc E:1.11Tb St	16Gb	Windows 2008 Standard
5	HP Proliant DL380 G5	Lisa Farmaenlace Aplicaciones BaseDatos	5	Intel Xeon Dual Core 3.00Ghz	C:140Gb D:700Gb	8Gb	Windows 2003 Enterprise
6	Enclosure Blade System HP C3000	Chasis de servidores Blade					
6.1	HP BL480c	Lisa Magda Aplicaciones	2	Intel Xeon Dual Core 2.66Ghz	C:50Gb D:140Gb	8Gb	Windows 2003 Enterprise
6.2	HP BL480c	Aplicaciones Desarrollo	19	Intel Xeon Dual Core	C:50Gb E:361Gb	8Gb	Windows 2003

		Humano		2.66Ghz			Enterprise
6.3	HP BL460c G6	Aplicaciones Web 2	6	Intel Xeon Dual Core 2.27Ghz	C:100Gb	8Gb	Windows 2003 Enterprise
6.4	HP BL460c	Domain Controller Farmaenlace.com	1	Intel Xeon Dual Core 2.50Ghz	C:140Gb	4Gb	Windows 2003 Enterprise
6.5	HP BL460c G6	Bussines Intelligence Qlick View	26	Intel Xeon Dual Core 2.53Ghz	C:100Gb D:181Gb	64Gb	Windows 2008 Standard
6.5	HP BL460c G7	Active Directory Backup, Srv tarjetas	2	Intel Xeon Dual Core 2.53Ghz	C:50Gb D:87Gb	6Gb	Windows 2008 Standard
7	Clon	Linux Correo Electrónico	251	Intel Core 2 Duo 2.66Ghz	160Gb	2Gb	Linux Centos 5.3
8	Clon	Linux Navegación y Firewall	254	Intel Core 2 Duo 2.66Ghz	160 Gb	2Gb	Linux Centos 5.3
9	Clon	Activos Fijos ECAF	22	Intel Core 2 Cuad 2.66Ghz	C: 100Gb D:360Gb	3Gb	Windows Xp
10	Clon	Cubos Magda	7	Intel Pentium 4 3.4Ghz	C:149Gb D:149Gb	2Gb	Windows 2003 Enterprise
11	HP Proliant ML150	Servicios Datafast y Broadnet	8	Intel Xeon Dual Core 2.00Ghz	C: 149Gb	4Gb	Windows 2003 Enterprise
12	HP Proliant ML370 G4	Aplicaciones Web 3 Base Datos Varias	34	Intel Xeon Dual Core 3.40Ghz	C:140Gb	4Gb	Windows 2003 Enterprise
13	HP Proliant ML370 G4	Pruebas nuevos proyectos	3	Intel Xeon Dual Core 3.40Ghz	C: 240Gb	5Gb	Linux Debian 4
14	Clon	TINI 100	24	Intel Core 2 Duo 2.66Ghz	C: 90Gb D:24Gb	2Gb	Windows XP
15	Clon	SrvMedianet	23	Intel Core 2 Duo	C:100Gb	2Gb	Windows 2003

				2.80Ghz			Enterpise
16	Clon	TINI 99	4	Intel Core 2 Duo 2.80Ghz	C:100Gb	2Gb	Windows 2003 Enterprise
17	Clon	Taller Easyfarma	35	Intel Core 2 Duo 2.80Ghz	C:100 Gb D:1Tb	4Gb	Windows 2003 Enterprise

Tabla 3:2 Listado de equipos servidores en DataCenter Farmaenlace

3.6 Documentación de Red

Es necesario detallar el estado final en que queda la red de Farmaenlace 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 bodegas de Farmaenlace; y red WAN abarcando los enlaces con sucursales y oficinas remotas además de enlaces con proveedores de servicios.

3.6.1 Red LAN

La red interna de Farmaenlace 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 de Farmaenlace 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. Esta red era la que Farmaenlace mantenía y por decisión de la gerencia de sistemas se mantiene, debido al incremento de equipos tanto servidores como equipos de usuario, la cantidad soportada por esta red fue superada. Para solucionar este inconveniente y aumentar el número de equipos soportados por la red se decide migrar a una red 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. La red clase B se destina a todos los equipos cliente de los

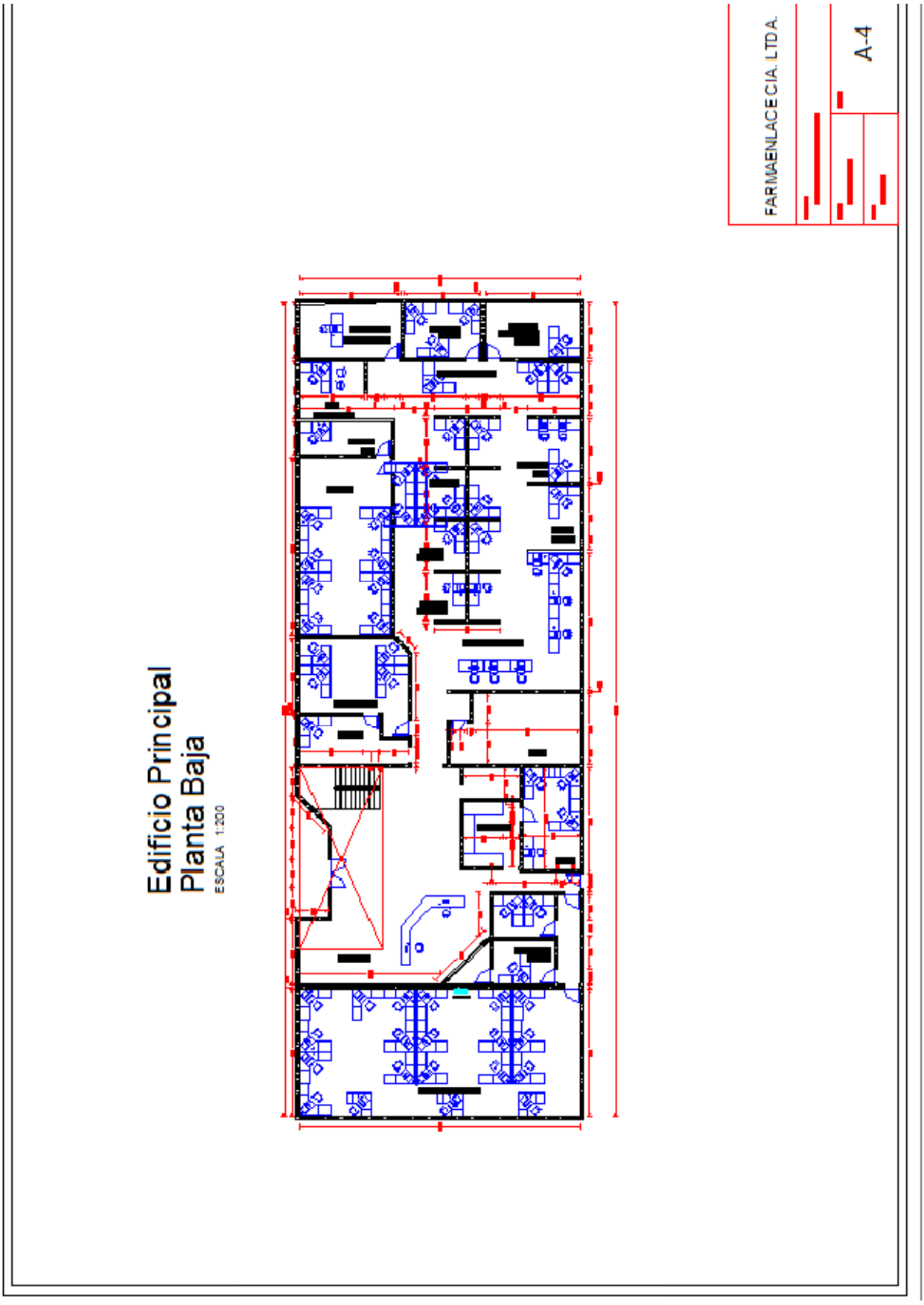
usuarios en todo el edificio matriz segmentando administrativamente la red de la siguiente manera:

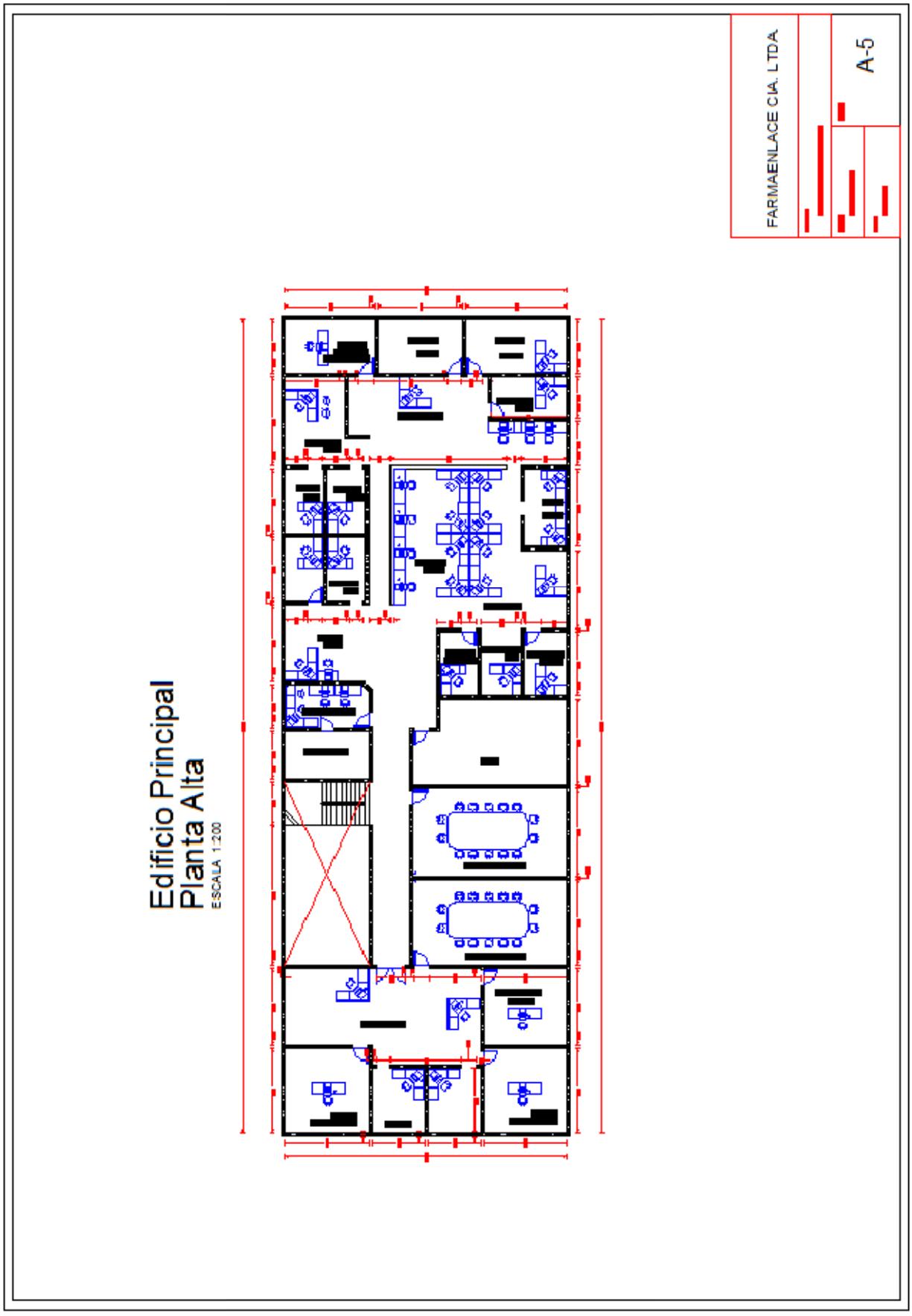
1. 172.30.1.1 hasta 172.30.1.255 equipos con acceso ilimitado a internet.
2. 172.30.2.1 hasta 172.30.2.255 equipos con acceso limitado a internet y uso de aplicaciones reservadas.
3. 172.30.3.1 hasta 172.30.3.255 equipos sin acceso a internet.

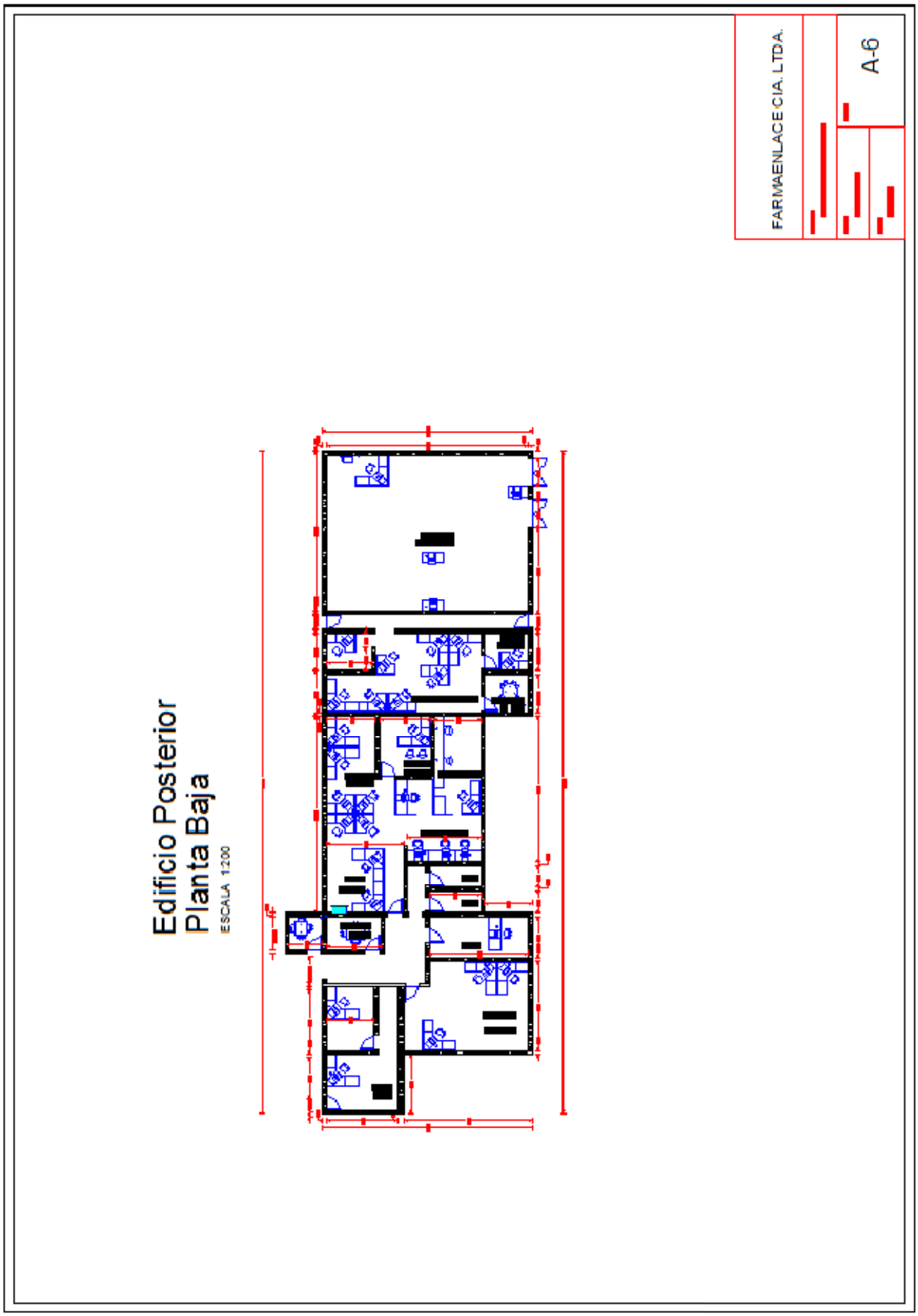
b) La VLAN No. 2 soporta todo el servicio de telefonía IP tanto el edificio matriz como en sucursales, a esta red se le asigna la dirección IP clase C 192.168.110.0/24.

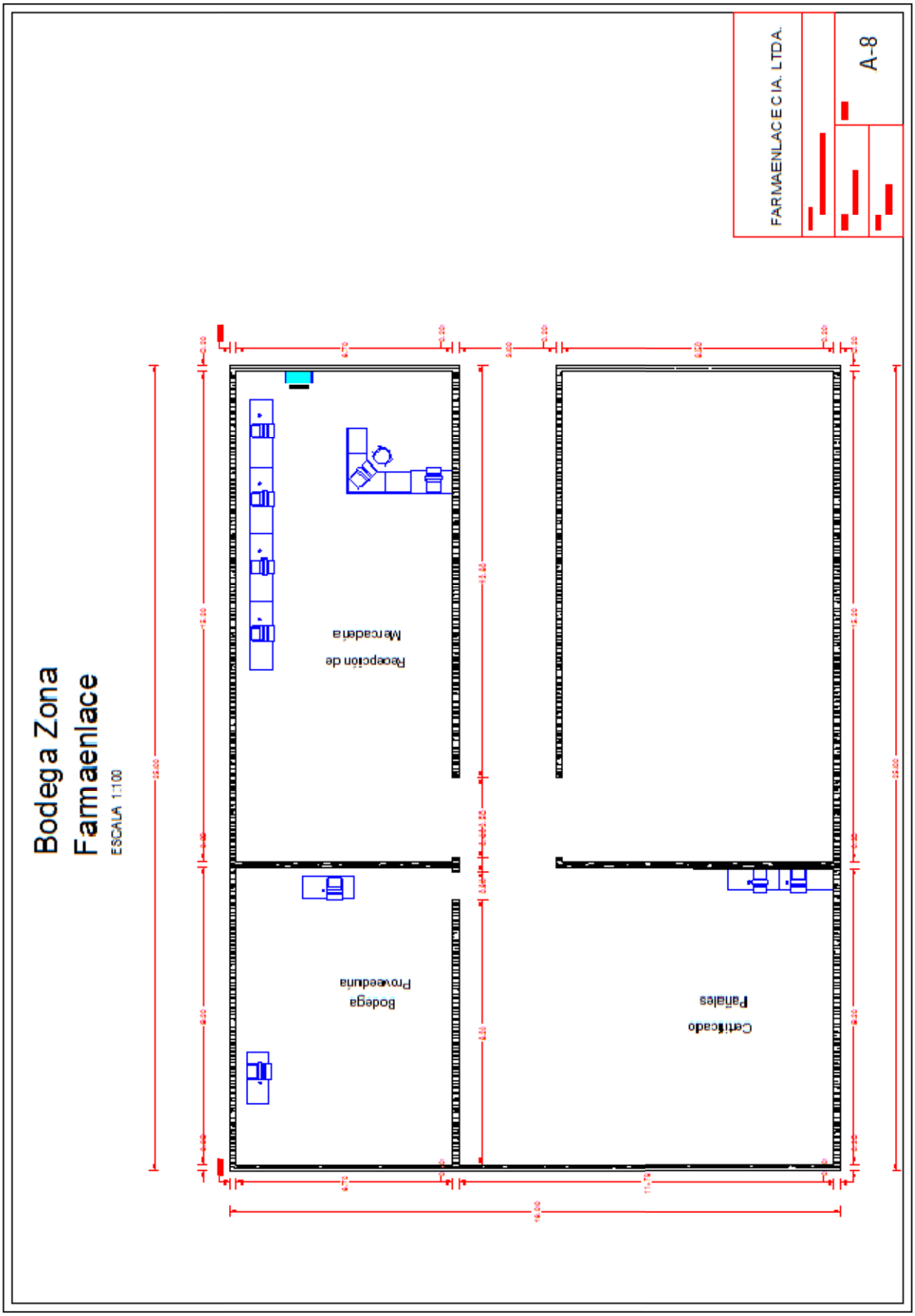
c) La VLAN No. 3 se encuentra asignada para soportar el tráfico de datos con toda el área correspondiente a Farmacia Medicity Magda La Luz. Se mantiene la dirección de red clase C192.168.101.0/24.

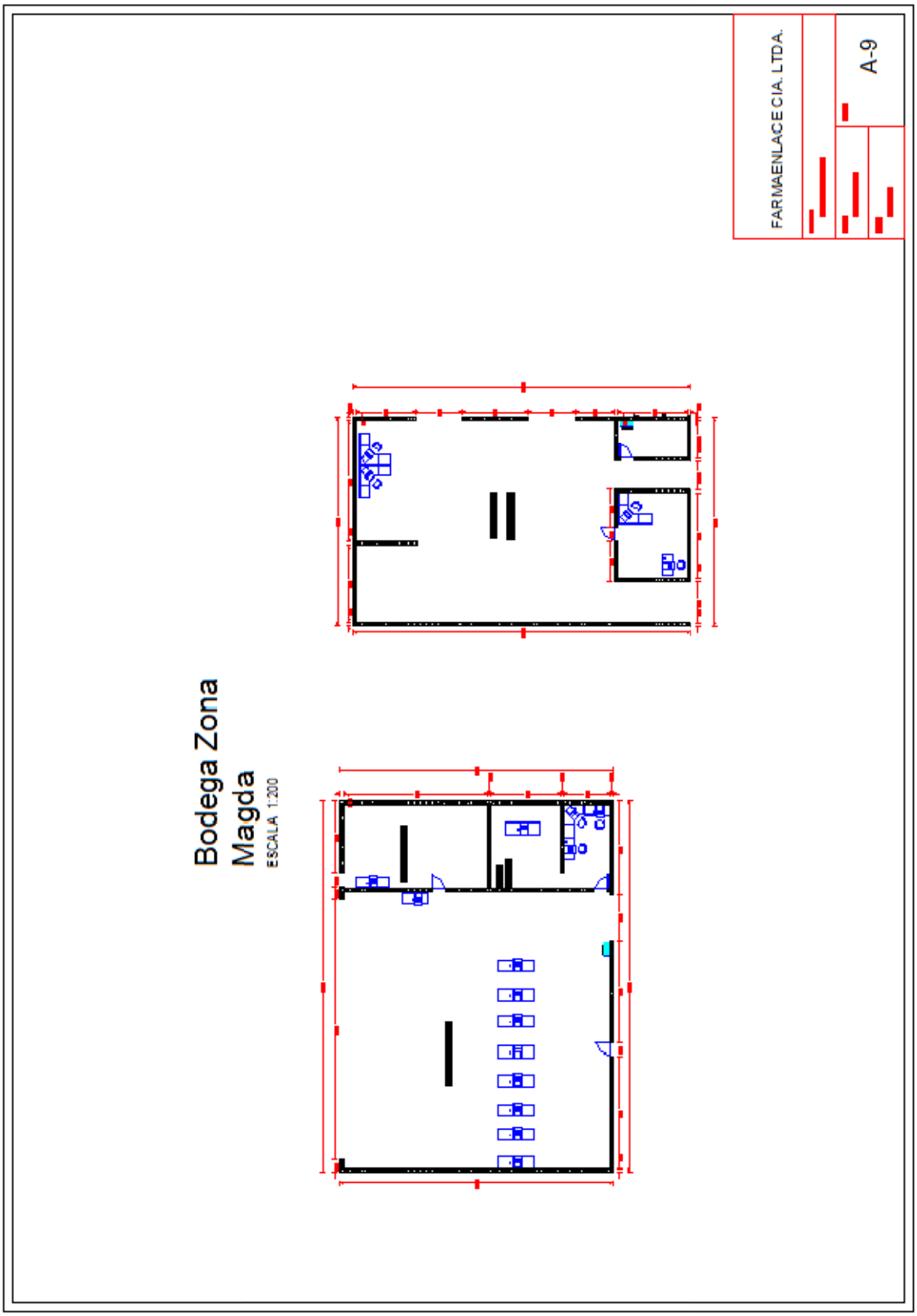
3.6.1.1 Diagramas de ubicación de puntos de red del cableado estructurado


FARMAENLACE CIA. LTDA.
A-4
Edificio Principal
Planta Baja
ESCALA 1:200


FARMAENLACE CIA. LTDA.
A-5
Edificio Principal
Planta Alta
ESCALA 1:200


FARMAENLACE CIA. LTDA.
A-6
Edificio Posterior
Planta Baja
ESCALA 1:200


FARMAENLACE C IA. LTDA.
A-8
Bodega Zona
Famaenlace
ESCALA 1:100
Recepción de
Mercadería
Bodega
Proveeduría
Certificado
Fármacos


FARMAENLACE CIA. LTDA.
A-9
Bodega Zona
Magda
ESCALA 1:200

3.6.2 Red WAN

La red WAN de Farmaenlace Cía. Ltda. es una estrella de enlaces que tiene como punto central a las oficinas de Farmaenlace Matriz en la ciudad de Quito, 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 provisto por la Corporación Nacional de Telecomunicaciones CNT, por fibra óptica y radio enlace provisto por las empresas Global Crossing, Telconet y Powerfast, tres locales por su nivel de transaccionalidad y servicios poseen enlaces de 1Mbps.

El listado de enlaces de datos de Farmaenlace Cía. Ltda. se presenta en el anexo D.

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 de CNT 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 de Farmaenlace.

Además de los enlaces de datos con las sucursales farmacias o supermercados, también se encuentran instalados enlaces de datos de proveedores de servicios adicionales que complementan el negocio de Farmaenlace como por ejemplo Datafast y Medianet quienes permiten el pago con tarjeta de crédito, un enlace con la empresa SALUD S.A. para provisión de crédito corporativo de afiliados a este plan de medicina prepagada, un enlace de datos con la empresa EasySoft para desarrollo complementario de sistemas y uso del sistema corporativo de pagos/cobros de servicios básicos, y un enlace de datos con Zermat Internacional, una parte del corporativo Farmaenlace con oficinas independientes.

A continuación se presenta el diagrama de distribución de los enlaces de datos de la red WAN de Farmaenlace.

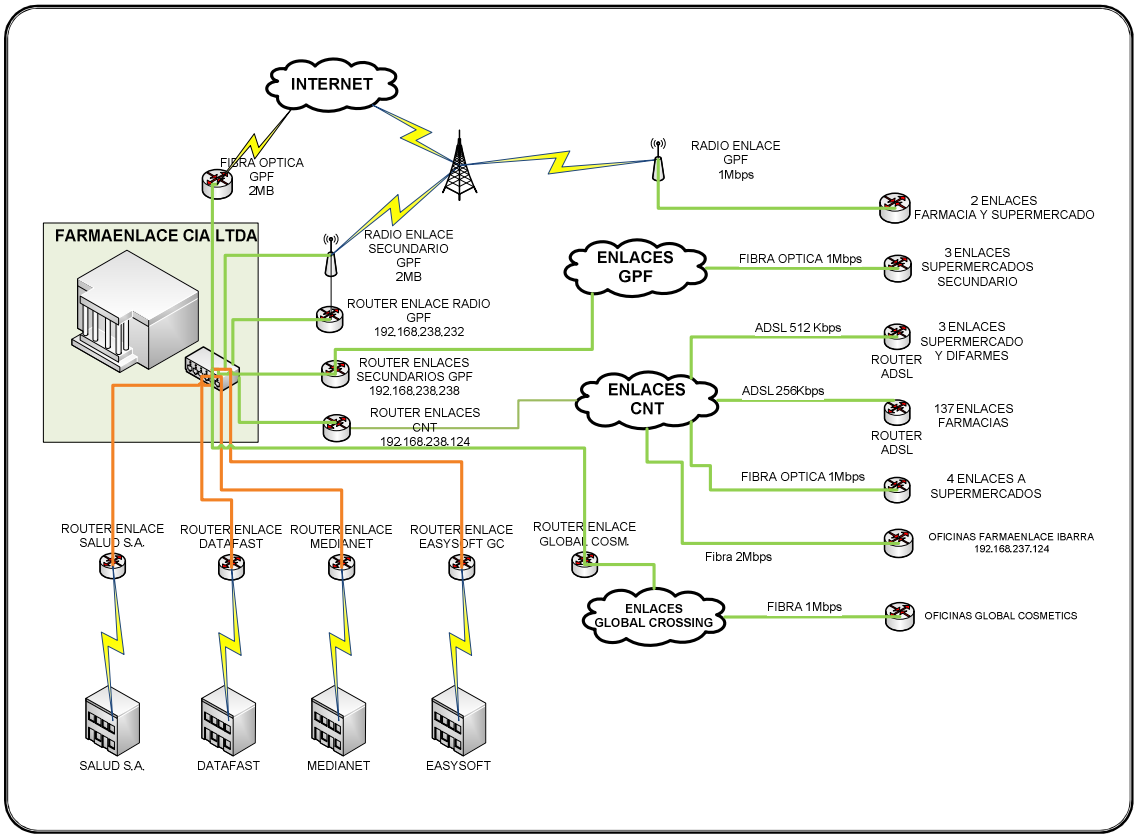


Ilustración 3:58 Diagrama de Red WAN de Farmaenlace

CAPÍTULO 4

4 IMPLEMENTACIÓN DEL PROYECTO (Servicios)

El presente capítulo se enfoca en la implementación de servicios en la empresa FARMAENLACE CIA. LTDA. luego de la reubicación y migración de equipos al nuevo DataCenter, los servicios que se deben implementar son: Active Directory para manejo de usuarios, administración de políticas de seguridad; asignación automática de direcciones de red mediante un servicio DHCP, un servicio a actualización automática de Windows para todos los dispositivos con este sistema operativo; adicional parametrizar los accesos a navegación y correo.

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. En el caso de Farmaenlace es necesario configurar un servidor de Active Directory principal, un servidor secundario ubicado en Farmaenlace Matriz y adicional un servidor secundario que estará ubicado en Oficinas de Ibarra.

Se decide que el nombre del nuevo dominio será: ***farmaenlace.com***.

4.1.1 Configuración

1. Instalación de Active Directory Principal

Para la configuración del servicio de Active Directory se utilizará un servidor con sistema operativo Windows 2003 Enterprise SP2 y que cumple con los requisitos que exige la instalación de Active Directory.

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

a. Haga clic en **Inicio**, haga clic en **Ejecutar**, y escriba **dcpromo** luego presione Enter, esto invocará al asistente para la configuración de active Directory.

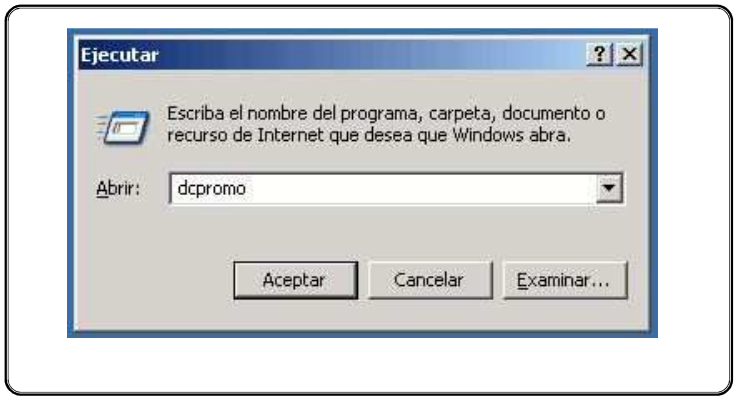


Ilustración 4:1 Configuración Active Directory 1

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 de Active Directory no está en marcha. Si cualesquiera de estas verificaciones fallan, un mensaje de error aparece y termina el asistente.

b. En la página **Bienvenida**, haga clic en **Siguiente**

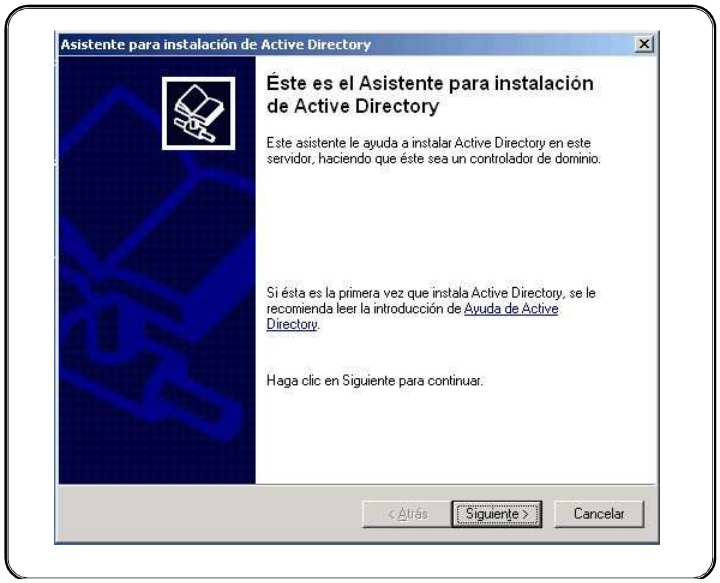


Ilustración 4:2 Configuración Active Directory 2

c. En la página **Compatibilidad de Sistema Operativo**, haga clic en **Siguiente**.

Ilustración 4:3 Configuración Active Directory 3

d. En la página **Tipo de Controlador de Dominio**, haga clic en **Controlador de Dominio para un Dominio Nuevo,** y después haga clic en **Siguiente**.

Ilustración 4:4 Configuración Active Directory 4

e. En la página **Crear Nuevo Dominio**, haga clic en **Dominio en un nuevo Bosque**, y después haga clic en **Siguiente**.

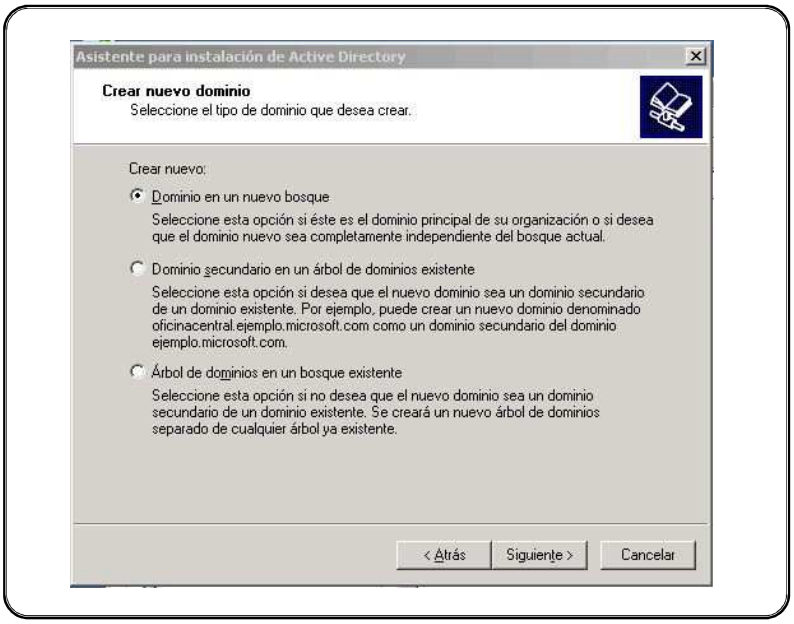


Ilustración 4:5 Configuración Active Directory 5

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

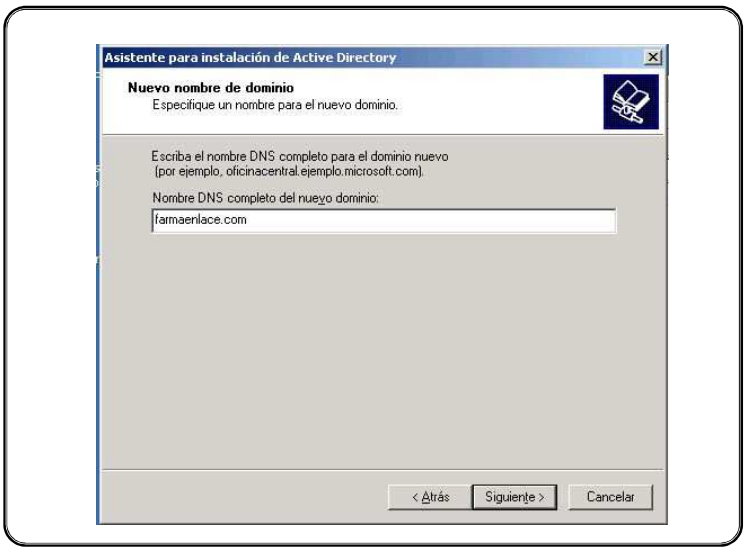


Ilustración 4:6 Configuración Active Directory 6

g. En la página **Nombre de Dominio NetBIOS**, escribir el nombre NetBIOS (FARMAENLACE) 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.

Ilustración 4:7 Configuración Active Directory 7

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**.

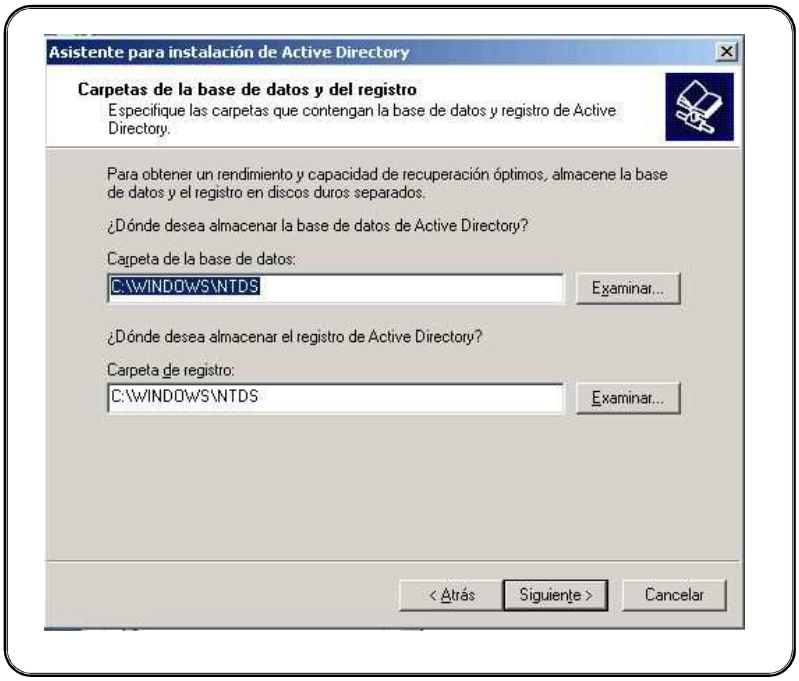


Ilustración 4:8 Configuración Active Directory 8

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**.

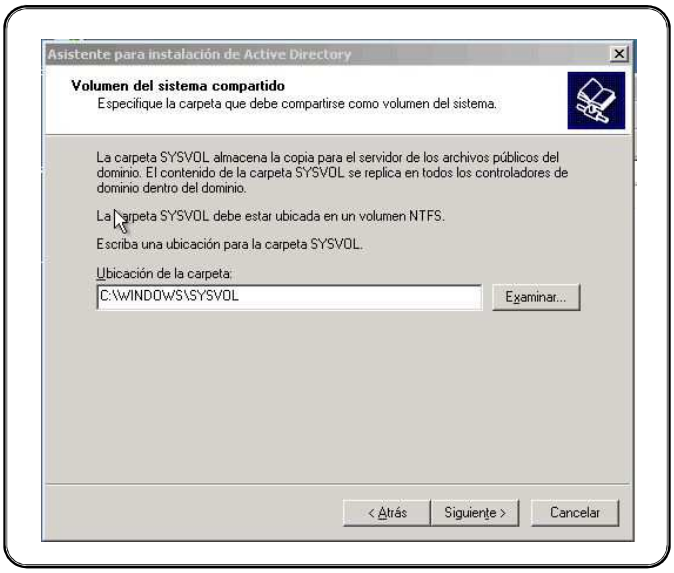


Ilustración 4:9 Configuración Active Directory 9

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**.

Ilustración 4:10 Configuración Active Directory 10

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.

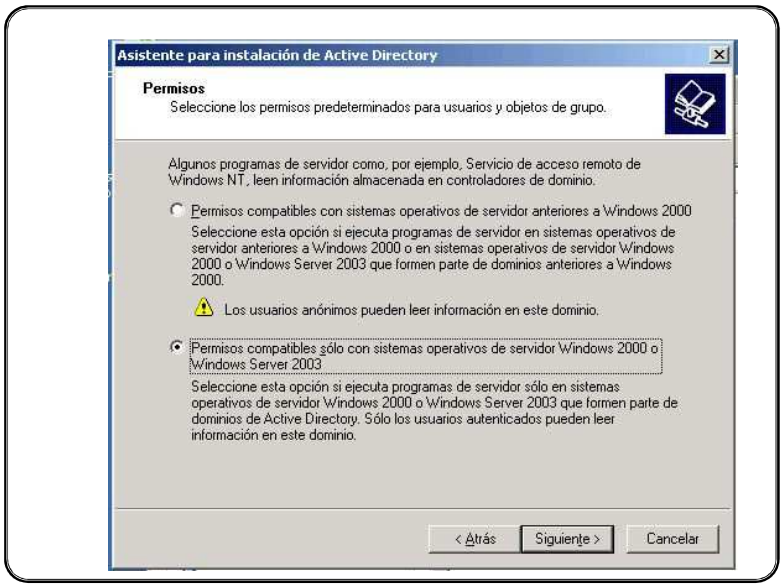


Ilustración 4:11 Configuración Active Directory 11

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.

Ilustración 4:12 Configuración Active Directory 12

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.

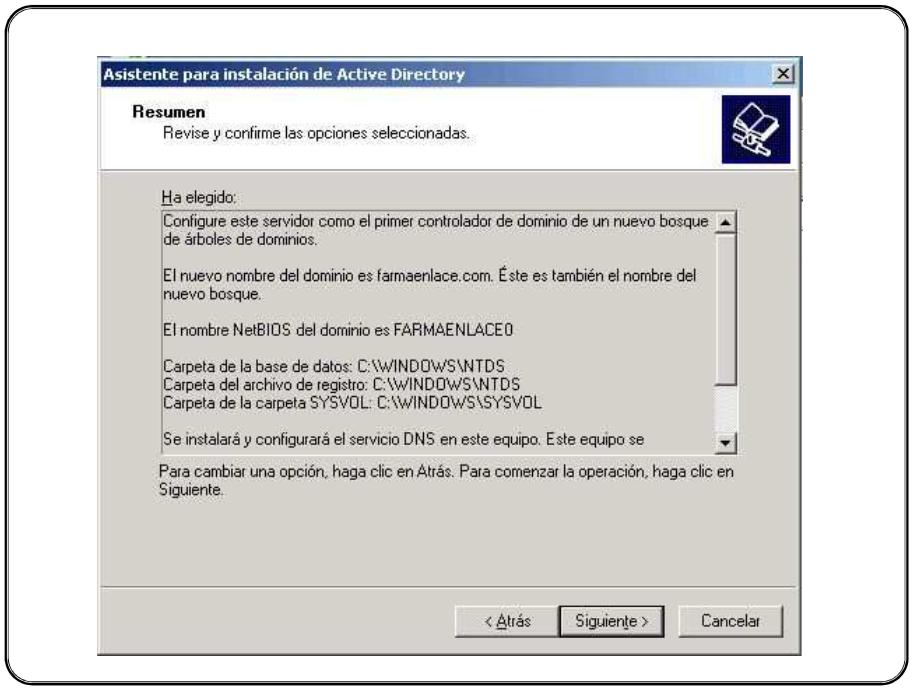


Ilustración 4:13 Configuración Active Directory 13

Si todo esta correcto haga clic en **Siguiente** para comenzar la instalación.

Ilustración 4:14 Configuración Active Directory 14

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

Ilustración 4:15 Configuración Active Directory 15

4.1.2 Configuración de un Controlador de Dominio Adicional

El procedimiento de configuración de controladores de dominio adicionales para el dominio de Farmaenlace 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.

Ilustración 4:16 Configuración servidor Active Directory Adicional

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

1. Controlador de Dominio Principal ubicado en Farmaenlace Matriz
2. Controlador secundario en Farmaenlace Matriz
3. Controlador secundario en Oficinas Ibarra

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. También se debe tomar en cuenta que las unidades organizativas son las unidades más pequeñas a las cuales se les puede asignar políticas de seguridad; mismas

que afectarán a cada uno de los elementos que se encuentren dentro de las unidades organizativas, es otro factor a considerar en el diseño de su estructura.

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.

Ingresar a la consola de administración de Usuarios y equipos de Active Directory cuyo acceso se encuentra en Herramientas Administrativas, luego de hacer clic en el botón inicio.

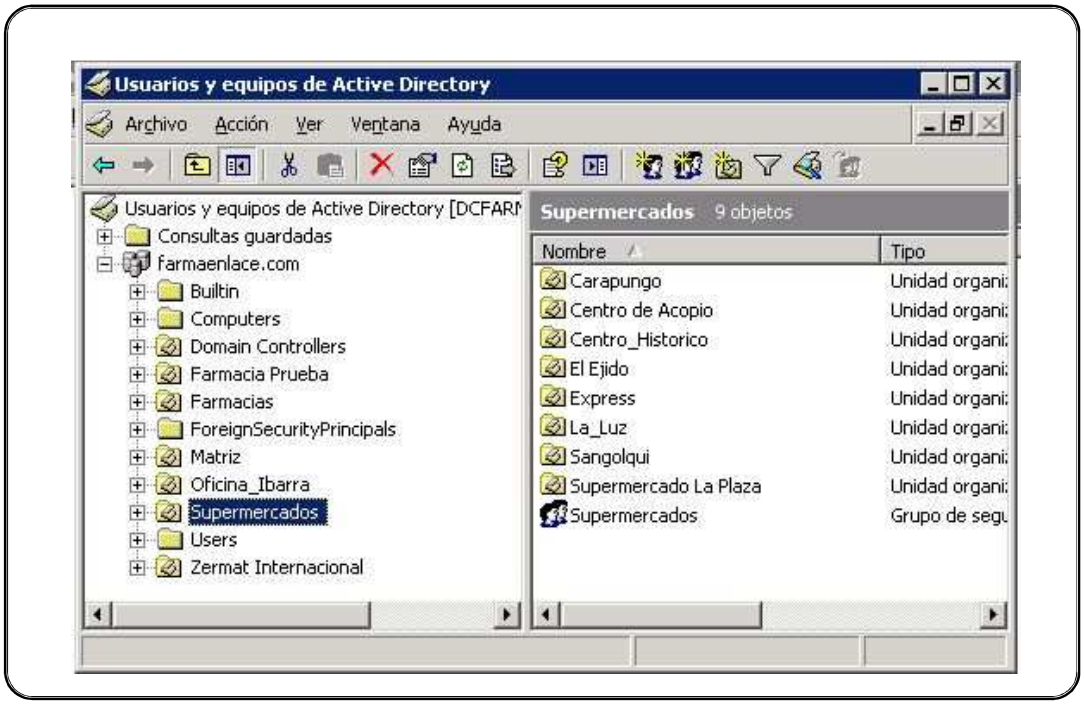


Ilustración 4:17 Configuración de Unidades Organizativas 1

Una vez abierto, se debe proceder con la creación de las unidades organizativas (OU), se puede crear haciendo clic en el ícono de creación de OU ubicado en la barra de herramientas en la parte superior de la ventana.

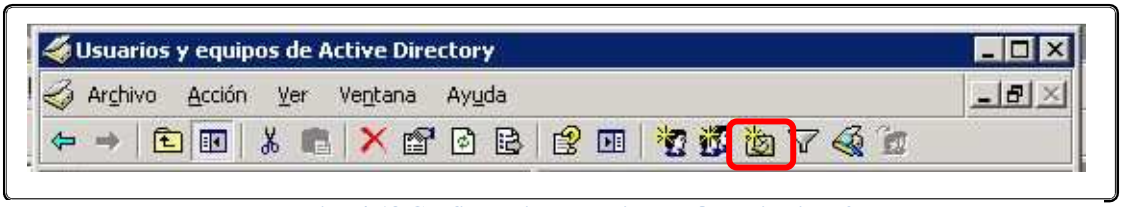


Ilustración 4:18 Configuración de Unidades Organizativas 2

Se debe tomar en cuenta que cuando se cree una nueva OU, se debe estar correctamente posicionado en el panel de navegación del costado izquierdo en la Unidad Organizativa superior dentro de la cual se creara la nueva OU, en el caso de las primeras OU que van directamente debajo de la raíz, se debe estar posicionado sobre el ícono que identifica al Domain Root.

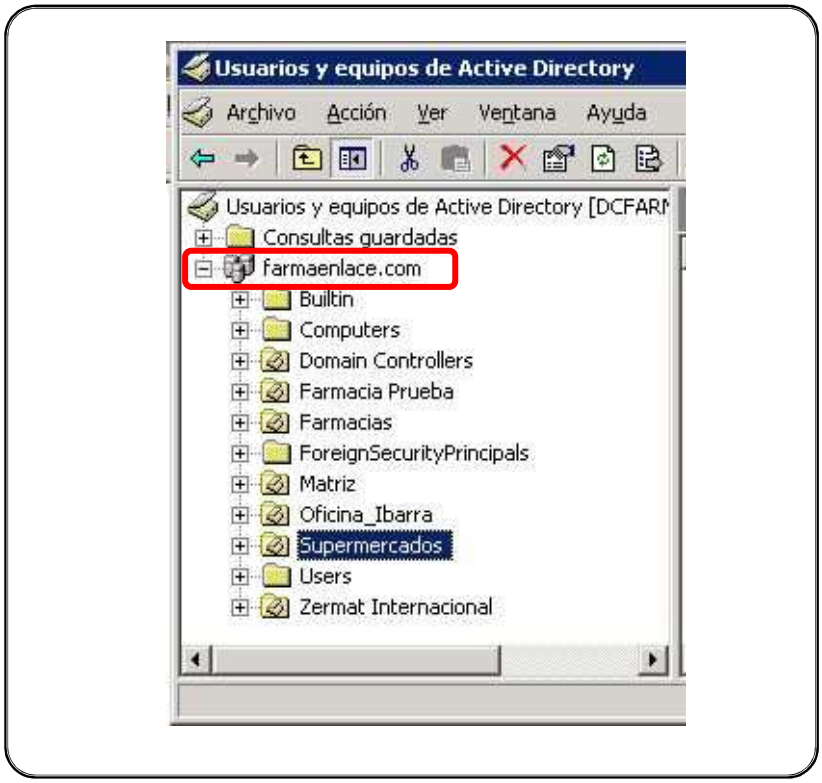


Ilustración 4:19 Configuración de Unidades Organizativas 3

Para el caso de Farmaenlace, se define la estructura de las unidades organizativas (OU) separando primeramente por oficinas, farmacias y supermercados; dentro de estas se desglosan nuevas unidades organizativas de nivel inferior como muestra el esquema a continuación:

Dominio: **Farmaenlace.com**

a. Farmacias

a) Difarmes

a: Administrativos

b: Equipos

c: Punto_Venta

b) Económicas

a: Equipos

b: Listado de farmacias Económicas

c) Medicity

a: Equipos

b: Listado de farmacias Medicity

d) PAF

a: Equipos

b: Listado de farmacias PAF

b. Matriz

a) Administrativos

a: Equipos

b: Usuarios

a. Adquisiciones y compras
b. Auditoria
c. Comercial
d. Contabilidad
e. Crédito
f. Gerencias y Vicepresidencias
g. Global
h. Infraestructura
i. Operaciones
j. Proyectos
k. RRHH
l. Seguridad
m. Serv. Generales

b) Bodega

a: Equipos

b: Usuarios

c) Call Center

a: Equipos

b: Usuarios

d) Sistemas

a: Equipos

b: Servidores

c: Usuarios

a. Usuarios Genéricos

c. Oficina Ibarra

a) Administrativos
   a: Equipos
   b: Usuarios
b) Call_Center
   a: Equipos
   b: Usuarios
c) Sistemas
   a: Equipos
   b: Usuarios

4.2 Implementación de Directivas de Grupo

4.2.1 Instalación de consola de administración de Directivas Grupo

(Holem & Thomas, 2006) dice que una directiva de grupo (Group Policy o GPO por sus siglas en ingles) permite centralizar el manejo de los usuarios y equipos computacionales de una empresa, estas políticas pueden ser aplicadas a nivel jerárquico a la organización entera todo el dominio, o a nivel de unidades organizacionales, en el momento que se aplica una GPO a una unidad organizacional (OU) todas las demás OU que se encuentren dentro de esta también serán afectadas por la GPO que se aplique.

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 Domain Controller 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.

Las GPO de computador toman precedencia sobre las GPO de usuario en caso de estar en conflicto.

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 2003, 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.

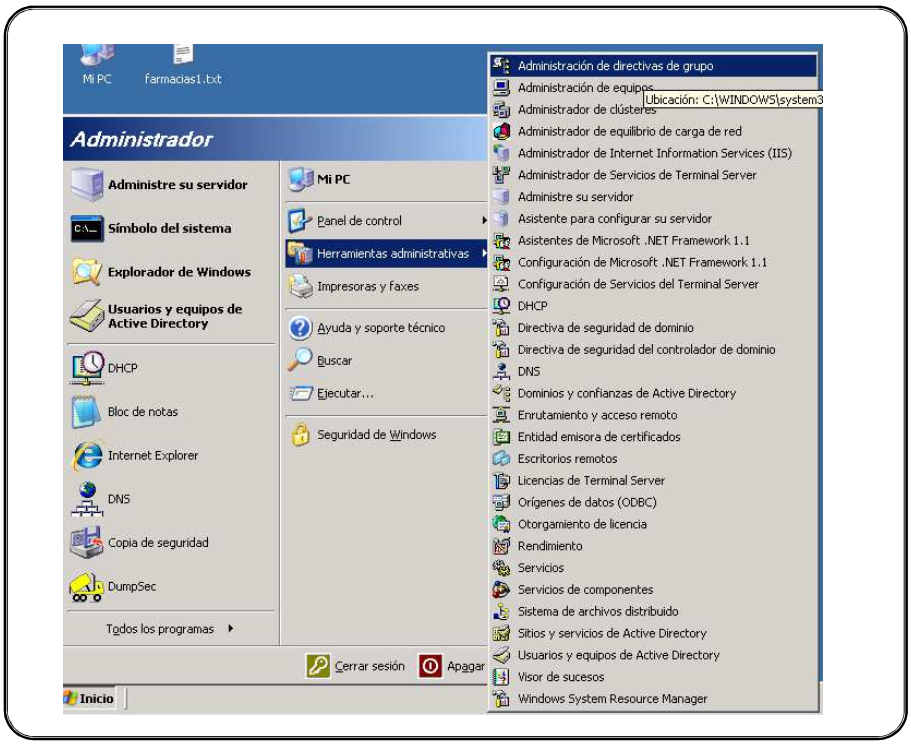


Ilustración 4:20 Configuración de Políticas de Grupo 1

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

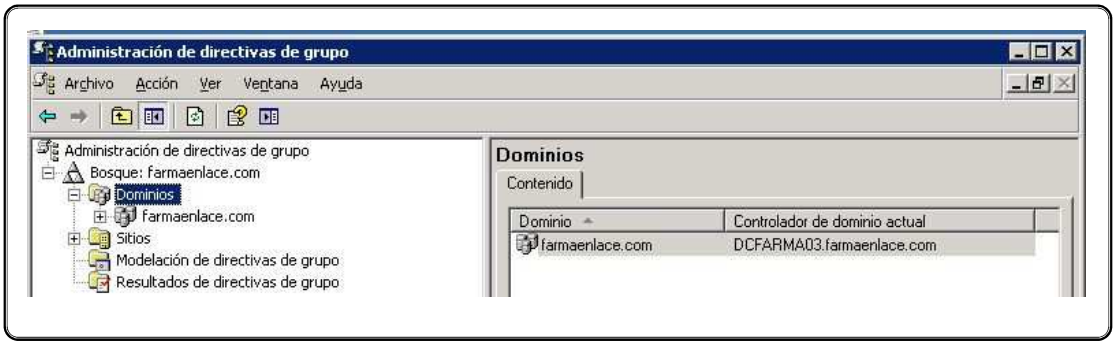


Ilustración 4:21 Configuración de Políticas de Grupo 2

Dentro del forest, se despliegan los dominios en caso de tener varios dominios configurados dentro de un mismo forest. Para el caso de Farmaenlace se mostrará un único dominio (farmaenlace.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.

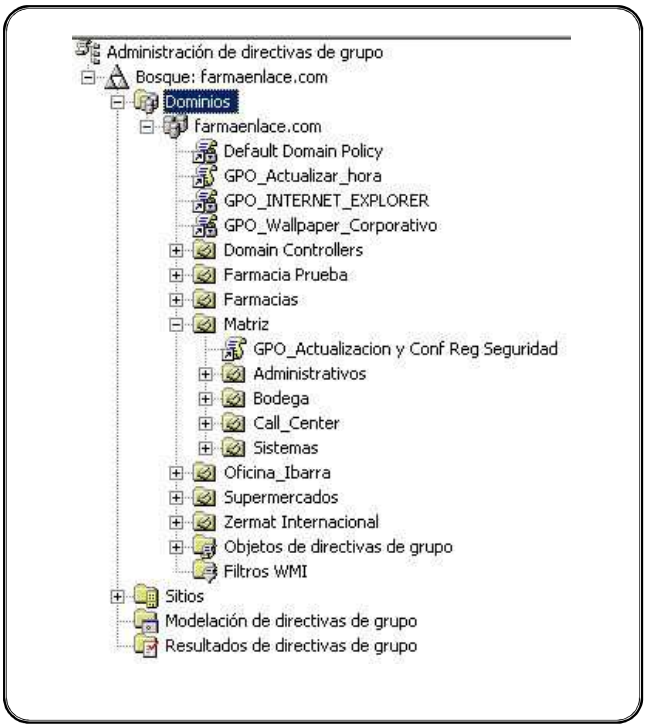


Ilustración 4:22 Configuración de Políticas de Grupo 3

Adicional se muestra un contenedor denominado objetos de directivas de grupo que despliega todas las GPO del dominio.

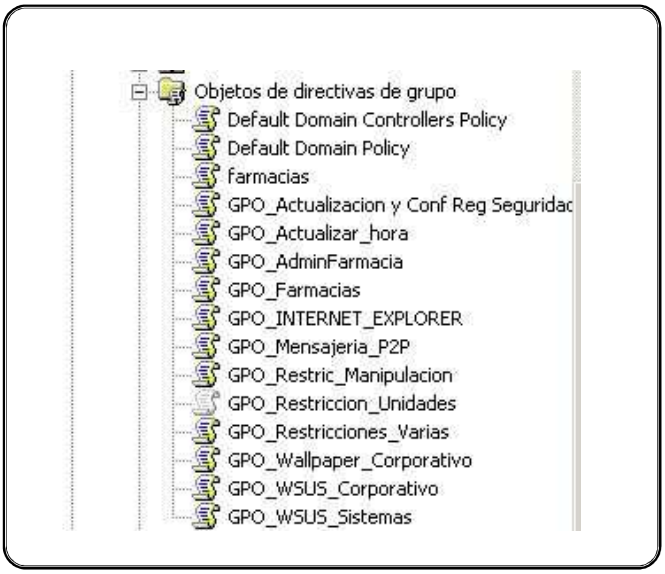


Ilustración 4:23 Configuración de Políticas de Grupo 4

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".

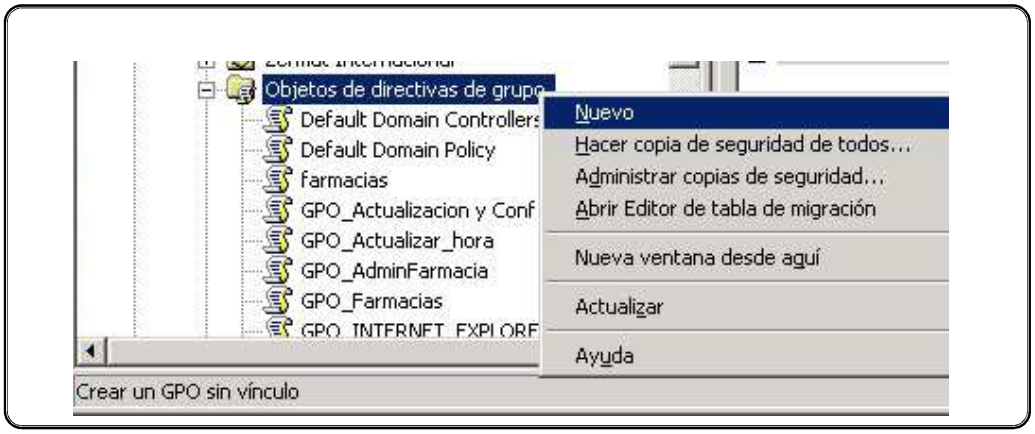


Ilustración 4:24 Configuración de Políticas de Grupo 5

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.

Ilustración 4:25 Configuración de Políticas de Grupo 6

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:

Ilustración 4:26 Configuración de Políticas de Grupo 7

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.

Ilustración 4:27 Configuración de Políticas de Grupo 8

Se abrirá una ventana de configuración con las diferentes opciones configurables

Ilustración 4:28 Configuración de Políticas de Grupo 9

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

Para el caso de Farmaenlace se han creado las siguientes Directivas de Grupo:

a. Default Domain Policy
b. Default Domain Controllers Policy
c. GPO_Actualización y configuración de seguridad
d. GPO_Actualizar_hora
e. GPO_Admin_Farmacia
f. GPO_Farmacias
g. GPO_Internet_Explorer
h. GPO_Mensajeria_P2P
i. GPO_Restric_Manipulacion
j. GPO_Restricción_Unidades
k. GPO_Restricciones_Varias
l. GPO_WallPaper_Corporativo
m. GPO_Wsus_Corporativo
n. GPO_Wsus_Sistemas

El detalle de configuración de las GPO se encuentra en el Anexo E

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. Seleccionar la opción "Agregar o quitar componentes de Windows"
c. En la ventana de asistente se debe seleccionar **Servicios de Red** y luego hacer clic en detalles
d. En esta ventana se debe seleccionar **Protocolo de configuración dinámica de host (DHCP)** con un visto y se da clic en Aceptar.

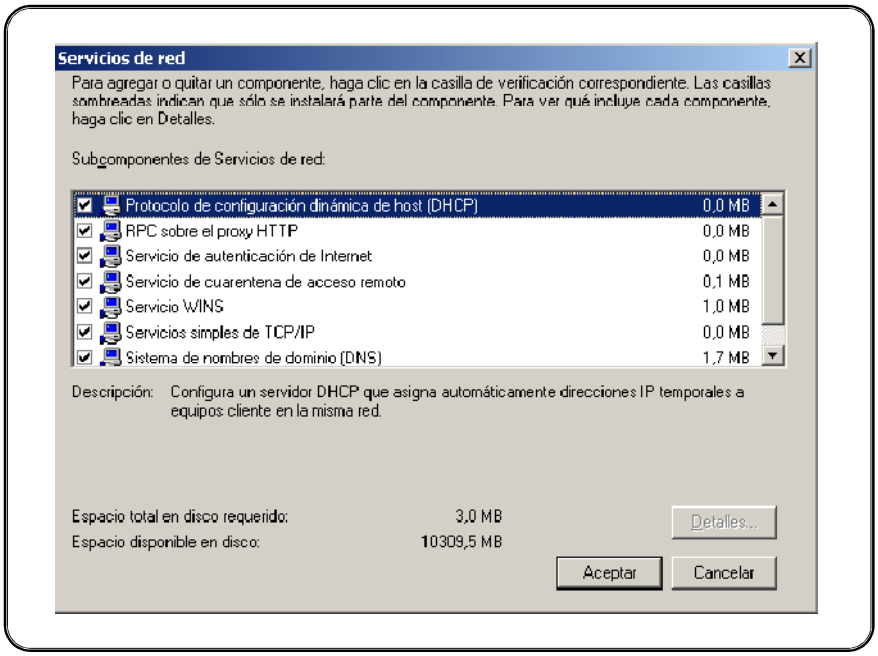


Ilustración 4:29 Configuración DHCP 1

e. Al volver a la ventana anterior se hace clic 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.

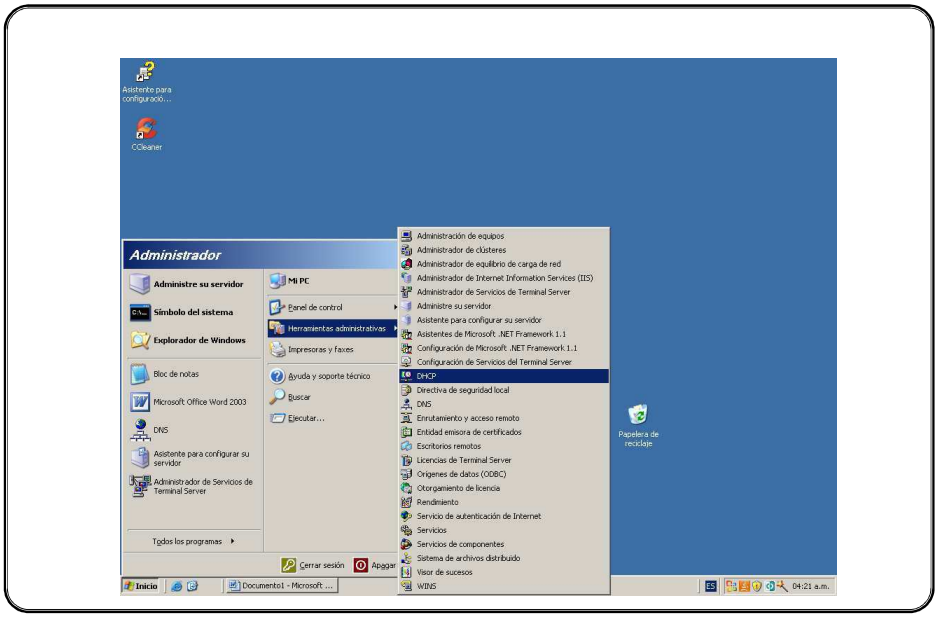


Ilustración 4:30 Configuración DHCP 2

La consola de administración se muestra de la siguiente manera:

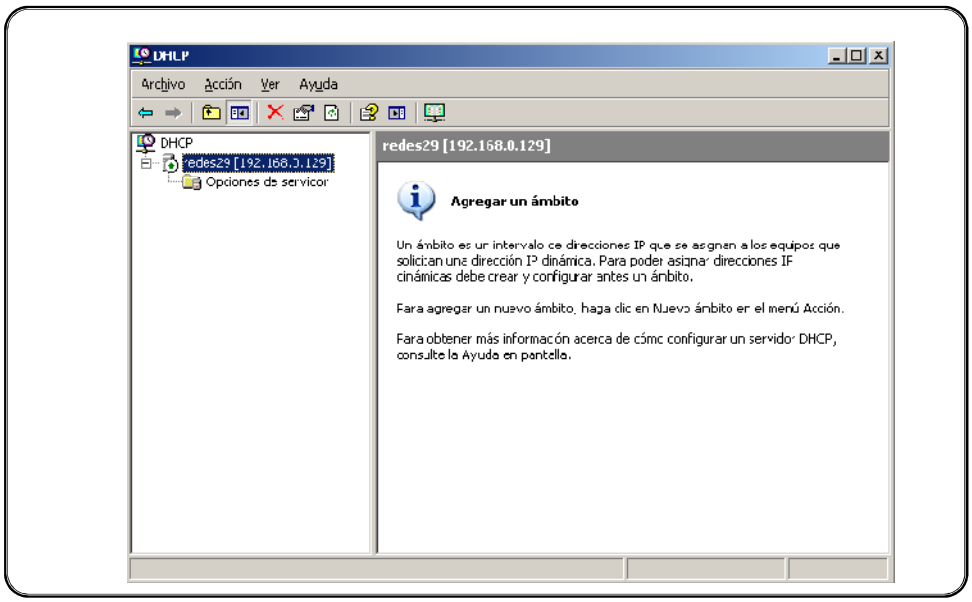


Ilustración 4:31 Configuración DHCP 3

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

b. Clic derecho sobre el nombre del servidor.

c. Seleccionar la opción **Ámbito Nuevo.**

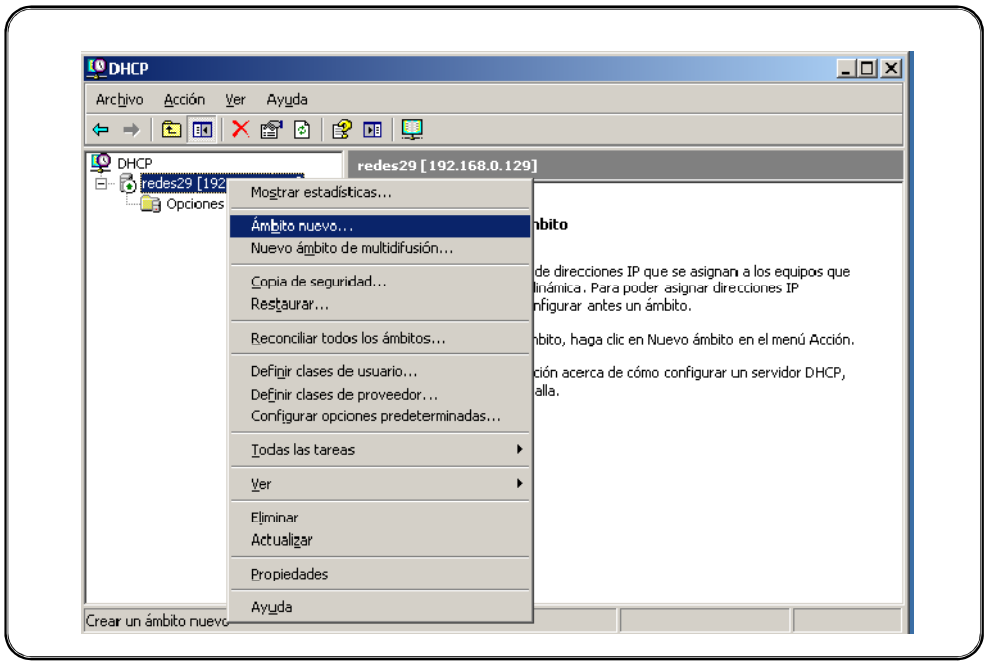


Ilustración 4:32 Configuración DHCP 4

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

e. En esta pantalla se debe indicar el nombre del Ámbito y una descripción.

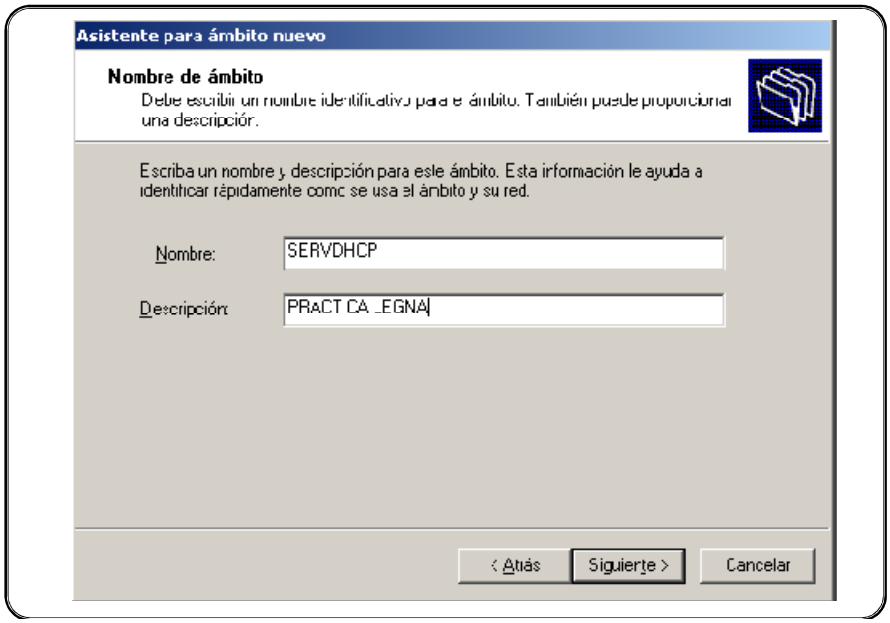


Ilustración 4:33 Configuración DHCP 5

Los datos que se colocan son:

Ámbito: TIPO B

Descripción: Red Farmaenlace

Esto debido a que la red que se va a asignar como Ámbito DHCP es la red tipo B 172.30.0.0

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

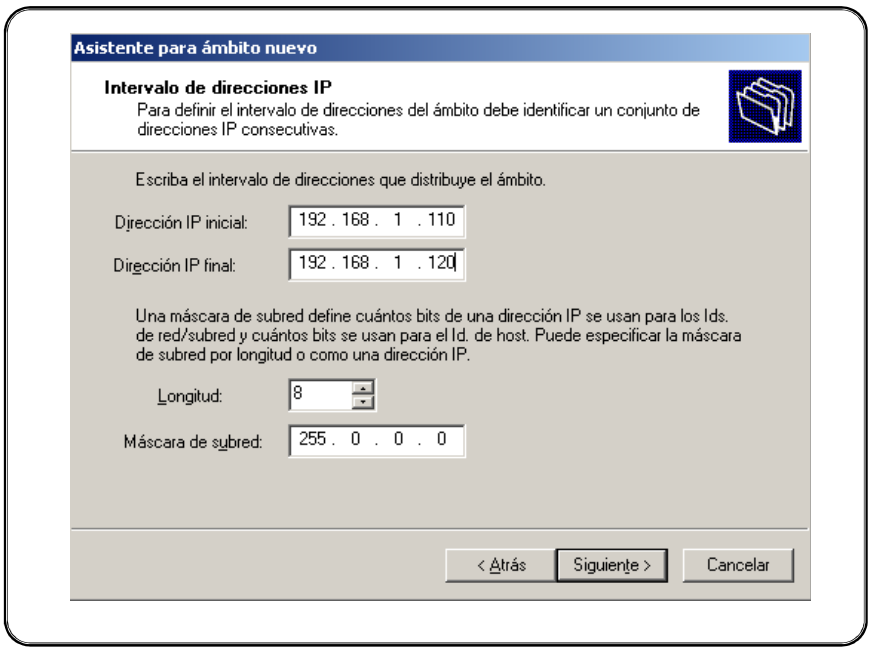


Ilustración 4:34 Configuración DHCP 6

Para Farmaenlace se define:

1. Dirección IP Inicial: 172.30.3.1
2. Dirección IP Final: 172.30.3.254
3. Mascara de Subred: 255.255.0.0

Administrativamente se decide organizar las direcciones IP de la red tipo B 172.30.0.0 /16 de la siguiente manera:

El rango de direcciones desde 172.30.1.1 hasta 172.30.1.255 se asignará por reserva de direcciones en el servidor DHCP para todos los computadores que necesitan acceso abierto al internet.

El rango de direcciones desde 172.30.2.1 hasta 172.30.2.255 se asignará mediante reserva de direcciones en el servidor DHCP a todos los equipos que necesiten acceso limitado a internet o acceso a aplicaciones específicas que validan que el host tenga una IP para permitir el acceso.

El rango de direcciones desde 172.30.3.1 hasta 172.30.3.254 se deja como rango de asignación dinámica sin acceso a internet.

g. Se pueden agregar exclusiones para direcciones especificas 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.

Ilustración 4:35 Configuración DHCP 7

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

La configuración se define en:

Días: 0

Horas: 8

Minutos: 0

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

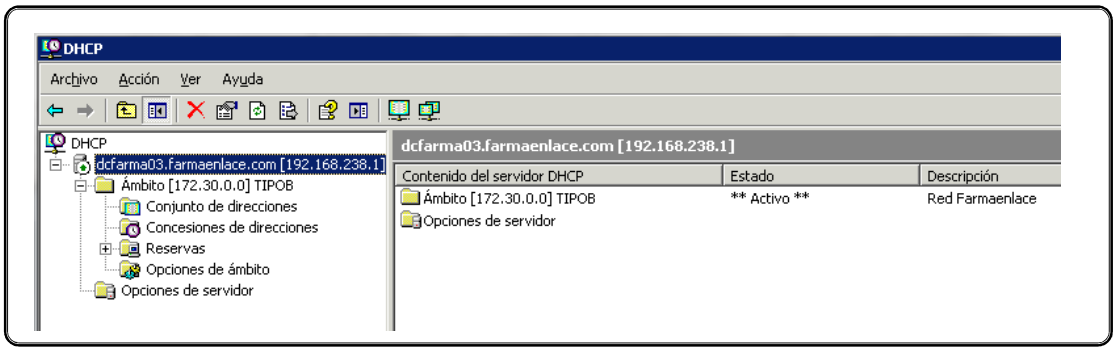


Ilustración 4:36 Configuración DHCP 8

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

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

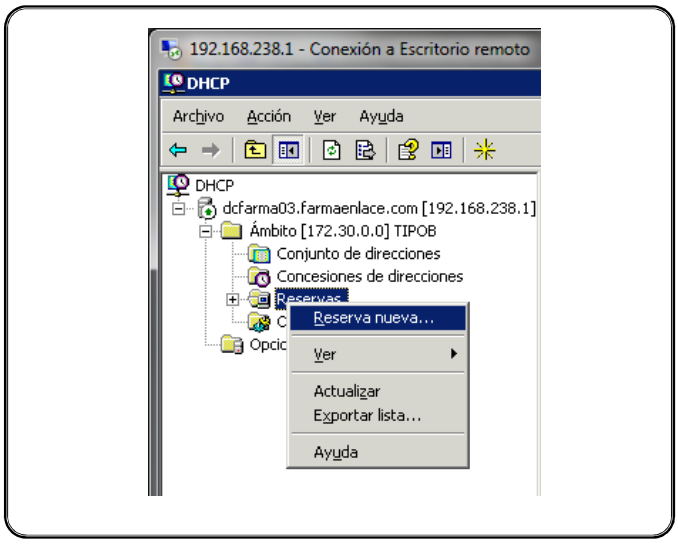


Ilustración 4:37 Configuración DHCP 9

b. En la ventana que aparece se deben ingresar los siguientes datos para realizar una reserva de dirección IP:

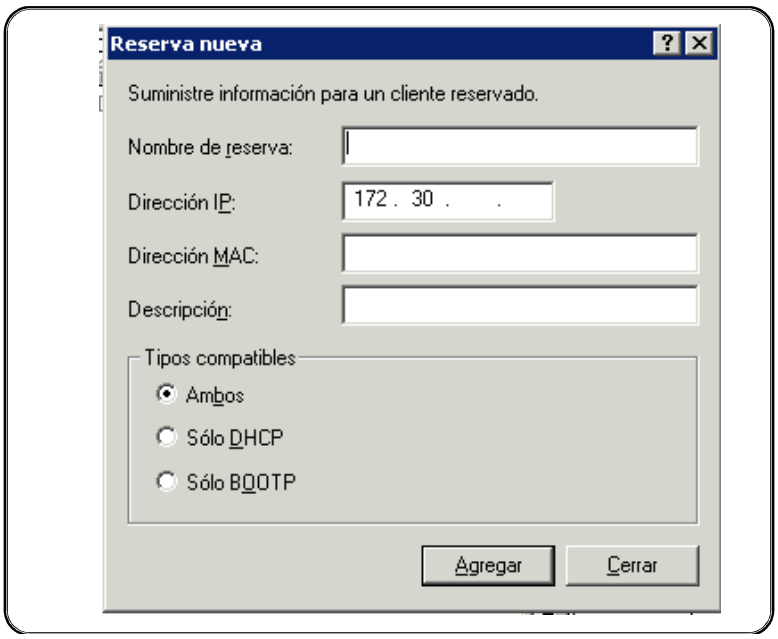


Ilustración 4:38 Configuración DHCP 10

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: La dirección física o MAC Address 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

Según (Norwood, 2007), Microsoft Windows Server Update Services (WSUS) 3.0 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 3.0

1. Haga doble clic en el archivo del instalador, **WSUSSetup.exe**.
2. En la página de **bienvenida** del Asistente para la instalación, haga clic en **Siguiente**.
3. En la página **Selección del modo de instalación**, haga clic en **Instalación de servidor completa incluida la consola de administración** si desea instalar el servidor en este equipo o **Sólo la consola de administración** si únicamente desea instalar la consola de administración.
4. En la página **Contrato de licencia**, lea los términos del contrato de licencia, haga clic en **Acepto los términos del Contrato de licencia** y después haga clic en **Siguiente**.

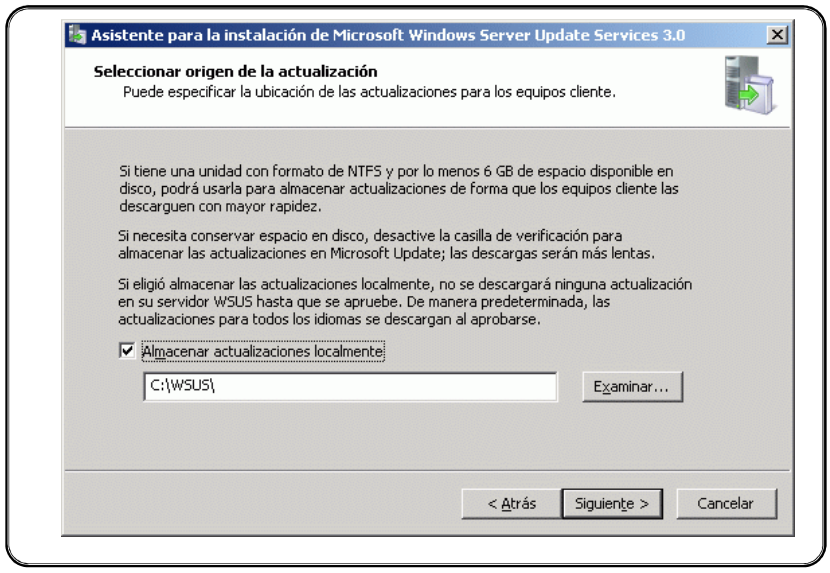


Ilustración 4:39 Configuración WSUS 1

5. En la página **Seleccionar origen de la actualización** del Asistente para la instalación, puede especificar dónde obtienen las actualizaciones los clientes. Si

activa la casilla de verificación **Almacenar actualizaciones localmente**, las actualizaciones se almacenarán en el servidor WSUS 3.0 y seleccionará una ubicación en el sistema de archivos para almacenar actualizaciones. Si no almacena las actualizaciones localmente, los equipos cliente se conectarán a Microsoft Update para obtener actualizaciones aprobadas. Conservar las opciones predeterminadas y haga clic en **Siguiente**.

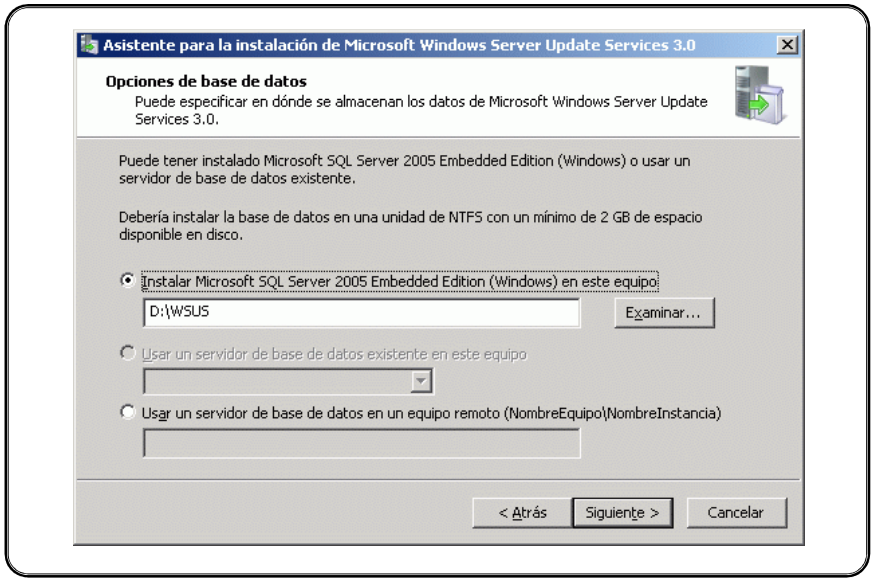


Ilustración 4:40 Configuración WSUS 2

6. En la página Opciones de base de datos, seleccione el software utilizado para administrar la base de datos de WSUS 3.0 de manera predeterminada, el programa de instalación de WSUS ofrece la opción de instalar Windows Internal Database, si el equipo en el que se realiza la instalación ejecuta Windows Server 2003.
7. Si no desea usar Windows Internal Database, deberá indicar una instancia de SQL Server para WSUS, haciendo clic en Usar un servidor de base de datos existente en este equipo y escribiendo el nombre de instancia en el cuadro. El nombre de la instancia debe aparecer como <nombreServidor>\<nombreInstancia>, donde nombreServidor es el nombre del servidor y nombreInstancia es el nombre de la instancia SQL. Realizar la selección y después haga clic en Siguiente.
8. En la página Conectando con la instancia de SQL Server, WSUS intentará conectarse a la instancia especificada de SQL Server. Cuando se haya conectado correctamente, haga clic en Siguiente para continuar.

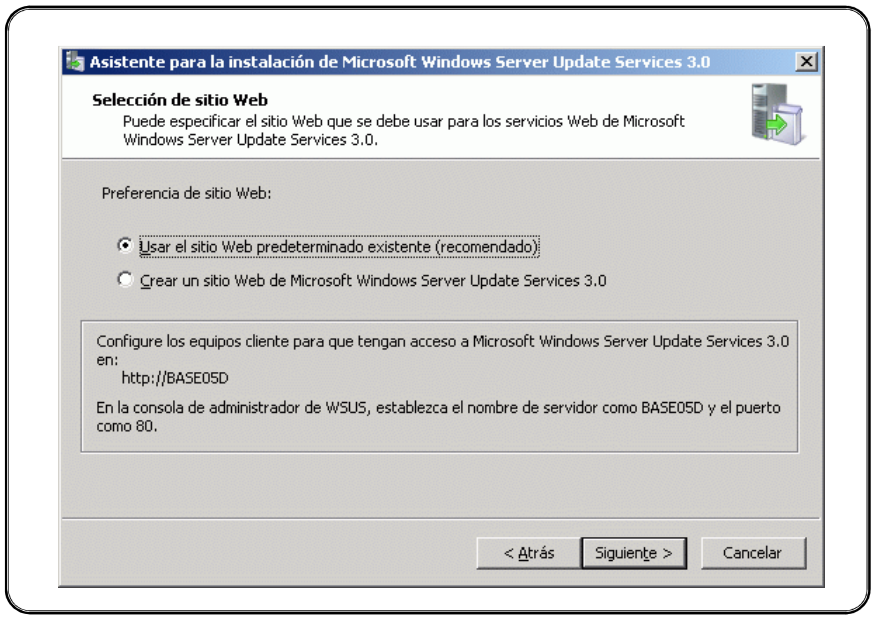


Ilustración 4:41 Configuración WSUS 3

9. En la página Selección de sitio Web, indique el sitio Web que utilizará WSUS 3.0. Si desea utilizar el sitio Web de IIS predeterminado en el puerto 80, seleccione la primera opción. Si ya tiene un sitio Web en el puerto 80, podrá crear un sitio alternativo en el puerto 8530 si selecciona la segunda opción. Conserve la opción predeterminada y haga clic en Siguiente.
10. En la página Preparado para instalar Windows Server Update Services, compruebe las selecciones y haga clic en Siguiente.
11. La página final del Asistente para la instalación le dirá si la instalación de WSUS 3.0 se completó correctamente. Después de hacer clic en Finalizar, el Asistente para la configuración se iniciará.
12. Después de instalar WSUS 3.0, el Asistente para la configuración se iniciará de forma automática. También puede ejecutarlo en otro momento a través de la página **Opciones** de la consola de WSUS 3.0.

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**

Como primer paso hay que configurar la salida a internet por parte del servidor, ya que es necesario que WSUS se comunique con Microsoft Update para obtener las actualizaciones a través del puerto 80 para el protocolo HTTP y el puerto 443 para el protocolo HTTPS, se puede configurar acceso explicito únicamente a las siguientes páginas:

a. http://windowsupdate.microsoft.com

b. http://*.windowsupdate.microsoft.com

c. https://*.windowsupdate.microsoft.com

d. http://*.update.microsoft.com

e. https://*.update.microsoft.com

f. http://*.windowsupdate.com

g. http://download.windowsupdate.com

h. http://download.microsoft.com

i. http://*.download.windowsupdate.com

j. http://wustat.windows.com

k. http://ntservicepack.microsoft.com

La primeara vez que se ingresa a la consola de WSUS se presenta un asistente de configuración, que muestra todos los parámetros necesarios para que el servicio funcione correctamente; mismos que se describen a continuación.

Por defecto la configuración de descarga de actualizaciones es a través de Internet, pero puede configurarse WSUS para descargar actualizaciones de otro servidor WSUS para esta configuración se debe realizar lo siguiente:

1. Desde el Asistente para la configuración, y después de unirse al Programa de mejora de Microsoft, haga clic en **Siguiente** para elegir el servidor que precede en la cadena.

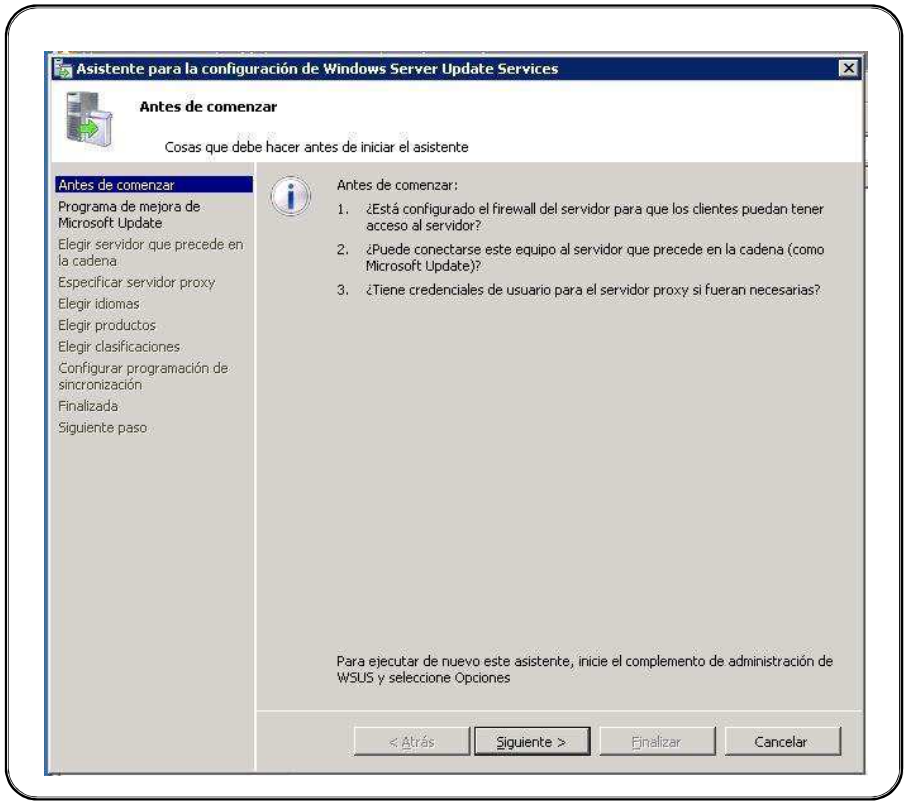


Ilustración 4:42 Configuración WSUS 4

2. Si elige sincronizar desde Microsoft Update, habrá terminado con esta página. Haga clic en **Siguiente.**

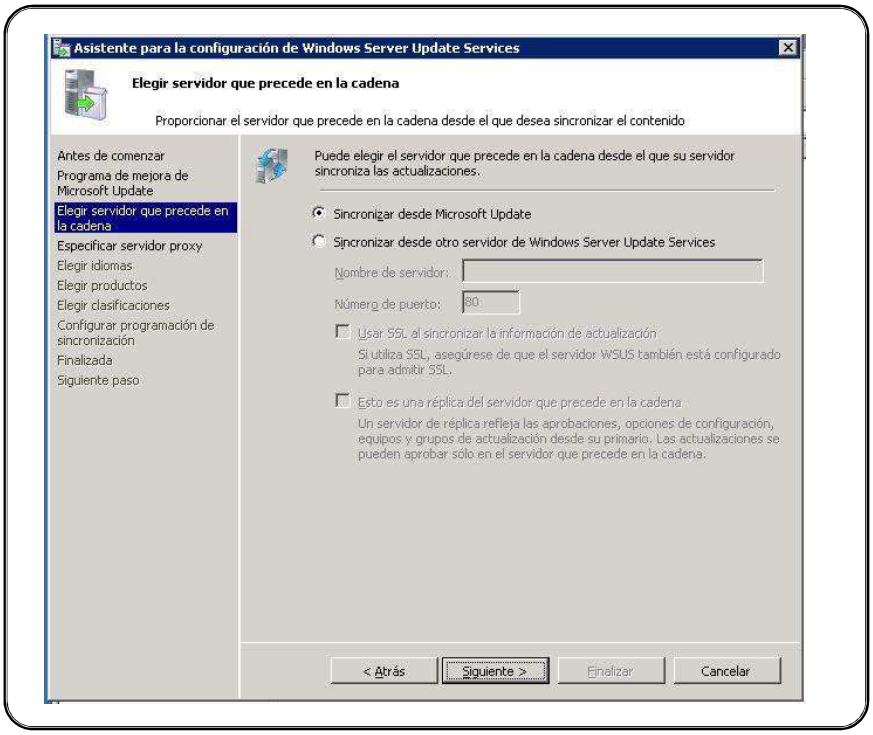


Ilustración 4:43 Configuración WSUS 5

3. Si elige sincronizar desde otro servidor WSUS, especifique el nombre del servidor y el puerto en que este servidor se comunicará con el servidor que precede en la cadena.

4. Para usar SSL, active la casilla de verificación **Usar SSL al sincronizar la información de actualización**. En ese caso los servidores usarán el puerto 443 para la sincronización. (Debe asegurarse de que tanto este servidor como el que precede en la cadena admiten SSL.)

5. Si se trata de un servidor de réplica, active la casilla de verificación "**Esto es una réplica del servidor que precede en la cadena"**.

6. En este punto ha terminado con la configuración del servidor que precede en la cadena. Haga clic en **Siguiente**

En la siguiente pantalla se debe configurar si es necesario la conexión a internet a través de un servidor proxy, en este caso no se realizará ninguna configuración y se pasa a la siguiente pantalla donde antes de proceder con las demás configuraciones es necesario iniciar la conexión con el servidor de Windows Update, que permite al servidor verificar si tiene acceso completo a las actualizaciones de Microsoft, en caso de ocurrir algún error de conexión se notificará para las pertinentes correcciones, en el momento que se tienen una conexión exitosa se pasa a la siguiente pantalla.

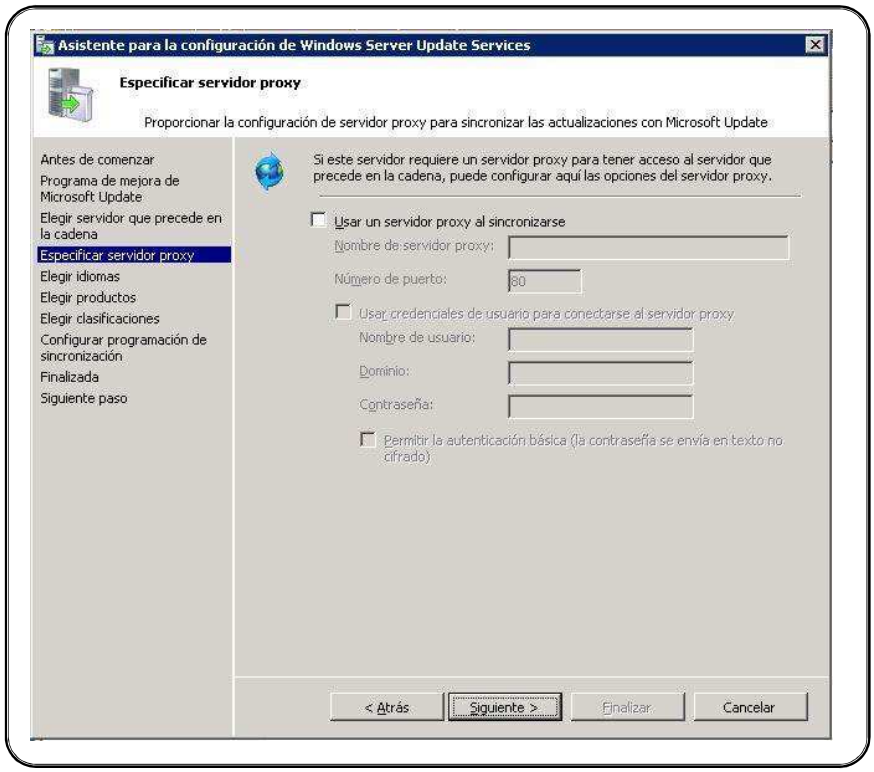


Ilustración 4:44 Configuración WSUS 6

La página **Elegir idiomas** permite obtener actualizaciones de todos los idiomas o de un subconjunto de idiomas. Si se selecciona un subconjunto de idiomas se ahorrará espacio en disco, pero es importante elegir todos los idiomas que necesitan todos los clientes de este servidor WSUS.

Si elige obtener actualizaciones sólo para algunos idiomas, seleccione **Descargar actualizaciones sólo en estos idiomas** y seleccione los idiomas para los que desea las actualizaciones

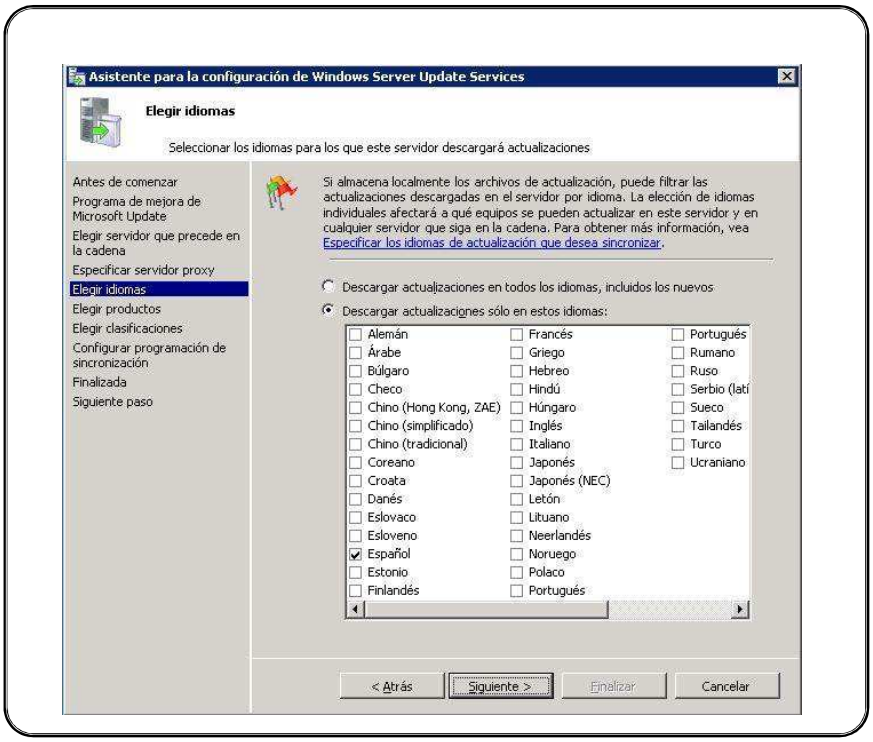


Ilustración 4:45 Configuración WSUS 7

El siguiente paso es elegir los productos que estarán sometidos a actualización, la página **Elegir productos** permite especificar los productos para los que se desea obtener actualizaciones, se puede seleccionar categorías de productos, como Windows, o productos específicos, como Windows Server 2003 o Microsoft Office. Si selecciona una categoría de productos, se seleccionarán también todos los productos contenidos dentro de esta.

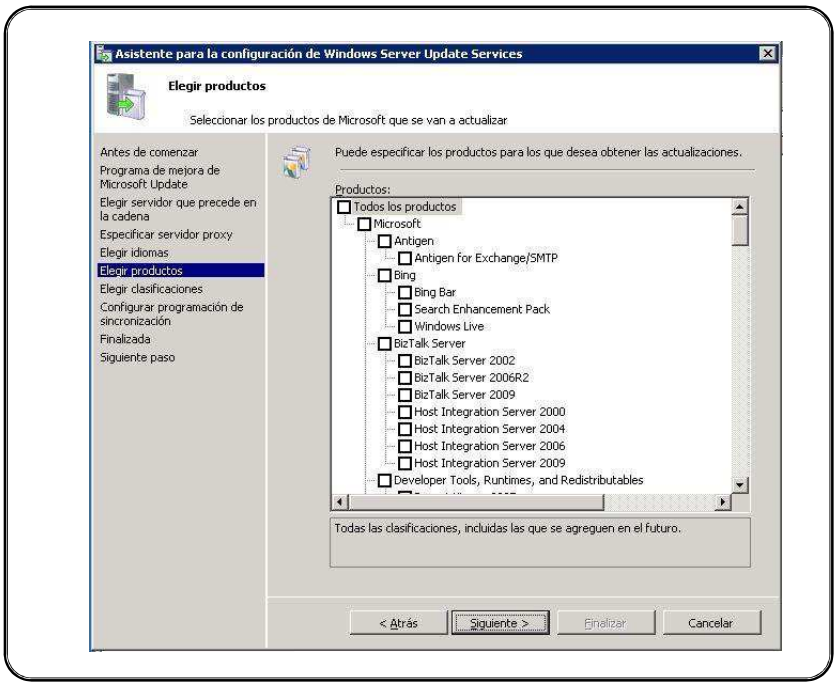


Ilustración 4:46 Configuración WSUS 8

A continuación, debe elegir las clasificaciones de actualización la página **Elegir clasificaciones** le permite elegir las clasificaciones de actualización que desee obtener. Puede elegir todas las clasificaciones o un subconjunto de ellas según la criticidad o paquetes que se desee actualizar mediante WSUS.

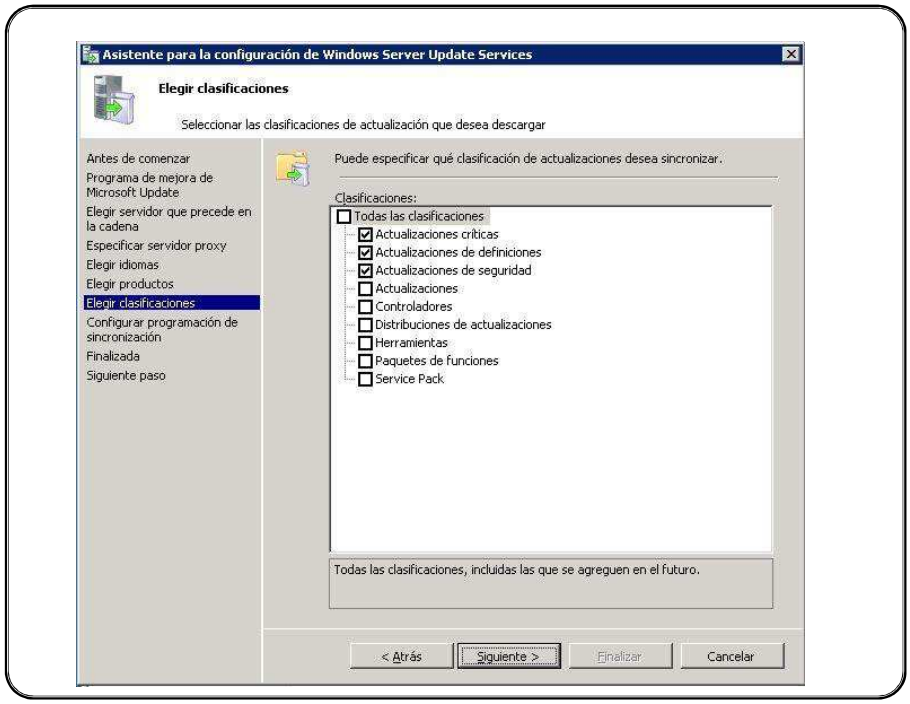


Ilustración 4:47 Configuración WSUS 9

Se procede a configurar la programación de sincronización que puede realizarse manual o automáticamente, siguiendo en el asistente de configuración. Aparecerá la página **Establecer una programación de sincronización**, que permite elegir si realizar la sincronización manual o automáticamente. Si se elige sincronizar manualmente en este servidor, tendrá que iniciar el proceso de sincronización desde la consola de administración de WSUS. Si elige sincronizar automáticamente, el servidor WSUS sincronizará en los intervalos especificados. Se debe establecer la hora de la primera sincronización y el número de sincronizaciones por día que desea que realice este servidor. Por ejemplo, si especifica que debe haber cuatro sincronizaciones al día, comenzando a las 3:00 a.m., las sincronizaciones tendrán lugar a las 3:00 a.m., 9:00 a.m., 3:00 p.m. y 9:00 p.m.

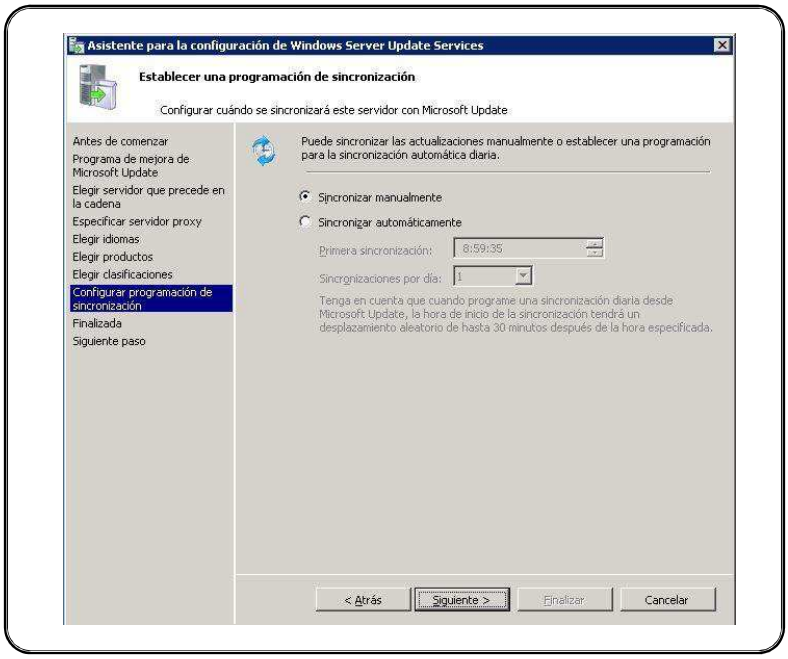


Ilustración 4:48 Configuración WSUS 10

Tras haber completado todos los pasos de configuración anteriores, seleccione la página **Finalizada** en el asistente para la configuración. Puede iniciar la consola de administración de WSUS si deja activada la casilla de verificación **Iniciar el complemento de administraciones de Windows Server Update Services** e iniciar la primera sincronización si deja activada la casilla de verificación **Iniciar sincronización inicial**.

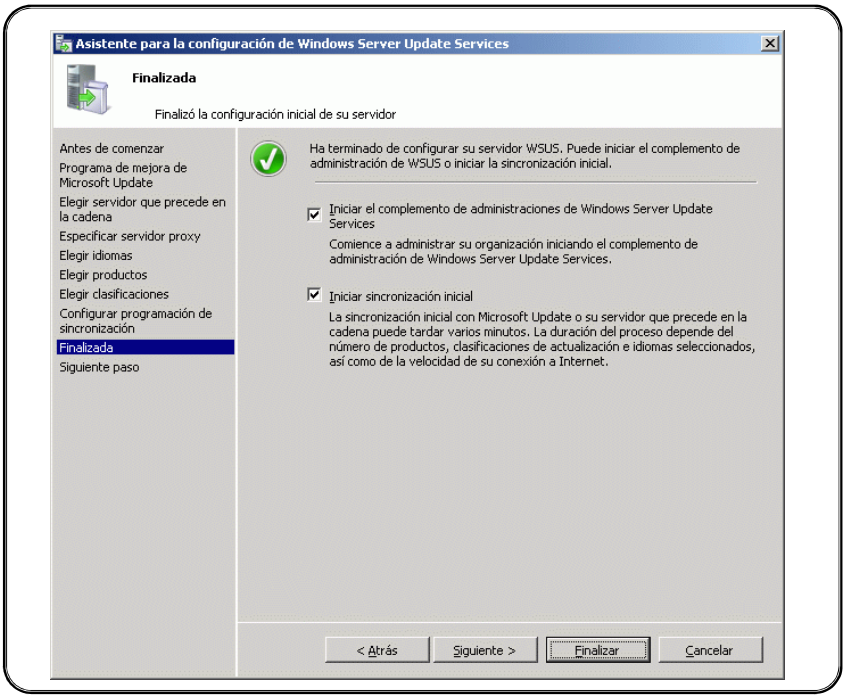


Ilustración 4:49 Configuración WSUS 11

Cuando se termine con el asistente se podrá acceder a la consola de administración de WSUS, donde se irán agregando actualizaciones y equipos que se conviertan en clientes de este servidor y se podrá conocer el estado de actualizaciones que tenga cada cliente mediante los reportes que emite esta consola.

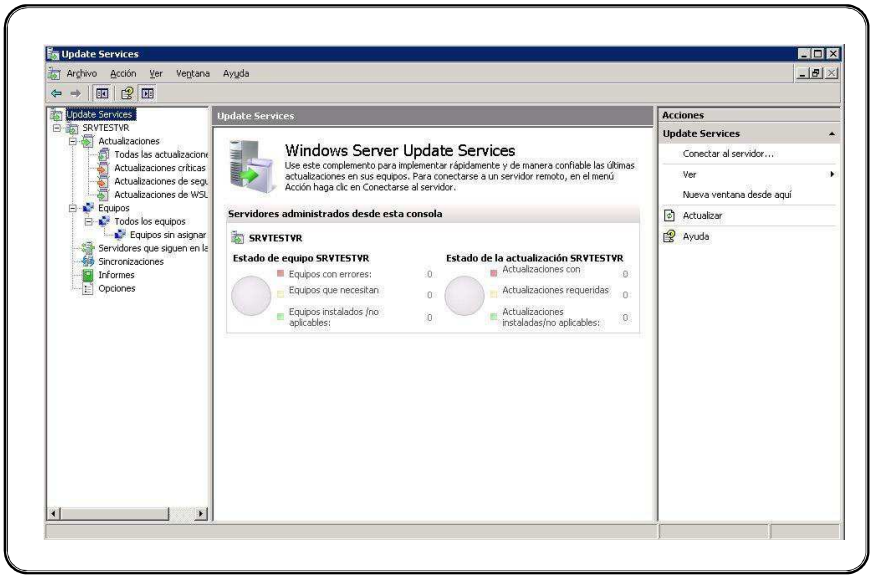


Ilustración 4:50 Configuración WSUS 12

Una vez que se ha terminado de configurar el servicio de actualizaciones automáticas WSUS, es hora de configurar las actualizaciones automáticas en los equipos cliente, Los equipos cliente de WSUS requieren una versión compatible de actualizaciones automáticas. El programa de instalación de WSUS configura automáticamente IIS para distribuir la versión más reciente de Actualizaciones automáticas en cada equipo cliente que se ponga en contacto con el servidor WSUS.

La mejor manera de configurar las Actualizaciones automáticas en un entorno con Active Directory, es usar un objeto de directiva de grupo (GPO) basado en dominios. Si usa el objeto de directiva de grupo local o un GPO basado en dominios, tiene que señalar con sus equipos cliente al servidor WSUS y, a continuación, configurar Actualizaciones automáticas.

Se procede con la creación de una GPO que almacenará la configuración para que los clientes accedan al servicio de actualizaciones automáticas, una vez creada la GPO se procede a configurarla:

1. En el Editor de objetos de directiva de grupo, expandir Configuración del equipo, Plantillas administrativas, Componentes de Windows y haga clic en Windows Update.

2. En el panel de detalles, haga doble clic en Configurar actualizaciones automáticas.

3. Haga clic en Habilitadas y realice una de las acciones siguientes:

   a) **Notificar descarga y notificar instalación**: Esta opción envía una notificación a un usuario administrativo que ha iniciado sesión antes de que comience la descarga y la instalación de las actualizaciones.

   b) **Descargar automáticamente y notificar instalación**: Esta opción comienza automáticamente a descargar actualizaciones y a continuación, envía una notificación a un usuario administrativo que ha iniciado sesión antes de instalar las actualizaciones.

   c) **Descargar automáticamente y programar la instalación**: Si las actualizaciones automáticas se configuran para realizar una instalación programada, tiene que establecer el día y la hora para la instalación programada recurrente.

   d) **Permitir que el administrador local elija la opción**: Con esta opción, los administradores locales pueden usar Actualizaciones automáticas del Panel de control para seleccionar la opción de configuración que deseen. Por ejemplo, pueden elegir su propia hora de instalación programada. Los administradores locales no pueden deshabilitar las actualizaciones automáticas.

Para configurar la ruta al servidor WSUS:

1. En el Editor de objetos de directiva de grupo, expanda Configuración del equipo, Plantillas administrativas, Componentes de Windows y haga clic en Windows Update.

2. En el panel de detalles, haga doble clic en Especificar la ubicación del servicio Windows Update en la intranet.

3. Haga clic en Habilitada y escriba la dirección URL de HTTP del mismo servidor WSUS en los cuadros Establecer el servicio de actualización de la intranet para detectar

actualizaciones y Establecer el servidor de estadísticas de la intranet. Por ejemplo, escriba *http://nombreServidor* en ambos cuadros y a continuación, haga clic en Aceptar.

Tras configurar un equipo cliente, transcurrirán unos minutos antes de que aparezca en la página **Equipos** de la consola de WSUS. Para los equipos cliente configurados con una directiva de grupo basada en dominios, tardará alrededor de 20 minutos después de que la directiva de grupo se actualice (es decir, se aplique cualquier configuración de directiva nueva al equipo cliente). De manera predeterminada, la directiva de grupo se actualiza en segundo plano cada 90 minutos, con un intervalo aleatorio de 0 a 30 minutos. Si desea actualizar la directiva de grupo antes, puede ir a un símbolo del sistema del equipo cliente y escribir: **gpupdate /force**.

Para los equipos cliente configurados con la GPO local, la directiva de grupo se aplica inmediatamente y la actualización dura alrededor de 20 minutos.

Una vez aplicada la directiva de grupo, puede iniciar manualmente la detección.

Para iniciar manualmente la detección del servidor WSUS realizar lo siguiente:

1. En un equipo cliente, haga clic en **Inicio** y después en **Ejecutar**.
2. Escriba **cmd** en el cuadro **Abrir** y después haga clic en **Aceptar**.
3. En el símbolo del sistema, escriba **wuauclt.exe /detectnow**. Esta opción de línea de comandos hace que Actualizaciones automáticas se ponga en contacto con el servidor WSUS inmediatamente.

4.5 Correo electrónico

De acuerdo con las decisiones administrativas de unificación de servicios, conserva el servicio de correo bajo el dominio de Farmaenlace.com, este servicio que se encuentra configurado en un servidor con sistema operativo Linux Centos 5.3, 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 especifico, 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 (quarantine).

Los parámetros configurados dentro de Farmaenlace para el servicio de correo electrónico son:

a) Dominio de cuentas de correo: farmaenlace.com
b) Límite de tamaño en archivo adjunto para envío y recepción: 10Mb

c) En caso de detectarse correo Spam: enviar a la cuenta spamcop@farmaenlace.com

d) En caso de detectarse correo dañino o con virus se enviará a la carpeta ubicada en var/spool/MailScanner/quarantine/

4.6 Navegación y servicios Web

Para el servicio de navegación y firewall, se mantiene el servidor que utiliza Farmaenlace basado en un sistema operativo Linux Centos 5.3, configurado como proxy transparente con la utilización del servicio SQUID para permitir la navegación de la red de Farmaenlace 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 por lo general sus extensiones son gob.ec.

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 vuelos y páginas afines.
d. Seguridad y monitoreo.- contiene páginas de agencias de seguridad y páginas de monitoreo y rastreo satelital de vehículos.
e. Antivirus.- lista de acceso para que se permita la descarga de actualizaciones en línea de software antivirus.

CAPÍTULO 5

5 IMPLEMENTACIÓN DEL PROYECTO (Procedimientos y Políticas)

Una vez concluida la migración en su aspecto físico y de configuración de servicios, para garantizar un correcto funcionamiento y administración de todo el nuevo DataCenter y por ende todas las prestaciones que se brindan a la empresa Farmaenlace, es necesario establecer la documentación adecuada para que sirva de guía y fuente de consulta continua de tal manera que un operario del área de sistemas sea capaz de utilizar esta documentación para configurar accesos, conceder permisos, controlar el funcionamiento

y sobre todo normar el correcto aprovechamiento de los recursos de la empresa y el uso de la información y los sistemas que permiten el acceso a la misma.

A continuación se describen las principales políticas y procedimientos con los que se trabaja en Farmaenlace Cía. Ltda.

5.1 Procedimiento de Configuración de equipos Cliente

Un equipo cliente o host perteneciente a cualquier colaborador de la empresa antes de ser entregado al colaborador deberá ser configurado siguiendo las siguientes normas:

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. Número de Equipo (2 dígitos)

Ejemplo:

Para nombrar al equipo de Oficina Matriz en el área de contabilidad número 5 se deberá colocar el nombre de equipo:

MACON05

b. **Ingreso del equipo al dominio de Farmaenlace.-** Un equipo nuevo debe ser agregado como equipo cliente del dominio de Farmaenlace para esto se debe realizar los siguientes pasos:

a. Clic en inicio

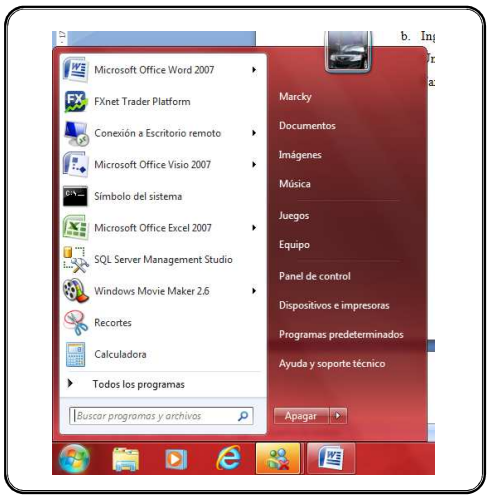


Ilustración 5:1 Agregar equipo al Dominio 1

b. Clic derecho en Mi PC(Windows Xp y 2003) o en Equipo (Windows Vista o Windows 7)

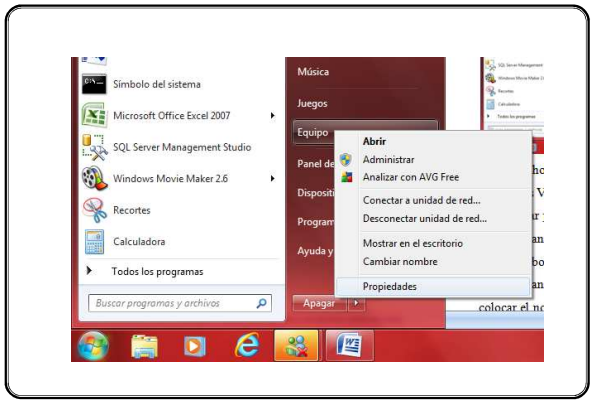


Ilustración 5:2 Agregar equipo al Dominio 2

c. Seleccionar propiedades, si el equipo posee sistema operativo Windows 7 o Windows Vista, en la ventana de propiedades se debe hacer clic en configuración avanzada del sistema.

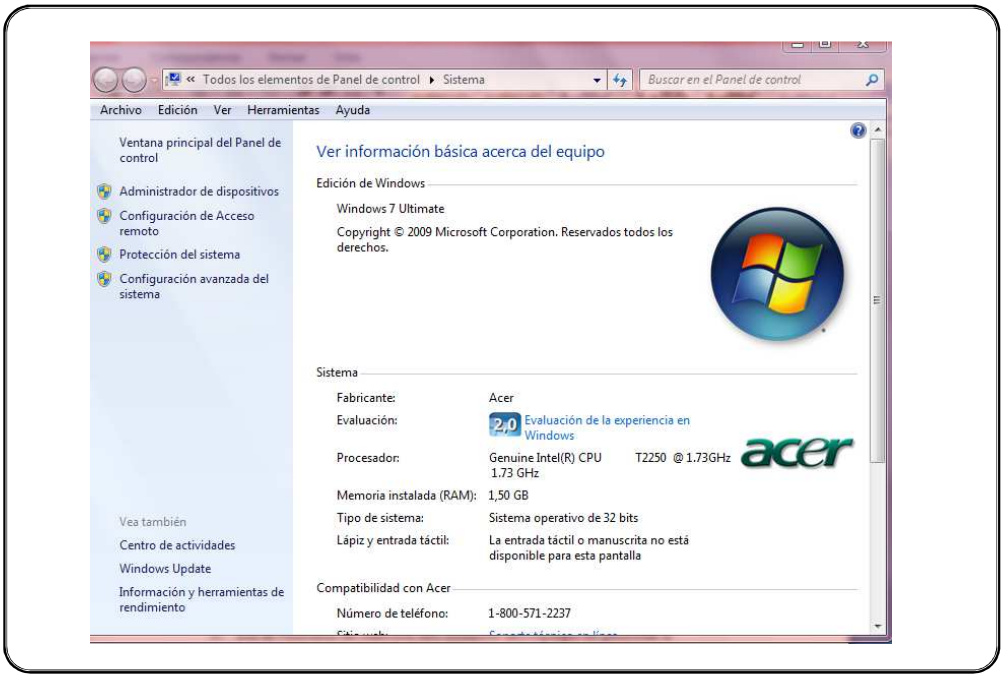


Ilustración 5:3 Agregar equipo al Dominio 3

d. En la ventana de propiedades seleccionar Nombre del Equipo

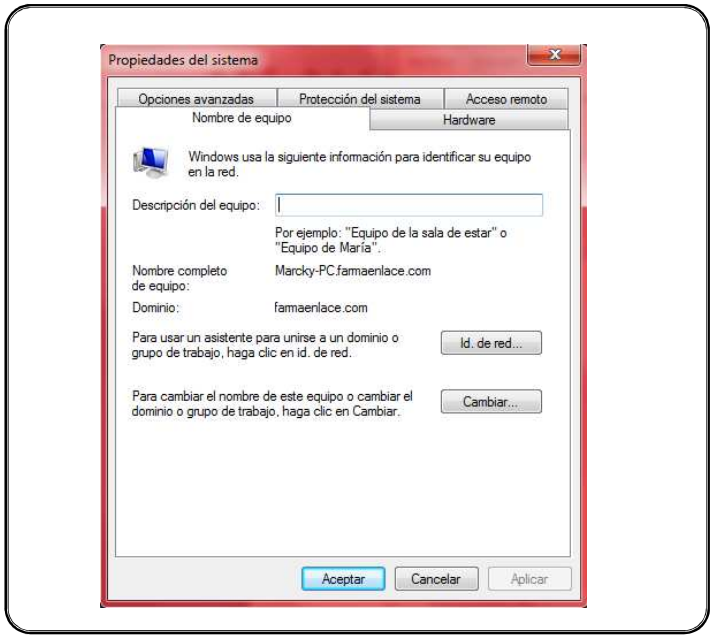


Ilustración 5:4 Agregar equipo al Dominio 4

Clic en el botón Cambiar

e. En la ventana de edición del nombre del equipo se procede a colocar el nombre previamente definido y en el campo Dominio se coloca Farmaenlace.com que corresponde al dominio al cual se deberá ingresar el equipo en mención.

Ilustración 5:5 Agregar equipo al Dominio 5

f. 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, colocar las credenciales correctas y hacer clic en aceptar.

Ilustración 5:6 Agregar equipo al Dominio 6

g. 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.
h. 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.
i. 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 Farmaenlace.com

La información necesaria para crear un nuevo usuario es:

a. Nombres del usuario a crear
b. Área donde pertenece el usuario

Además del controlador principal de dominio existen los servidores secundarios que se encuentran ubicados en los lugares donde mayor concentración de usuarios existe que son: oficinas Ibarra y supermercados.

El procedimiento para crear un nuevo usuario es:

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

Ilustración 5:7 Creación de usuarios 1

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

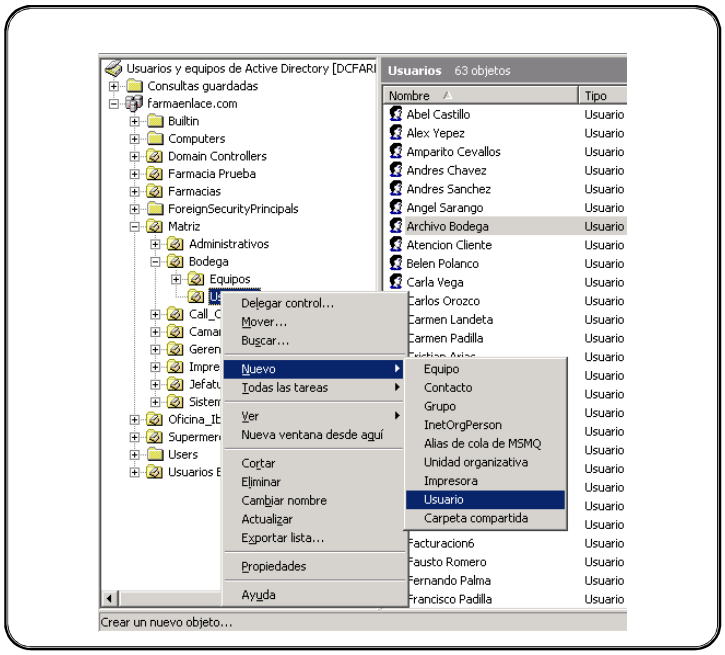


Ilustración 5:8 Creación de usuarios 2

c. En la carpeta **Usuarios** hacer clic derecho y luego a *Nuevo > Usuario*

d. Se procede a llenar los campos que indica la gráfica. El "**Nombre de inicio de sesión de usuario"** debe seguir las políticas de creación de usuarios.

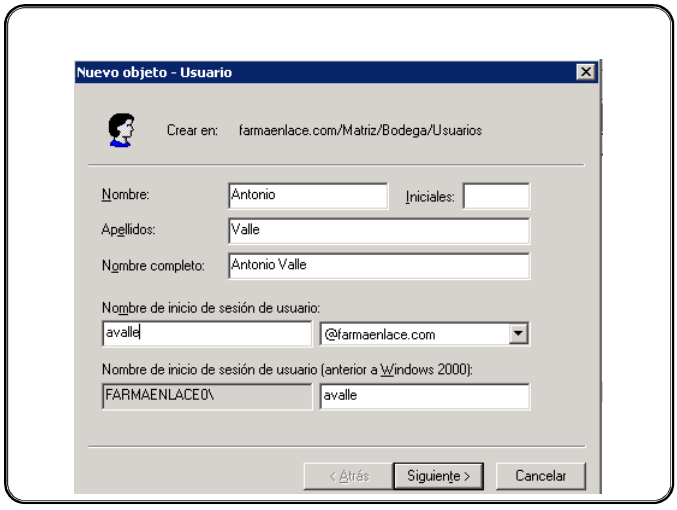


Ilustración 5:9 Creación de usuarios 3

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

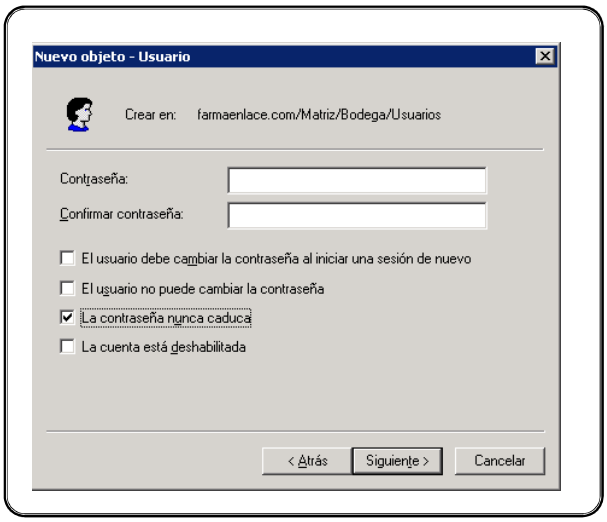


Ilustración 5:10 Creación de usuarios 4

f. Una vez creado el usuario hacer clic 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.

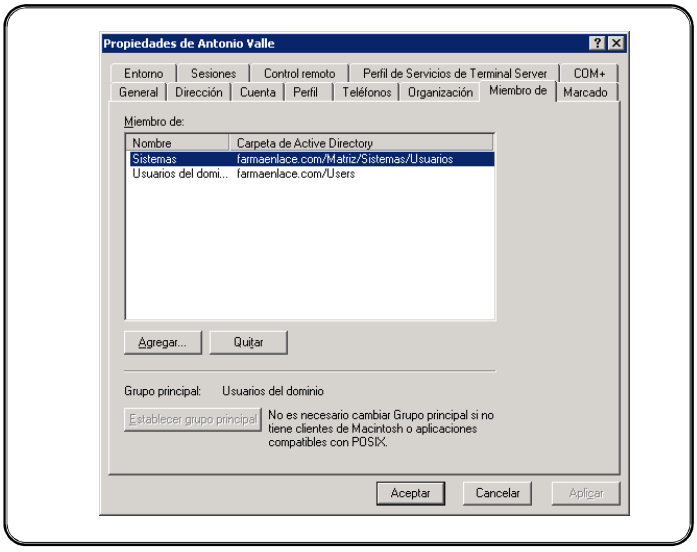


Ilustración 5:11 Creación de usuarios 5

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 puerto 6222. 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

Volviendo a la pantalla de comandos y luego de ingresar el comando "**su –"** en la consola de LINUX, 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 @farmaenlace.com, por ejemplo, si el nuevo usuario tiene el nombre de Juan Pérez el comando deberá ser:

useradd *juanperez*

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 ***juanperez***

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 Farmaenlace se deberá digitar el nombre de la cuenta sin el dominio; es decir sin @farmaenlace.com y si son cuentas de otros dominios se deberá digitar las cuentas de correo completas.

Ejemplo:

Contabilidad: *pedrorodriguez, ximenaparedes, juanlopez@hotmail.com*

Cuando se termina de editar el archivo para guardar los 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 deben ser realizados 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 pagina institucional de la empresa y aplicaciones web internas (intranet)

La configuración de los permisos de navegación se lo realiza en los archivos ACL determinados para este fin como se describe a continuación:

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 Juan Pérez

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.

NUM	DESCRIPCION
0	BANCOS Y ENTIDADES FINANCIERAS
1	ENTIDADES DE GOBIERNO
2	SERVICIOS Y TELECOMUNICACIONES
3	TARJETAS Y CELULARES
4	SEGURIDAD Y MONITOREO
5	FARMAENLACE

6	CREDITO Y CONTABILIDAD
7	PERIODICOS Y SEGUROS
8	PAGS DE COMPRAS
9	EMPLEO Y CAPACITACION
10	MESSENGER Y HOTMAIL
11	CLIENTES MAYORISTAS
12	ACTUALIZACIONES ANTIVIRUS
lista	NAVEGACION ABIERTA

Tabla 5:2Grupos de Acceso a Navegacion Internet

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

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 **ipsweb** que 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.**

Ejemplo: ipsweb0.txt para ingresar una IP que necesita acceso a los bancos y entidades financieras.

a. Agregar nuevas categorías mediante archivos ACL

Para agregar más categorías de navegación se necesita ingresar al directorio: "**/etc/squid/**" y abrir el archivo denominado **squid.conf.**

Dentro del archivo ingresar el siguiente texto:

Acl ipsweb(num) src (path del archivo ipsweb.txt)

Acl dominiosweb(num) dstdomain (path del archivo dominiosweb.txt)

http_access allow ipsweb(num) dominiosweb(num)

Ejemplo:

Acl ipsweb15 src /etc/squid/ipsweb15.txt

Acl dominiosweb15 dstdomain /etc/squid/dominiosweb15.txt

http_access allow ipsweb15 dominiosweb15

Guardar el archivo de configuración mediante el comando **F2** y salir del archivo mediante el comando **F10**.

Ejecutar el comando de reinicio:"**service squid restart"** para reiniciar el servicio y cargar las nuevas configuraciones.

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 mas actualizado posible de los datos y aplicaciones que dan servicio a Farmaenlace Cía. Ltda.

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.

El responsable deberá diariamente revisar que los procesos automáticos del día anterior se ejecutaron exitosamente, de ser necesario comprimirlos y salvaguardar dicha información en un dispositivo de almacenamiento externo.

Los servidores de comunicaciones con sistema operativo LINUX deberán tener un backup completo de una periodicidad diaria, incluidos sábados, domingos y feriados, de todos los servicios que se ejecutan en estos servidores, mantener total énfasis en CORREO, SERVICIO WEB y SQUID. En caso que los discos superen el 95% de uso, se borrarán dichos históricos dejando mínimo los respaldos de los últimos 30 días.

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 30 días al área de Servicios Redes y Telecomunicaciones los datos de la nueva sucursal 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 SRI. Que será utilizado como parámetro de la dirección IP de la red LAN de la nueva 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 Farmaenlace.

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. FARMAENLACE CIA. LTDA, administra el servicio de correo electrónico bajo el dominio "farmaenlace.com".

La forma común de una cuenta de correo electrónico es:

<alias_del_usuario>@dominio_de_correo

En FARMAENLACE CIA.LTDA, el <alias_del_usuario> se construye utilizando los siguientes criterios:

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. Los conflictos no aclarados por las reglas anteriores serán resueltos a criterio del usuario y con la aprobación del Departamento de Sistemas.

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

La creación de un alias o lista de correo está restringida a los departamentos y servicios de la Empresa y deberá satisfacer los siguientes criterios:

a. Tamaño mínimo: 3 caracteres.

b. Tamaño máximo: 14 caracteres.

c. Formato del <alias_del_usuario>: descriptivo de la función que realiza.

En ningún caso podrá hacer referencia a una persona física a menos que el colaborador deje de pertenecer a la empresa y se necesite que los correos electrónicos dirigidos a él lleguen a otro colaborador que asuma el cargo, esto deberá ser realizado mediante solicitud expresa del gerente del departamento al que pertenece el colaborador y con la aprobación del Coordinador del área de Servicios Redes y Telecomunicaciones.

Los pasos a seguir para obtener una cuenta de correo electrónico en Farmaenlace es el siguiente:

b. 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.
c. 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, en las oficinas de sistemas o vía WebMail.
d. Es responsabilidad del usuario el cambio de clave así como mantener la confidencialidad de la misma.
e. 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, se permite mantener los mensajes en el servidor únicamente al personal que no tiene asignado un computador o a usuarios móviles que aun no descargan su correo en su equipo principal.
f. Es responsabilidad del usuario depurar su cuenta periódicamente para que exista espacio disponible y administrar su correo en forma responsable.
g. La vigencia de la cuenta comprende el periodo de compromiso de trabajo entre el usuario con la empresa, o por decisión expresa de la Gerencia de Sistemas, consultada con la gerencia del departamento del usuario.
h. Los mensajes de correo que ingresaron al servidor de la empresa en la cuenta de cualquier usuario, no podrán ser borrados sin autorización del propietario de la cuenta.
i. Es responsabilidad del usuario hacer buen uso de su cuenta, entendiendo por buen uso:
    1. El empleo de su cuenta con fines laborales.
    2. Leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.
    3. El uso de un lenguaje apropiado en sus comunicaciones.
    4. No permitir que segundas personas hagan uso de su cuenta.
j. Está estrictamente prohibido:
    1. Usar de la cuenta para fines no laborales.
    2. Enviar o contestar cadenas de correo.

3. Enviar SPAMS de información (correo basura), o enviar archivos adjuntos que pudieran contener información nociva para otro usuario como virus o pornografía.
4. Usar la cuenta de otro usuario.
5. Utilizar como repositorio para archivos de música presentaciones de PowerPoint, imágenes o videos.

k. 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 se debe solicitar la asistencia del personal de Soporte Técnico de Sistemas.

l. El Departamento de Sistemas y el departamento de Desarrollo Humano se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación institucional.

m. Para cualquier aclaración sobre su clave es necesario presentarse en el Departamento de Sistemas con algún documento que compruebe su identidad. No se darán clave, ni alguna otra información vía telefónica.

n. El tamaño máximo de los mensajes de correo electrónico incluyendo archivos adjuntos no debe superar los 5 Mb de tamaño.

o. Se restringe el paso de archivos adjuntos con las siguientes extensiones:

1. Pps
2. Lnk
3. Vb
4. Ws
5. Mpg
6. Tmp
7. Wmv
8. Bat

p. El servidor de correo electrónico analiza todo el tráfico de correo entrante y saliente, y rechazan el envío de mensajes que contienen virus. Cuando un mensaje es

rechazado se envía una notificación al destinatario del mensaje, salvo en el caso de virus que falsifiquen la cabecera de origen.

q. El Departamento de Sistemas se reserva el derecho a bloquear cuentas de correo que envíen hacia los servidores de Farmaenlace, cuyo contenido no sea laboral. De igual forma cuenta de correo que se envíe o reciba archivos no permitidos (listados en el punto anterior).

r. Las cuentas de correo serán borradas bajo las siguientes circunstancias:

   a. El usuario sale de la empresa, para lo cual el departamento de Desarrollo Humano deberá notificar al Departamento de Sistemas su salida.

   b. A solicitud del gerente del departamento del usuario.

   c. Por mal uso del servicio debidamente comprobado, la Gerencia de Sistemas consultada con la Gerencia del Departamento del usuario, serán quienes tomen la decisión.

s. El Departamento de Sistemas deberá salvaguardar la integridad y confidencialidad de la información contenida en el correo electrónico, conforme lo dicta la LEY DE COMERCIO ELECTRÓNICO FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS DEL ECUADOR.

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

a. Se privilegiará dentro de la Empresa la comunicación directa (cara a cara) 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 (pana, amigo, etc.).
   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 copiarán mails a Gerentes y/o Vicepresidentes. Por ejemplo si algún trabajo no ha sido atendido a tiempo pese a que se envió el correo a los involucrados.
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 Farmaenlace, 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 del FARMAENLACE CIA. LTDA. 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, Messenger Skype o ICQ entre otros, 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 como por ejemplo: kazaa, emule, napster, Imesh, etc. y la utilización de los recursos para distribución o reproducción, de este tipo de material ya sea vía Web o medios magnéticos.

g. Esta 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 FARMAENLACE. 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 FARMAENLACE.
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 trabajo y 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 Farmaenlace.

3. Referente a confidencialidad

Todo correo electrónico que salga desde los servidores de Farmaenlace debe llevar el siguiente texto:

> **"NOTA DE CONFIDENCIALIDAD. La información contenida en este correo electrónico es confidencial y sólo puede ser utilizada por el individuo o entidad a la cual está dirigido. Cualquier difusión, distribución o copia de mensajes netamente institucionales hacia terceros está prohibida y es sancionada por la ley. Si por error recibe este mensaje, favor notificar al remitente y borrarlo."**

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 7 caracteres.

c. La clave debe poseer números y letras.

d. La clave debe ser cambiada cada 90 días.

e. La clave no puede ser la misma de las últimas dos veces que ingresó una clave nueva (es decir debe manejar al menos 3 claves distintas).

f. El usuario será bloqueado por 30 minutos luego de 3 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.

Se recomienda bloquear el acceso a los computadores cada vez que por cualquier razón se deba abandonar el lugar de trabajo.

4. Referente a uso de recursos.

a. Todas las herramientas tales como computadoras, programas y dispositivos externos que Farmaenlace 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 Farmaenlace 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 Departamento de 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.

Se ha diseñado una matriz de análisis de riesgos para evaluar los principales procesos y el impacto que podrían producir en caso de una falla y definir los pasos a seguir para recuperar los servicios y el correcto funcionamiento de la empresa; para esto es necesario acudir al análisis de riesgos general de la empresa donde se toman en cuenta los riesgos

principales que afectarían al correcto funcionamiento en general; una vez obtenida esta información, es necesario que se tome en cuenta la parte orientada a tecnología y alinear los servicios del área de tal manera que se acoplen a la visión general.

MATRIZ DE ANALISIS DE RIESGO		PROBABILIDAD DE AMENAZA						
ELEMENTOS DE INFORMACION	MAGNITUD DE DAÑO	SUCESOS MALICIOSOS		SUCESOS NO CONTROLABLES			NEGLIGENCIA	
		ACCESO NO AUTORIZADO	VIRUS	FALLA DEL SERVICIO	DAÑO EN EQUIPOS	FALLA ELECTRICA	MAL USO DEL RECURSO	NO SE TIENE RESPALDOS
		2	4	4	3	1	3	2
DATOS E INFORMACION								
ENLACES DE DATOS	3	6	12	12	9	3	9	6
CORREO ELECTRONICO	3	6	12	12	9	3	9	6
NAVEGACION WEB	2	4	8	8	6	2	6	4
SERVIDORES DE APLICACIONES	4	8	16	16	12	4	12	8
BASES DE DATOS	4	8	16	16	12	4	12	8

Tabla 5:3 Matriz de analisis de riesgos para servicios de tecnologia Farmaenlace

A continuación se detallan los procesos a seguir para recuperar la operatividad de los servicios debido a los principales eventos que pueden producirse y que logran afectar al normal desempeño dentro de la empresa Farmaenlace.

5.10.1 Enlaces de Datos

En Farmaenlace Cía. Ltda. 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 daño 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.

Dicho sistema contiene una representación gráfica de todos los enlaces de datos que mantiene Farmaenlace, segmentados en grupos a nivel de provincias, exceptuando la provincia de Pichincha lugar donde mayor número de enlaces se tiene segmentado a nivel de sectores; adicionalmente se tiene la configuración de alarmas definidas para cuando un enlace falla, alarmar gráficamente a los 2 minutos en primera instancia, colocando el ícono representativo del enlace en color amarillo; luego, a los 5 minutos de no tener respuesta, se genera una nueva alarma, se cambia el color del ícono del enlace a rojo y se genera una alarma sonora indicando el punto caído y el tiempo que lleva sin respuesta. Si el enlace no ha regresado durante un lapso de 20 minutos, se genera una nueva alarma sonora indicando el punto que se encuentra sin conectividad y el tiempo que lleva fuera de servicio.

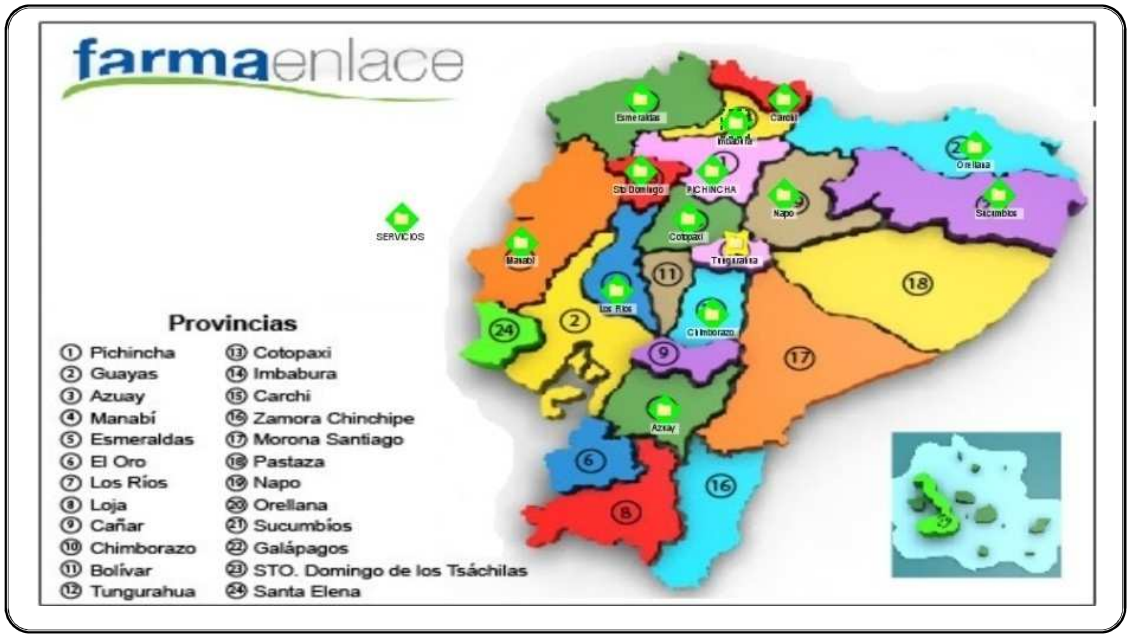


Ilustración 5:12 Imagen de sistema de monitoreo Farmaenlace

En el caso de que se detecta la caída presentada por el sistema de monitoreo se deben seguir los siguientes pasos:

1. Identificar el enlace que tiene la falla de conectividad.
2. En caso que este punto remoto tenga un enlace de respaldo (Backup) y si se debe hacer una configuración manual de intercambio de enlace, proceder a configurar las puertas de enlace predeterminadas de los equipos destino, para que apunten a la dirección IP del equipo perteneciente al enlace secundario. En caso de que el enlace de Backup tenga una configuración de conmutación automática, verificar si el enlace de backup está funcionando correctamente y que la conmutación se realizó de manera exitosa.
3. Si el punto no tiene un enlace de respaldo es necesario trabajar en la recuperación del servicio lo más pronto posible.
4. Proceder a comunicarse con el punto remoto, de preferencia con el administrador del local o el personal con conocimiento técnico del área telefónicamente y con la ayuda del personal del punto remoto realizar una revisión de las instalaciones.
5. Identificar posibles fallas eléctricas, en ese caso se debe indicar al personal que se desconecte desde la alimentación eléctrica todos los equipos electrónicos y que los vuelvan a conectar en el momento que se restablezca y se estabilice la

alimentación eléctrica en dicho lugar. Y que se comunique inmediatamente cuando el fluido eléctrico haya regresado para proceder a verificar la funcionalidad del enlace de datos.

6. Si la falla no es de carácter eléctrico, revisar el estado del equipo de comunicación del enlace de datos que puede ser un Router o un Modem ADSL, identificar si se encuentra funcionando y que indicadores luminosos se encuentran trabajando, revisar si los cables de conexión del equipo se encuentran correctamente conectados a sus dos extremos. Adicionalmente se puede solicitar al operario del sitio que reinicie el equipo indicándole el proceso a seguir, con esto debería restablecerse el servicio en caso de que el equipo estuviera inhibido.
7. Si luego de este procedimiento el enlace no ha sido restablecido, se puede considerar que puede ser una falla a nivel del proveedor, es necesario comunicarse con la central de atención al cliente del proveedor del enlace de datos y reportar la caída; indicándole que ya se hicieron las pruebas anteriormente mencionadas. El proveedor abrirá un caso y asignará su personal técnico para la revisión de este particular. Se deberá recibir un número identificativo del caso ya sea de manera verbal o por medio de correo electrónico para respaldo y posterior seguimiento del tema hasta su solución.

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.
   Ej: ping 192.168.8.1 -t

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 Farmaenlace, para lo cual es necesario revisar la configuración de los equipos de conmutación ubicados en Farmaenlace Matriz, el quipo 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.

Vía web:

Ingresar a la interfaz de administración digitando en un browser web la dirección IP del Switch Core (192.168.238.245) se solicitarán las credenciales de acceso.

En la pantalla de administración en el menú desplegable del costado izquierdo seleccionar la opción IP Route.

En esta pantalla se despliegan las rutas tanto estáticas como dinámicas aprendidas por el equipo.

Proceder a ubicar la ruta hacia el enlace deseado, si no la encuentra puede ser que dicha ruta fue deshabilitada o fue reemplazada por otra por error, es necesario eliminarla en el caso de que sea una ruta estática y volverla a configurar para esto se debe hacer clic en la pestaña REMOVE, donde se listarán las rutas agregadas manualmente, seleccionar la ruta que se desea eliminar y hacer clic en el botón REMOVE. Si la ruta es dinámica es decir que ha sido aprendida por protocolos de ruteo como RIP u OSPF es necesario agregar una ruta estática que la reemplace.

Para agregar nuevas rutas por el método gráfico debe hacer clic en la pestaña ADD en donde se debe llenar los siguientes datos:

1. Red de destino
2. Máscara de subred
3. Próximo Salto

Una vez que se han llenado los campos hacer clic en el botón Add.

Vía Consola de administración por comandos:

Conectarse por telnet al dispositivo mediante una ventana de D.O.S o un gestor de telnet.

Ej: telnet 192.168.238.245

Cuando el equipo responde se presentará una pantalla solicitando la autenticación.

Una vez dentro es necesario ingresar a modo configuración digitando el comando ***system*** lo que cambiará el inicio de línea de $ a # indicando que se pueden realizar configuraciones sobre el equipo.

Para revisar la configuración del equipo utilizar el comando ***display current configuration.***

Para eliminar rutas estáticas que se encuentren creadas digitar el siguiente comando

No ip route-static (dirección de red) (mascara de subred) (gateway)
Ej:
No ip route static 192.168.34.0 255.255.255.0 192.168.238.124

Para añadir una nueva ruta estática digitar el siguiente comando

ip route-static (dirección de red) (mascara de subred) (gateway)

Ej:

ip route static 192.168.34.0 255.255.255.0 192.168.238.124

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 Farmaenlace.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[22] 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 el parámetro (***-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 Farmaenlace.com en lo que se denomina listas negras; para solventar este inconveniente es necesario ingresar a las páginas de administración de Listas

[22] SSH: **S**ecure **SH**ell, en español: intérprete de órdenes segura

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.

Si ha dado de baja de los listados sospechosos, se debe esperar un tiempo prudencial de replicación a las demás entidades reguladoras, para que el dominio quede totalmente libre y vuelva a su funcionamiento normal.

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 el envió en pendiente por un lapso aproximado de dos horas, si al pasar este tiempo aun 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 realiza conectándose 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.

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, localizar su similar en los respaldos y proceder a reemplazarlo en el archivo original.

Una vez realizado el reemplazo es necesario realizar un reinicio del servicio para verificar que vuelva a operar correctamente.

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 recuperar la 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 Farmaenlace.
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 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 Telnet SSH 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.

Una vez realizado el reemplazo es necesario realizar un reinicio del servicio para verificar que vuelva a operar correctamente.

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 recuperar la 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 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 Farmaenlace.

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 Farmaenlace Cía. Ltda. 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 Farmaenlace 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.

Si la actualización va a realizarse en horario normal de labores, se debe comunicar al todo el personal que tiene acceso a los sistemas que van a ser afectados indicándoles la caída programada del servicio y el tiempo aproximado de restablecimiento del mismo, recomendándoles que si es necesario guarden todos los cambios realizados hasta el momento y cierren los sistemas hasta nueva orden.

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; hasta asegurarse 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.

Es función del personal de administración de sistemas el constante monitoreo y verificación de estado de los servidores para detectar posibles fallas de nivel físico.

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 configuración con los más actuales obtenidos en los respaldos de información.
3. Colocar en funcionamiento el servidor de reemplazo y notificar a los usuarios para que continuen 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 funcionamiento 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 Farmaenlace se mantiene un sistema de almacenamiento de información basado en un equipo Storage que tiene una capacidad aproximada de 3 TB[23] y está configurado en varios LUN[24]s 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 mas pronta 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.

[23] TB: TeraByte
[24] LUN: Logical Unit

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.

Los errores de configuración pueden únicamente presentarse cuando el personal ingrese a realizar manipulación de la configuración del Storage, por lo que el personal que realice esta configuración debe ser calificado y tener en cuenta cada movimiento realizado en el momento que está configurando el Storage, para que si comete un error pueda reversarlo de la manera más rápida posible; se recomienda siempre que se realice un trabajo de mantenimiento y configuración, realizarlo con el mayor cuidado y documentar detalladamente todos los procesos antes de efectuar cualquier cambio.

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.

Si no es posible restaurar las bases de datos en el servidor de producción, se procederá a preparar un servidor de respaldo con capacidad de almacenamiento suficiente para soportar las bases de datos afectadas.

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.

El tiempo de suspensión de los sistemas dependerá enteramente del tiempo que se tarde la restauración completa de la base de datos.

Se recomienda que luego de una restauración de base de datos, se ejecuten planes de mantenimiento de regeneración de índices y actualización de estadísticas para recuperar el rendimiento normal de la base de datos.

5.10.6 Plan de recuperación en caso de desastres

El peor de los casos que puede presentarse durante la vida útil de un DataCenter, es estar expuesto a un desastre que afecte el funcionamiento de manera total de toda el área que corresponde a esta importante zona, los posibles eventos pueden ir desde un desastre natural como un terremoto por ejemplo, hasta un atentado de carácter criminal o bélico, son panoramas bastante desalentadores y en muchos de los casos muy poco probables que lleguen a presentarse; pero aun así es necesario dentro de las guías de contingencia, que se tome en cuenta que pueden ocurrir y documentar los pasos a seguir para lograr recuperar el funcionamiento de todos los servicios del DataCenter; sea en el mismo lugar o un una zona alterna, siempre tomando en cuenta que los servicios no pueden estar sin operar demasiado tiempo, ya que ese riesgo representa pérdidas importantes en ingresos para la empresa y sobre todo en la imagen corporativa que esta proyecta al mercado.

Los planes de Recuperación de Desastres se han tornado cada vez más importantes a medida que las tecnologías de información han ganado importancia en el desarrollo y soporte de los procesos del negocio. Una creciente conciencia lograda muchas veces a partir de experiencias desafortunadas, se ha estado desarrollando sobre el impacto del mal funcionamiento de los sistemas informáticos. Este puede limitar severamente la capacidad de proveer servicios y productos, afectando a las ventas, la satisfacción del cliente, el comportamiento de los accionistas, las relaciones públicas y la imagen corporativa, y dañando por consiguiente la rentabilidad. Los planes de Recuperación de Desastres

permiten identificar los procesos y funciones críticas a partir de las estrategias del negocio y analizarlos en términos de sus riesgos potenciales.

Entre las posibles causas que afectan la normal actividad de una empresa son:

1. Desastres Naturales
2. Huelgas
3. Fallas de energía
4. Sabotajes
5. Amenazas de bomba

El objetivo principal de un plan de recuperación de desastres o DRP por sus siglas en inglés, es minimizar el impacto que tendría una interrupción no planeada de los servicios que presta el área de Sistemas, hacia los usuarios internos y externos de FARMAENLACE y puntos de venta, planificando la reconstrucción de los equipos y/o información requerida para continuar con las operaciones del negocio.

Es necesario utilizar un sitio de respaldo alterno tomando en cuenta además la Infraestructura de redes Lan y Wan, restableciendo las operaciones de una manera rápida, planificada y eficiente, teniendo presente que un Plan de Contingencias no duplica un ambiente normal de negocios, proveyendo además de servicios principales de operación.

Para esto se plantea el siguiente escenario:

DATA CENTER DE FARMAENLACE QUITO APAGADO

Se declara la Contingencia en el Data Center de las oficinas de FARMAENLACE Quito, mismo que está brindando servicio de acceso y utilización de los recursos tecnológicos hacia los usuarios internos y externos de FARMAENLACE y puntos de venta, para lo cual el servidor de Dominio, de Base de Datos, de correo electrónico, Web, de aplicaciones, y antivirus, deberán ser apagados y los usuarios que tienen acceso a estos equipos no podrán acceder a ninguno de estos servicios sino hasta que el personal de Administración de Sistemas comunique que el sitio de Respaldo está habilitado y listo para trabajar.

El sitio de contingencia donde se levantará un DataCenter emergente será las oficinas de Farmaenlace ubicadas en la ciudad de Ibarra, ciertos usuarios deberán trasladarse a las oficinas de FARMAENLACE en Ibarra, con el fin de procesar la información correspondiente del negocio.

Las personas que deben movilizarse a FARMAENLACE en Ibarra son:

1. Coordinador de Servicios Redes y Telecomunicaciones
2. Tecnicos de servicios, redes y telecomunicaciones
3. Lineamientos Estratégicos De La Contingencia

El procedimiento a seguir para declarar la contingencia en FARMAENLACE Quito es:

La persona que hará coordinación del D.R.P. en FARMAENLACE Ibarra es el coordinador encargado de Farmaenlace Ibarra, quien deberá notificar internamente el inicio de la contingencia y hacer los arreglos respectivos para recibir al personal designado para efectuar la recuperación.

Responsabilidades de Farmaenlace Ibarra:

Para la implementación de Servicios del Centro de Recuperación FARMAENLACE IBARRA.

a) FARMAENLACE Ibarra proporcionará un esquema de seguridad que garantice la confidencialidad de la información.

b) El Centro de Recuperación dispondrá de un mobiliario flexible y práctico de instalar, para poder disponer del mismo en un tiempo menor a 24 horas.

c) Para todo tipo de contingencia, FARMAENLACE Ibarra suministrará la configuración de hardware requerida.

d) El personal de seguridad deberá estar atento a los lineamientos requeridos, como: registro de entradas y salidas del personal de FARMAENLACE QUITO, registro de cualquier artículo eléctrico o electrónico que ingrese o salga de las oficinas, entre otros.

Responsabilidades de FARMAENLACE QUITO

a) Proporcionar al coordinador del D.R.P. de FARMAENLACE Ibarra un listado de las personas que requieran ingresar al CENTRO DE RECUPERACIÓN, para poder otorgarles la autorización correspondiente.

b) Solicitar al personal movilizado al Centro de Recuperación, registrar la entrada y salida, con un registro que deberá llevar el personal de Seguridad.

c) Registrar cualquier artículo eléctrico o electrónico ante el personal de Seguridad para evitar inconvenientes en el momento de retirarlos.

d) Proveer y responsabilizarse de los medios magnéticos necesarios para la recuperación y respaldo de su información durante el período de contingencia.

e) Durante el período de contingencia, el coordinador de recuperación y/o su delegado de FARMAENLACE QUITO es el responsable de todas aquellas actividades a desarrollar en el Centro DE RECUPERACIÓN DE FARMAENLACE IBARRA para la recuperación de la información y de los procesos críticos, así como también de la seguridad e integridad de esa información.

f) Las aplicaciones desarrolladas por terceros, que tengan requerimientos específicos y restringidos, como es el caso del número de serie que permite validar las respectivas licencias, el coordinador de recuperación y/o su delegado de FARMAENLACE QUITO se contactará con los respectivos proveedores para que les ofrezcan una solución al respecto.

Instructivo Para Comunicar La Declaración De La Contingencia

a) FARMAENLACE QUITO deberá notificar telefónicamente a FARMAENLACE IBARRA que se ha declarado en contingencia.

b) El coordinador de recuperación de FARMAENLACE QUITO debe especificar que su llamada es para declarar la contingencia.

c) El coordinador de recuperación de FARMAENLACE QUITO debe suministrar al coordinador de D.R.P. de FARMAENLACE IBARRA, la siguiente información:

    a. Nombre de quién realiza la llamada.

b. Número de teléfono para mantener contacto

d) Motivo de Contingencia, esta información debe ser breve y concreta (Ej: por erupción del volcán Pichincha, por incendio de las instalaciones del centro de cómputo, entre otros).

e) La Coordinadora de Recuperación de FARMAENLACE IBARRA debe autorizar el inicio del proceso de contingencia y coordinar el operativo acorde lineamientos establecidos.

f) Posteriormente el Coordinador de Recuperación de FARMAENLACE QUITO deberá ratificar por escrito su respectiva declaración de contingencia al coordinador de D.R.P. de FARMAENLACE Ibarra.

Responsabilidades

El COORDINADOR DE RECUPERACIÓN FARMAENLACE QUITO (Gerente de Sistemas) debe:

a) Coordinar con el Vicepresidente Financiero Administrativo, la declaración de la contingencia.

b) Coordinar todas las operaciones desde el sitio de respaldo.

c) Informar a las oficinas de FARMAENLACE en Ibarra sobre la declaración de la contingencia.

d) Comunicar al personal de FARMAENLACE el nuevo sitio de respaldo para entradas de datos.

e) Solicitar a los responsables de ejecutar los procesos manuales de contingencia que actúen de acuerdo a los procedimientos establecidos para el caso.

f) Evaluar el daño y el grado del desastre.

g) Notificar la emergencia a los miembros del grupo. Ver ANEXO No.2 "NOTIFICACION DE LA CONTINGENCIA AL GRUPO DE D.R.P.".

h) Notificar al Staff de FARMAENLACE del problema suscitado, y estimar el tiempo que quedará fuera de servicio el sistema y si es necesario una

prolongación del mismo de acuerdo a carta formato. Ver ANEXO No.3 "NOTIFICACION DE LA CONTIGENCIA AL STAFF DE FARMAENLACE".

i) Dirigir las operaciones de recuperación.

j) Establecer viajes del personal para la operación en el sitio de respaldo.

k) Obtener la autorización debida para el ingreso a los sitios de respaldo y el horario respectivo.

l) Proveer el dinero para los gastos necesarios con autorización del Vicepresidente Administrativo Financiero.

m) Proveer de informes continuos al Vicepresidente Administrativo Financiero.

n) Coordinar la restauración al proceso normal.

o) Efectuar simulacros en los sitios de respaldo.

El COORDINADOR DE RECUPERACIÓN FARMAENLACE IBARRA tiene las siguientes responsabilidades

a) Recibir del Coordinador de recuperación FARMAENLACE QUITO, la declaración de la contingencia.

b) Coordinar todas las operaciones desde el sitio de respaldo.

c) Informar a las oficinas de FARMAENLACE en Ibarra sobre la declaración de la contingencia.

d) Solicitar a los responsables de ejecutar los procesos manuales de contingencia que actúen de acuerdo a los procedimientos establecidos para el caso.

e) Notificar la emergencia a los miembros del grupo. Ver ANEXO No.2 "NOTIFICACION DE LA CONTINGENCIA AL GRUPO DE D.R.P.".

f) Apoyar al coordinador de recuperación FARMAENLACE QUITO en las operaciones de recuperación.

g) Coordinar la restauración al proceso normal.

h) Efectuar simulacros en los sitios de respaldo.

El COORDINADOR DE SERVICIOS DE REDES Y TELECOMUNICACIONES debe:

a) Proveerse de equipo alterno de comunicaciones de acuerdo a contrato firmado con un proveedor de telecomunicaciones.

b) Mantener actualizado el listado de proveedores de telecomunicaciones.

c) Disponer de los procedimientos impresos para instalación del servidor de Dominio, de Base de Datos, de correo electrónico, Web, de aplicaciones, y antivirus .

d) Disponer del software necesario para realizar la instalación del servidor de Dominio, de Base de Datos, de correo electrónico, Web, de aplicaciones, y antivirus.

e) Traslado al sitio de contingencia de los backups de los servidores de Dominio, de Base de Datos, de correo electrónico, Web, de aplicaciones, de taller y antivirus.

f) Instalar y configurar las estaciones de trabajo necesarias para la contingencia.

El Procedimiento para iniciar el plan es el siguiente:

a) Ante una contingencia, el primer paso a realizar es la notificación al grupo de D.R.P. y de esta manera ejecutar el Plan de Contingencia.

b) En el caso de no existir personal trabajando en FARMAENLACE QUITO, la notificación la hará el guardia de seguridad de turno, comunicándose al número de celular del Coordinador de Recuperación, mismo que se comunicará con el Vicepresidente Financiero Administrativo para informar lo que está sucediendo, a fin de que se defina si es o no necesaria la declaración de la contingencia.

c) Se evaluará por parte del Coordinador de Recuperación o su alterno, el daño y se estimará el tiempo en el que los servicios estarán fuera de servicio.

d) El Coordinador de recuperación, tomará las siguientes acciones:

e) Notificar vía telefónica, personalmente o por escrito al Vicepresidente Financiero Administrativo que se ha declarado la contingencia y que la recuperación ha sido iniciada.

f) Notificará a los usuarios que el servicio se ha interrumpido.

g) Verificar que los Coordinadores de Servicios Redes y Telecomunicaciones y el de Operaciones Soporte y Mantenimiento se encuentren revisando prioridades de ejecución para aquellos trabajos que sean críticos al momento y que permitan ejecutar un plan de acción establecido.

h) Verificar la recuperación de la información destruida, así como el mecanismo para restablecer el servicio en condiciones normales.

i) Verificar que el Centro de Cómputo vuelva a su normalidad una vez pasada la contingencia.

j) Coordinar el uso de sitios de respaldos mediante acuerdos, de existir.

k) El grupo de recuperación deberá seguir los siguientes pasos:

l) Evacuar los trabajos que estuvieron ejecutándose al momento del desastre.

m) Iniciar la recuperación total del computador original para reanudar el normal funcionamiento.

n) Decidir la posibilidad de extender o no el uso de los sitios de respaldo, hasta que el computador esté reparado en su totalidad.

o) Decidir las Aplicaciones a Restaurar.

p) Proveer de los suministros necesarios a cada uno de los sitios de respaldo.

CAPÍTULO 6

6 CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Luego de la finalización del presente proyecto se concluye:

Se ha diseñado e implementado una infraestructura tecnológica en el DataCenter de Farmaenlace Cia. Ltda. que cubre las necesidades de la empresa en su estado actual.

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 (Clean Agent).

Se tuvo la dificultad para la implementación de piso elevado o piso técnico debido a la altitud de la estructura del edificio de Farmaenlace 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 provocarán 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 además 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 Farmaenlace es considerado de nivel 1, aún queda mucho trabajo por hacer para que el DataCenter de Farmaenlace 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 y el proyecto de Farmaenlace seguirá implementándose conforme la empresa continúe en su acelerado crecimiento.

Todo el proceso de implementación del presente proyecto ha sido un constante aprendizaje y experiencia enriquecedora que será aprovechada en el futuro desempeño de mis labores dentro o fuera de esta prestigiosa empresa.

6.2 Recomendaciones

Se recomienda seguir las normas establecidas para DataCenter para las futuras adecuaciones o mejoras que se planeen hacer al DataCenter de Farmaenlace 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 una actualización del cableado estructurado del edificio por lo menos a categoría 6ª, ya que la tecnología de cableado 5e que posee el edificio principal ha terminado su vida útil y hay nuevas opciones de cableado estructurado que permiten más y mejores niveles de transmisión de datos.

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 correcto aprovechamiento de los recursos que Farmaenlace 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 Farmaenlace 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 Farmaenlace, así como también dar de baja aquellos equipos que ya han cumplido su vida útil dentro de los servidores de Farmaenlace

Bibliografía

3Com. (Junio de 2010). *3com Networking*. Recuperado el Agosto de 2011, de http://lat.3com.com/lat/jump_page/lat_5500.html

Cisco. (2005). *Cisco Networking Academy Program CCNA.* Cisco.

DataCenter Consultores. (Mayo de 2011). *DataCenter Consultores*. Recuperado el Julio de 2011, de http://www.datacenterconsultores.com/calculadora/

Holem, D., & Thomas, O. (2006). *Managing and Mantaining a Microsoft windows server 2003 Environment.* Washington: Microsoft Press.

HP. (Mayo de 2011). *HP BladeSystem c3000 Enclosure* -. Recuperado el Mayo de 2012, de http://h18004.www1.hp.com/products/blades/components/enclosures/c-class/c3000/

IEEE-803.3. (2002). *IEEE 802.3: LOCAL AND METROPOLITAN AREA NETWORK STANDARDS.* IEE Standards Asociation.

Infiesta Saborit, J. (Enero de 2008). *Fabila*. Recuperado el Agosto de 2011, de Fibras Monomodo: http://www.fabila.com/noticia.asp?id=667

Liebert Corporation. (Julio de 2010). *Emerson Network Power.* Recuperado el Agosto de 2011, de http://www.emersonnetworkpower.com/es-CALA/pages/default.aspx

NFPA. (2001). *Standard on clean Agent Fire Extinguishing Systems.*

Norwood, S. (2007). *Guía paso a paso para una introducción a Microsoft Windows Server Update Services 3.0.* Microsoft Press.

Oramas Bustillos, R. (08 de Octubre de 2010). *Profesor Java*. Recuperado el Agosto de 2011, de http://profejavaoramas.blogspot.com/2010/10/computacion-cliente-servidor.html

Polchowski, D. (2003). *Administracion Microsoft windows 2003.* Recuperado el Julio de 2011, de http://www.microsoft.com/latam/technet

Siemon. (2008). *DataCenter Ebook.* Recuperado el Julio de 2011, de http://www.siemon.com

Tanenbaum, A. S. (2003). *Redes de Computadoras.* Pearson Educación.

TIA-942. (2005). *Estándar TIA-942 Telecommunications Infrastructure Standard for Data Centers.* Arlington: TELECOMMUNICATIONS INDUSTRY ASSOCIATION.

Wikipedia. (Junio de 2011). *Wikipedia - Fibra Optica.* Recuperado el Febrero de 2012, de https://es.wikipedia.org/wiki/Fibra_%C3%B3ptica

yio.com.ar. (Noviembre de 2007). *Fibras Ópticas*. Recuperado el Agosto de 2011, de http://www.yio.com.ar/fo/empalmes.html

Anexos

ANSI/TIA-942-2005
Approved: April 12, 2005

TIA STANDARD

Telecommunications Infrastructure Standard for Data Centers

TIA-942

April 2005

TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Representing the telecommunications industry in association with the Electronic Industries Alliance

NOTICE

TIA Engineering Standards and Publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for their particular need. The existence of such Standards and Publications shall not in any respect preclude any member or non-member of TIA from manufacturing or selling products not conforming to such Standards and Publications. Neither shall the existence of such Standards and Publications preclude their voluntary use by Non-TIA members, either domestically or internationally.

Standards and Publications are adopted by TIA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, TIA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(From Standards Proposal No. 3-0092-C-1, formulated under the cognizance of the TIA TR-42.1, Subcommittee on Commercial Building Telecommunications Cabling).

Published by

©TELECOMMUNICATIONS INDUSTRY ASSOCIATION
Standards and Technology Department
2500 Wilson Boulevard
Arlington, VA 22201 U.S.A.

PRICE: Please refer to current Catalog of
TIA TELECOMMUNICATIONS INDUSTRY ASSOCIATION STANDARDS AND ENGINEERING PUBLICATIONS
or call Global Engineering Documents, USA and Canada
(1-800-854-7179) International (303-397-7956)
or search online at http://www.tiaonline.org/standards/search_n_order.cfm

NOTICE OF DISCLAIMER AND LIMITATION OF LIABILITY

The document to which this Notice is affixed (the "Document") has been prepared by one or more Engineering Committees or Formulating Groups of the Telecommunications Industry Association ("TIA"). TIA is not the author of the Document contents, but publishes and claims copyright to the Document pursuant to licenses and permission granted by the authors of the contents.

TIA Engineering Committees and Formulating Groups are expected to conduct their affairs in accordance with the TIA Engineering Manual ("Manual"), the current and predecessor versions of which are available at http://www.tiaonline.org/standards/sfg/engineering_manual.cfm. TIA's function is to administer the process, but not the content, of document preparation in accordance with the Manual and, when appropriate, the policies and procedures of the American National Standards Institute ("ANSI"). TIA does not evaluate, test, verify or investigate the information, accuracy, soundness, or credibility of the contents of the Document. In publishing the Document, TIA disclaims any undertaking to perform any duty owed to or for anyone.

If the Document is identified or marked as a project number (PN) document, or as a standards proposal (SP) document, persons or parties reading or in any way interested in the Document are cautioned that: (a) the Document is a proposal; (b) there is no assurance that the Document will be approved by any Committee of TIA or any other body in its present or any other form; (c) the Document may be amended, modified or changed in the standards development or any editing process.

The use or practice of contents of this Document may involve the use of intellectual property rights ("IPR"), including pending or issued patents, or copyrights, owned by one or more parties. TIA makes no search or investigation for IPR. When IPR consisting of patents and published pending patent applications are claimed and called to TIA's attention, a statement from the holder thereof is requested, all in accordance with the Manual. TIA takes no position with reference to, and disclaims any obligation to investigate or inquire into, the scope or validity of any claims of IPR. TIA will neither be a party to discussions of any licensing terms or conditions, which are instead left to the parties involved, nor will TIA opine or judge whether proposed licensing terms or conditions are reasonable or non-discriminatory. TIA does not warrant or represent that procedures or practices suggested or provided in the Manual have been complied with as respects the Document or its contents.

TIA does not enforce or monitor compliance with the contents of the Document. TIA does not certify, inspect, test or otherwise investigate products, designs or services or any claims of compliance with the contents of the Document.

ALL WARRANTIES, EXPRESS OR IMPLIED, ARE DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY AND ALL WARRANTIES CONCERNING THE ACCURACY OF THE CONTENTS, ITS FITNESS OR APPROPRIATENESS FOR A PARTICULAR PURPOSE OR USE, ITS MERCHANTABILITY AND ITS NON-INFRINGEMENT OF ANY THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS. TIA EXPRESSLY DISCLAIMS ANY AND ALL RESPONSIBILITIES FOR THE ACCURACY OF THE CONTENTS AND MAKES NO REPRESENTATIONS OR WARRANTIES REGARDING THE CONTENT'S COMPLIANCE WITH ANY APPLICABLE STATUTE, RULE OR REGULATION, OR THE SAFETY OR HEALTH EFFECTS OF THE CONTENTS OR ANY PRODUCT OR SERVICE REFERRED TO IN THE DOCUMENT OR PRODUCED OR RENDERED TO COMPLY WITH THE CONTENTS.

TIA SHALL NOT BE LIABLE FOR ANY AND ALL DAMAGES, DIRECT OR INDIRECT, ARISING FROM OR RELATING TO ANY USE OF THE CONTENTS CONTAINED HEREIN, INCLUDING WITHOUT LIMITATION ANY AND ALL INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, LITIGATION, OR THE LIKE), WHETHER BASED UPON BREACH OF CONTRACT, BREACH OF WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING NEGATION OF DAMAGES IS A FUNDAMENTAL ELEMENT OF THE USE OF THE CONTENTS HEREOF, AND THESE CONTENTS WOULD NOT BE PUBLISHED BY TIA WITHOUT SUCH LIMITATIONS.

Telecommunications Infrastructure Standard for Data Centers

Table of Contents

List of figures

List of tables

FOREWORD

(This foreword is not considered part of this Standard.)

Approval of this Standard

This Standard was approved by the Telecommunications Industry Association (TIA) Subcommittee TR 42.2, TIA Technical Engineering Committee TR 42, and the American National Standards Institute (ANSI).

TIA reviews standards every 5 years. At that time, standards are reaffirmed, rescinded, or revised according to the submitted updates. Updates to be included in the next revision of this Standard should be sent to the committee chair or to TIA.

Contributing organizations

More than 60 organizations within the telecommunications industry contributed their expertise to the development of this Standard (including manufacturers, consultants, end users, and other organizations).

The TR-42 Committee contains the following subcommittees that are related to this activity.

- TR-42.1 - Subcommittee on Commercial Building Telecommunications Cabling
- TR-42.2 - Subcommittee on Residential Telecommunications Infrastructure
- TR-42.3 - Subcommittee on Commercial Building Telecommunications Pathways and Spaces
- TR-42.4 - Subcommittee on Outside Plant Telecommunications Infrastructure
- TR-42.5 - Subcommittee on Telecommunications Infrastructure Terms and Symbols
- TR-42.6 - Subcommittee on Telecommunications Infrastructure and Equipment Administration
- TR-42.7 - Subcommittee on Telecommunications Copper Cabling Systems
- TR-42.8 - Subcommittee on Telecommunications Optical Fiber Cabling Systems
- TR-42.9 - Subcommittee on Industrial Telecommunications Infrastructure

Documents superseded

This Standard is the first edition.

Relationship to other TIA standards and documents

The specifications and recommendations of this Standard will take precedence for use in data centers.

- ANSI/TIA/EIA-568-B.1, *Commercial Building Telecommunications Cabling Standard; Part 1 General Requirements*

- ANSI/TIA/EIA-568-B.2, *Commercial Building Telecommunications Cabling Standard; Part 2 Balanced Twisted-Pair Cabling Components*
- ANSI/TIA/EIA-568-B.3, *Optical Fiber Cabling Components Standard*
- ANSI/TIA-569-B, *Commercial Building Standard for Telecommunications Pathways and Spaces*
- ANSI/TIA/EIA-606-A, *Administration Standard for Commercial Telecommunications Infrastructure*
- ANSI/TIA/EIA-J-STD-607, *Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications*
- ANSI/TIA-758-A, *Customer-Owned Outside Plant Telecommunications Cabling Standard*

This Standard contains references to national and international standards as well as other documents when appropriate.

- National Electrical Safety Code (NESC)

  (IEEE C 2)

- Life Safety Code (NEC)

  (NFPA 101)

- National Electrical Code (NEC)

  (NFPA 70)

- Standard for the Protection of Information Technology Equipment

  (NFPA 75)

- Engineering Requirements for a Universal Telecommunications Frame

  (ANSI T1.336)

- Recommended Practice for Powering and Grounding Electronic Equipment

  (IEEE Std. 1100)

- Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications

  (IEEE Std. 446)

- Telcordia specifications

  (GR-63-CORE (NEBS)) and (GR-139-CORE)

- ASHRAE

In Canada, the National Building Code, the National Fire Code, Canadian Electrical Code (CSA CEC C22.1), and other documents including CAN/ULC S524, CAN/ULC S531 may be used for cross-reference to NFPA 72, NFPA 70 section 725-8 and section 725-54.

Useful supplements to this Standard are the Building Industry Consulting Service International (BICSI) *Telecommunications Distribution Methods Manual,* the *Customer-owned Outside Plant Design Manual,* and the *Telecommunications Cabling Installation Manua*l. These manuals provide recommended practices and methods by which many of the requirements of this Standard may be implemented.

Other references are listed in annex I.

Annexes A, B, C, D, E, F, G and H are informative and not considered to be requirements of this Standard except when specifically referenced within the main document.

Purpose of this Standard

The purpose of this Standard is to provide requirements and guidelines for the design and installation of a data center or computer room. It is intended for use by designers who need a comprehensive understanding of the data center design including the facility planning, the cabling system, and the network design. The standard will enable the data center design to be considered early in the building development process, contributing to the architectural considerations, by providing information that cuts across the multidisciplinary design efforts; promoting cooperation in the design and construction phases. Adequate planning during building construction or renovation is significantly less expensive and less disruptive than after the facility is operational. Data centers in particular can benefit from infrastructure that is planned in advance to support growth and changes in the computer systems that the data centers are designed to support.

This document in particular, presents an infrastructure topology for accessing and connecting the respective elements in the various cabling system configurations currently found in the data center environment. In order to determine the performance requirements of a generic cabling system, various telecommunications services and applications were considered. In addition, this document addresses the floor layout topology related to achieving the proper balance between security, rack density and manageability.

The standard specifies a generic telecommunications cabling system for the data center and related facilities whose primary function is information technology. Such application spaces may be dedicated to a private company or institution, or occupied by one or more service providers to host Internet connections, and data storage devices.

Data centers support a wide range of transmission protocols. Some of these transmission protocols impose distance restrictions that are shorter than those imposed by this Standard. When applying specific transmission protocols, consult standards, regulations, equipment vendors, and system service suppliers for applicability, limitations, and ancillary requirements. Consider consolidating standardized and proprietary cabling into a single structured cabling system.

Data centers can be categorized according to whether they serve the private domain (“enterprise” data centers) or the public domain (internet data centers, co-location data centers, and other service provider data centers). Enterprise facilities include private corporations, institutions or government agencies, and may involve the establishment of either intranets or extranets. Internet facilities include traditional telephone service providers, unregulated competitive service providers

and related commercial operators. The topologies proposed in this document, however, are intended to be applicable to both in satisfying their respective requirements for connectivity (internet access and wide-area communications), operational hosting (web hosting, file storage and backup, database management, etc.), and additional services (application hosting, content distribution, etc.). Failsafe power, environmental controls and fire suppression, and system redundancy and security are also common requirements to facilities that serve both the private and public domain.

Specification of criteria

Two categories of criteria are specified; mandatory and advisory. The mandatory requirements are designated by the word “shall”; advisory requirements are designated by the words “should”, “may” or “desirable” which are used interchangeably in this Standard.

Mandatory criteria generally apply to protection, performance, administration and compatibility; they specify the absolute minimum acceptable requirements. Advisory or desirable criteria are presented when their attainment will enhance the general performance of the cabling system in all its contemplated applications. A note in the text, table, or figure is used for emphasis or for offering informative suggestions.

Metric equivalents of US customary units

The majority of dimensions in this Standard are metric. Soft conversions from metric to US customary units are provided in parenthesis; e.g., 103 millimeters (4 inches).

Life of this Standard

This Standard is a living document. The criteria contained in this Standard are subject to revisions and updating as warranted by advances in building construction techniques and telecommunications technology.

1 SCOPE

1.1 General

This Standard specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms including single tenant enterprise data centers and multi-tenant Internet hosting data centers. The topology proposed in this document is intended to be applicable to any size data center.

1.2 Normative references

The following standard contains provisions that, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards published by them.

- ANSI/TIA/EIA-568-B.1-2001, *Commercial Building Telecommunications Cabling Standard: Part 1: General Requirements;*
- ANSI/TIA/EIA-568-B.2-2001, *Commercial Building Telecommunications Cabling Standard: Part 2: Balanced Twisted-Pair Cabling Components;*
- ANSI/TIA/EIA-568.B.3-2000, *Optical Fiber Cabling Components Standard;*
- ANSI/TIA-569-B, *Commercial Building Standard for Telecommunications Pathways and Spaces;*
- ANSI/TIA/EIA-606-A-2002, *Administration Standard for Commercial Telecommunications Infrastructure;*
- ANSI/TIA/EIA-J-STD-607-2001, *Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications;*
- ANSI/TIA-758-A, *Customer-Owned Outside Plant Telecommunications Cabling Standard;*
- ANSI/NFPA 70-2002, *National Electrical Code;*
- ANSI/NFPA 75-2003*, Standard for the protection of information technology equipment;*
- ANSI T1.336*, Engineering requirements for a universal telecommunications frame;*
- ANSI T1.404, *Network and customer installation interfaces – DS3 and metallic interface specification;*
- ASHRAE, *Thermal Guidelines for Data Processing Environments;*
- Telcordia GR-63-CORE, *NEBS(TM) Requirements: physical protection;*
- Telcordia GR-139-CORE, *Generic requirements for central office coaxial cable;*

2 DEFINITION OF TERMS, ACRONYMS AND ABBREVIATIONS, AND UNITS OF MEASURE

2.1 General

This clause contains the definitions of terms, acronyms, and abbreviations that have special technical meaning or that are unique to the technical content of this Standard. Special definitions that are appropriate to individual technical clauses are also included.

2.2 Definition of terms

The generic definitions in this subclause have been formulated for use by the entire family of telecommunications infrastructure standards. Specific requirements are found in the normative clauses of this Standard. For the purposes of this Standard, the following definitions apply.

access floor: A system consisting of completely removable and interchangeable floor panels that are supported on adjustable pedestals or stringers (or both) to allow access to the area beneath.

access provider: The operator of any facility that is used to convey telecommunications signals to and from a customer premises.

administration: The method for labeling, identification, documentation and usage needed to implement moves, additions and changes of the telecommunications infrastructure.

backbone: 1) A facility (e.g., pathway, cable or conductors) between any of the following spaces: telecommunications rooms, common telecommunications rooms, floor serving terminals, entrance facilities, equipment rooms, and common equipment rooms. 2) in a data center, a facility (e.g. pathway, cable or conductors) between any of the following spaces: entrance rooms or spaces, main distribution areas, horizontal distribution areas, telecommunications rooms.

backbone cable: See **backbone**.

bonding: The permanent joining of metallic parts to form an electrically conductive path that will ensure electrical continuity and the capacity to conduct safely any current likely to be imposed.

cabinet: A container that may enclose connection devices, terminations, apparatus, wiring, and equipment.

cabinet (telecommunications): An enclosure with a hinged cover used for terminating telecommunications cables, wiring and connection devices.

cable: An assembly of one or more insulated conductors or optical fibers, within an enveloping sheath.

cabling: A combination of all cables, jumpers, cords, and connecting hardware.

centralized cabling: A cabling configuration from the work area to a centralized cross-connect using pull through cables, an interconnect, or splice in the telecommunications room.

channel: The end-to-end transmission path between two points at which application-specific equipment is connected.

common equipment room (telecommunications): An enclosed space used for equipment and backbone interconnections for more than one tenant in a building or campus.

computer room: An architectural space whose primary function is to accommodate data processing equipment.

conduit: (1) A raceway of circular cross-section. (2) A structure containing one or more ducts.

connecting hardware: A device providing mechanical cable terminations.

consolidation point: A location for interconnection between horizontal cables extending from building pathways and horizontal cables extending into furniture pathways.

cross-connect: A facility enabling the termination of cable elements and their interconnection or cross-connection.

cross-connection: A connection scheme between cabling runs, subsystems, and equipment using patch cords or jumpers that attach to connecting hardware on each end.

data center: a building or portion of a building whose primary function is to house a computer room and its support areas.

demarcation point: A point where the operational control or ownership changes.

earthing: see grounding

electromagnetic interference: Radiated or conducted electromagnetic energy that has an undesirable effect on electronic equipment or signal transmissions.

entrance room or space (telecommunications): A space in which the joining of inter or intra building telecommunications backbone facilities takes place.

equipment cable; cord: A cable or cable assembly used to connect telecommunications equipment to horizontal or backbone cabling.

equipment distribution area: the computer room space occupied by equipment racks or cabinets.

equipment room (telecommunications): An environmentally controlled centralized space for telecommunications equipment that usually houses a main or intermediate cross-connect.

fiber optic: See **optical fiber**.

ground: A conducting connection, whether intentional or accidental, between an electrical circuit (e.g., telecommunications) or equipment and the earth, or to some conducting body that serves in place of earth.

grounding: The act of creating a ground.

grounding conductor: A conductor used to connect the grounding electrode to the building's main grounding busbar.

horizontal cabling: 1) The cabling between and including the telecommunications outlet/connector and the horizontal cross-connect. 2) The cabling between and including the building automation system outlet or the first mechanical termination of the horizontal connection

point and the horizontal cross-connect. 3) in a data center, horizontal cabling is the cabling from the horizontal cross-connect (in the main distribution area or horizontal distribution area) to the outlet in the equipment distribution area or zone distribution area.

horizontal cross-connect: A cross-connect of horizontal cabling to other cabling, e.g., horizontal, backbone, equipment.

horizontal distribution area: a space in a computer room where a horizontal cross-connect is located.

identifier: An item of information that links a specific element of the telecommunications infrastructure with its corresponding record.

infrastructure (telecommunications): A collection of those telecommunications components, excluding equipment, that together provide the basic support for the distribution of all information within a building or campus.

interconnection: A connection scheme that employs connecting hardware for the direct connection of a cable to another cable without a patch cord or jumper.

intermediate cross-connect: A cross-connect between first level and second level backbone cabling.

jumper: An assembly of twisted-pairs without connectors, used to join telecommunications circuits/links at the cross-connect.

link: A transmission path between two points, not including terminal equipment, work area cables, and equipment cables.

main cross-connect: A cross-connect for first level backbone cables, entrance cables, and equipment cables.

main distribution area: The space in a computer room where the main cross-connect is located**.**

mechanical room: An enclosed space serving the needs of mechanical building systems.

media (telecommunications): Wire, cable, or conductors used for telecommunications.

modular jack: A female telecommunications connector that may be keyed or unkeyed and may have 6 or 8 contact positions, but not all the positions need be equipped with jack contacts.

multimode optical fiber: An optical fiber that carries many paths of light.

multipair cable: A cable having more than four pairs.

optical fiber: Any filament made of dielectric materials that guides light.

optical fiber cable: An assembly consisting of one or more optical fibers.

patch cord: A length of cable with a plug on one or both ends.

patch panel: A connecting hardware system that facilitates cable termination and cabling administration using patch cords.

pathway: A facility for the placement of telecommunications cable.

plenum: a compartment or chamber to which one or more air ducts are connected and that forms part of the air distribution system.

private branch exchange: A private telecommunications switching system.

pull box: A housing located in a pathway run used to facilitate the placing of wire or cables.

radio frequency interference: Electromagnetic interference within the frequency band for radio transmission.

screen: An element of a cable formed by a shield.

screened twisted-pair (ScTP): A balanced cable with an overall screen.

service provider: The operator of any service that furnishes telecommunications content (transmissions) delivered over access provider facilities.

sheath: See **cable sheath**.

shield: A metallic layer placed around a conductor or group of conductors.

single-mode optical fiber: An optical fiber that carries only one path of light.

singlemode optical fiber: see **single-mode**.

splice: A joining of conductors, meant to be permanent.

star topology: A topology in which telecommunications cables are distributed from a central point.

telecommunications: Any transmission, emission, and reception of signs, signals, writings, images, and sounds, that is, information of any nature by cable, radio, optical, or other electromagnetic systems.

telecommunications entrance point: See **entrance point (telecommunications)**.

telecommunications entrance room or space: See **entrance room or space (telecommunications)**.

telecommunications equipment room: See **equipment room (telecommunications)**.

telecommunications infrastructure: See **infrastructure (telecommunications)**.

telecommunications media: See **media (telecommunications)**.

telecommunications room: An enclosed architectural space for housing telecommunications equipment, cable terminations, and cross-connect cabling.

telecommunications space: See **space (telecommunications)**.

topology: The physical or logical arrangement of a telecommunications system.

uninterruptible power supply: A buffer between utility power or other power source and a load that requires continuous precise power.

wire: An individually insulated solid or stranded metallic conductor.

wireless: The use of radiated electromagnetic energy (e.g., radio frequency and microwave signals, light) traveling through free space to convey information.

zone distribution area: A space in a computer room where a zone outlet or a consolidation point is located

zone outlet: a connecting device in the zone distribution area terminating the horizontal cable enabling equipment cable connections to the equipment distribution area.

2.3 Acronyms and abbreviations

AHJ	authority having jurisdiction
ANSI	American National Standards Institute
AWG	American Wire Gauge
BICSI	Building Industry Consulting Service International
BNC	bayonet Neil-Concelman or bayonet navel connector
CCTV	closed-circuit television
CEC	Canadian Electrical Code, Part I
CER	common equipment room
CPU	central processing unit
CSA	Canadian Standards Association International
DSX	digital signal cross-connect
EDA	equipment distribution area
EIA	Electronic Industries Alliance
EMI	electromagnetic interference
EMS	energy management system
FDDI	fiber distributed data interface
HC	horizontal cross-connect
HDA	horizontal distribution area
HVAC	heating, ventilation and air conditioning
IC	intermediate cross-connect
IDC	insulation displacement contact

LAN	local area network
MC	main cross-connect
MDA	main distribution area
NEC	National Electrical Code
NEMA	National Electrical Manufacturers Association
NEXT	near-end crosstalk
NESC	National Electrical Safety Code
NFPA	National Fire Protection Association
OC	optical carrier
PBX	private branch exchange
PCB	printed circuit board
PDU	power distribution unit
PVC	polyvinyl chloride
RFI	radio frequency interference
RH	relative humidity
SAN	storage area network
ScTP	screened twisted-pair
SDH	synchronous digital hierarchy
SONET	synchronous optical network
STM	synchronous transport model
TIA	Telecommunications Industry Association
TR	telecommunications room
UL	Underwriters Laboratories Inc
UPS	uninterruptible power supply
UTP	unshielded twisted-pair
WAN	wide area network
ZDA	zone distribution area

2.4 Units of measure

A	Ampere
°C	degrees Celsius
°F	degrees Fahrenheit
ft	feet, foot
Gb/s	gigabit per second
Hz	hertz
in	inch
kb/s	kilobit per second
kHz	kilohertz
km	kilometer
kPa	kilopascal
kVA	kilovoltamp
kW	kilowatt
lbf	pound-force
m	meter
Mb/s	megabit per second
MHz	megahertz
mm	millimeter
nm	nanometer
μm	micrometer or micron

3 DATA CENTER DESIGN OVERVIEW

3.1 General

The intent of this subclause is to provide general information on the factors that should be considered when planning the design of a data center. The information and recommendations are intended to enable an effective implementation of a data center design by identifying the appropriate actions to be taken in each step of the planning and design process. The design specific details are provided in the subsequent clauses and annexes.

The steps in the design process described below apply to the design of a new data center or the expansion of an existing data center. It is essential for either case that the design of the telecommunications cabling system, equipment floor plan, electrical plans, architectural plan, HVAC, security, and lighting systems be coordinated. Ideally, the process should be:

a) Estimate equipment telecommunications, space, power, and cooling requirements of the data center at full capacity. Anticipate future telecommunications, power, and cooling trends over the lifetime of the data center.

b) Provide space, power, cooling, security, floor loading, grounding, electrical protection, and other facility requirements to architects and engineers. Provide requirements for operations center, loading dock, storage room, staging areas and other support areas.

c) Coordinate preliminary data center space plans from architect and engineers. Suggest changes as required.

d) Create an equipment floor plan including placement of major rooms and spaces for entrance rooms, main distribution areas, horizontal distribution areas, zone distribution areas and equipment distribution areas. Provide expected power, cooling, and floor loading requirements for equipment to engineers. Provide requirements for telecommunications pathways.

e) Obtain an updated plan from engineers with telecommunications pathways, electrical equipment, and mechanical equipment added to the data center floor plan at full capacity.

f) Design telecommunications cabling system based on the needs of the equipment to be located in the data center.

3.2 Relationship of data center spaces to other building spaces

Figure 1 illustrates the major spaces of a typical data center and how they relate to each other and the spaces outside of the data center. See clause 5 for information concerning the telecommunications spaces within the data center.

This Standard addresses telecommunications infrastructure for the data center spaces, which is the computer room and its associated support spaces.

Telecommunications cabling and spaces outside of the computer room and its associated support spaces are illustrated in figure 1 to demonstrate their relationships to the data center.

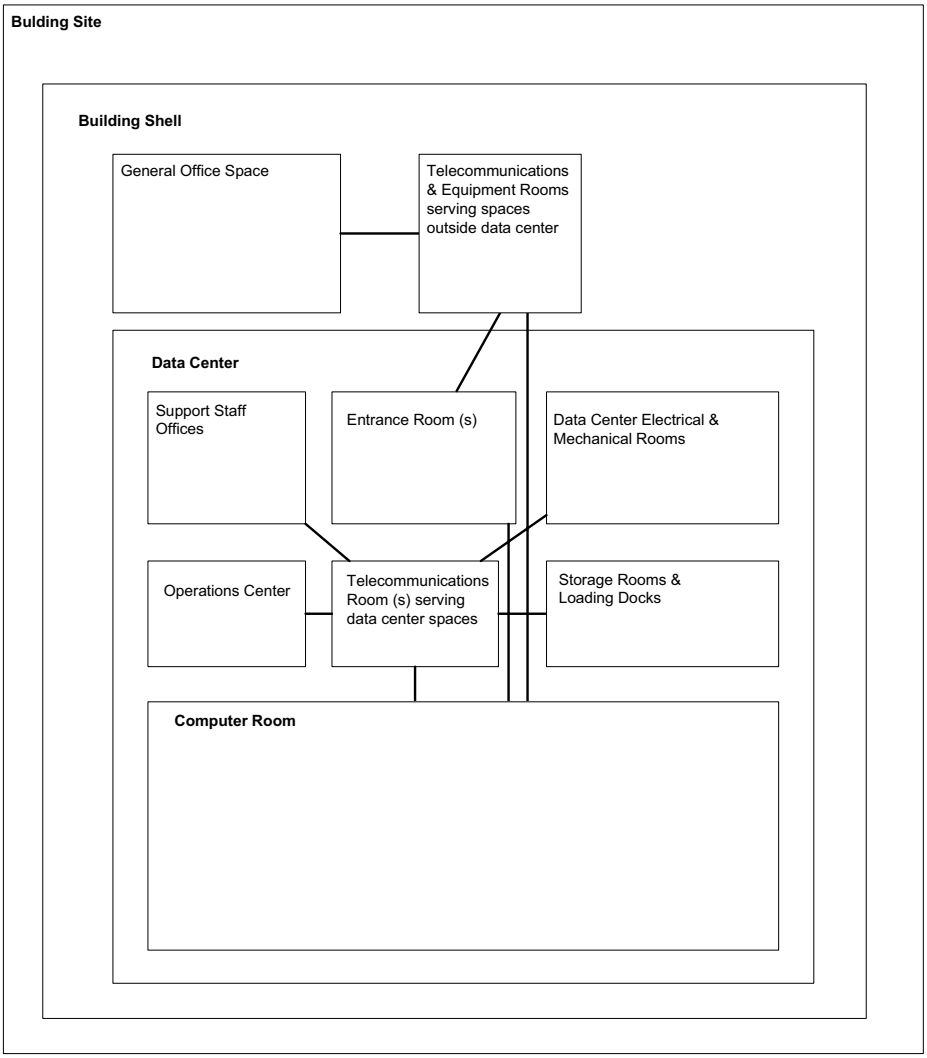


Figure 1: Relationship of spaces in a data center

3.3 Tiering

This Standard includes information for four tiers relating to various levels of availability and security of the data center facility infrastructure. Higher tiers correspond to higher availability and security. Annex G of this Standard provides detailed information for each of the four tiering levels.

3.4 Consideration for involvement of professionals

Data centers are designed to handle the requirements of large quantities of computer and telecommunications equipment. Therefore, telecommunications and information technology professionals and specifiers should be involved in the design of the data center from its inception. In addition to the space, environmental, adjacency, and operational requirements for the computer and telecommunications equipment, data center designs need to address the requirements of the telecommunications pathways and spaces specified in this Standard.

4 DATA CENTER CABLING SYSTEM INFRASTRUCTURE

4.1 The basic elements of the data center cabling system structure

Figure 2 illustrates a representative model for the various functional elements that comprise a cabling system for a data center. It depicts the relationship between the elements and how they are configured to create the total system.

The basic elements of the data center cabling system structure are the following:

a) Horizontal cabling (subclause 6.2)

b) Backbone cabling (subclause 6.3)

c) Cross-connect in the entrance room or main distribution area

d) Main cross-connect (MC) in the main distribution area

e) Horizontal cross-connect (HC) in the telecommunications room, horizontal distribution area or main distribution area.

f) Zone outlet or consolidation point in the zone distribution area

g) Outlet in the equipment distribution area

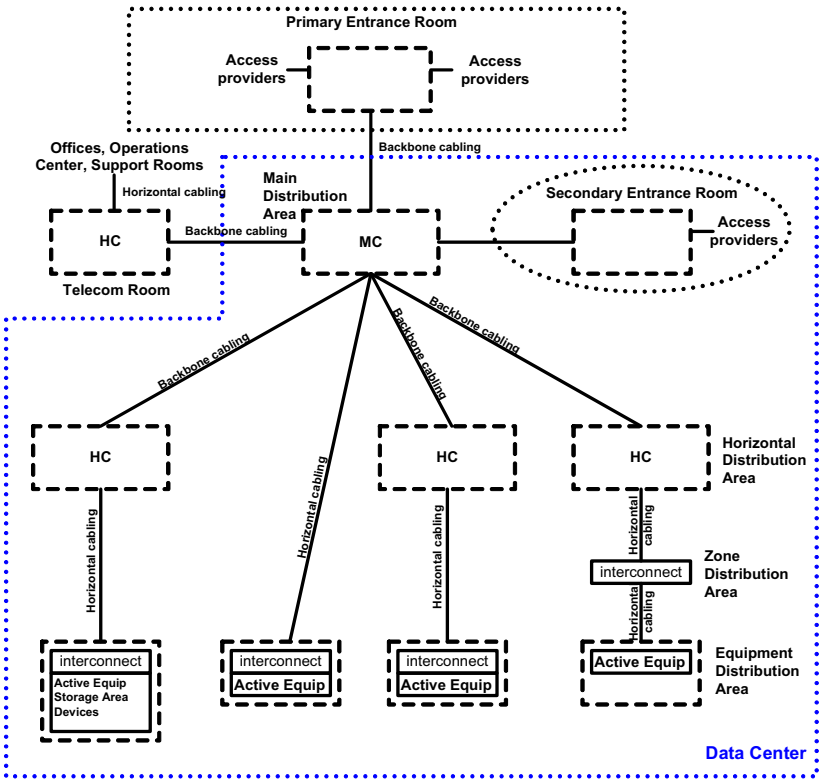


Figure 2: Data center topology

5 DATA CENTER TELECOMMUNICATIONS SPACES AND RELATED TOPOLOGIES

5.1 General

The data center requires spaces dedicated to supporting the telecommunications infrastructure. Telecommunications spaces shall be dedicated to support telecommunications cabling and equipment. Typical spaces found within a data center generally include the entrance room, main distribution area (MDA), horizontal distribution area (HDA), zone distribution area (ZDA) and equipment distribution area (EDA). Depending upon the size of the data center, not all of these spaces may be used within the structure. These spaces should be planned to provide for growth and transition to evolving technologies. These spaces may or may not be walled off or otherwise separated from the other computer room spaces.

5.2 Data center structure

5.2.1 Major elements

The data center telecommunications spaces include the entrance room, main distribution area (MDA), horizontal distribution area (HDA), zone distribution area (ZDA) and equipment distribution area (EDA).

The entrance room is the space used for the interface between data center structured cabling system and inter-building cabling, both access provider and customer-owned. This space includes the access provider demarcation hardware and access provider equipment. The entrance room may be located outside the computer room if the data center is in a building that includes general purpose offices or other types of spaces outside the data center. The entrance room may also be outside the computer room for improved security, as it avoids the need for access provider technicians to enter the computer room. Data centers may have multiple entrance rooms to provide additional redundancy or to avoid exceeding maximum cable lengths for access provider-provisioned circuits. The entrance room interfaces with the computer room through the main distribution area. The entrance room may be adjacent to or combined with the main distribution area.

The main distribution area includes the main cross-connect (MC), which is the central point of distribution for the data center structured cabling system and may include horizontal cross-connect (HC) when equipment areas are served directly from the main distribution area. This space is inside the computer room; it may be located in a dedicated room in a multi-tenant data center for security. Every data center shall have at least one main distribution area. The computer room core routers, core LAN switches, core SAN switches, and PBX are often located in the main distribution area, because this space is the hub of the cabling infrastructure for the data center. Access provider provisioning equipment (for example the M13 multiplexers) is often located in the main distribution area rather than in the entrance room to avoid the need for a second entrance room due to circuit length restrictions.

The main distribution area may serve one or more horizontal distribution areas or equipment distribution areas within the data center and one or more telecommunications rooms located outside the computer room space to support office spaces, operations center and other external support rooms.

The horizontal distribution area is used to serve equipment areas when the HC is not located in the main distribution area. Therefore, when used, the horizontal distribution area may include the HC, which is the distribution point for cabling to the equipment distribution areas. The horizontal distribution area is inside the computer room, but may be located in a dedicated room within the

computer room for additional security. The horizontal distribution area typically includes LAN switches, SAN switches, and Keyboard/Video/Mouse (KVM) switches for the end equipment located in the equipment distribution areas. A data center may have computer room spaces located on multiple floors with each floor being serviced by its own HC. A small data center may require no horizontal distribution areas, as the entire computer room may be able to be supported from the main distribution area. However, A typical data center will have several horizontal distribution areas.

The equipment distribution area (EDA) is the space allocated for end equipment, including computer systems and telecommunications equipment. These areas shall not serve the purposes of an entrance room, main distribution area or horizontal distribution area.

There may be an optional interconnection point within the horizontal cabling, called a zone distribution area. This area is located between the horizontal distribution area and the equipment distribution area to allow frequent reconfiguration and flexibility.

5.2.2 Typical data center topology

The typical data center includes a single entrance room, possibly one or more telecommunications rooms, one main distribution area, and several horizontal distribution areas. Figure 3 illustrates the typical data center topology.

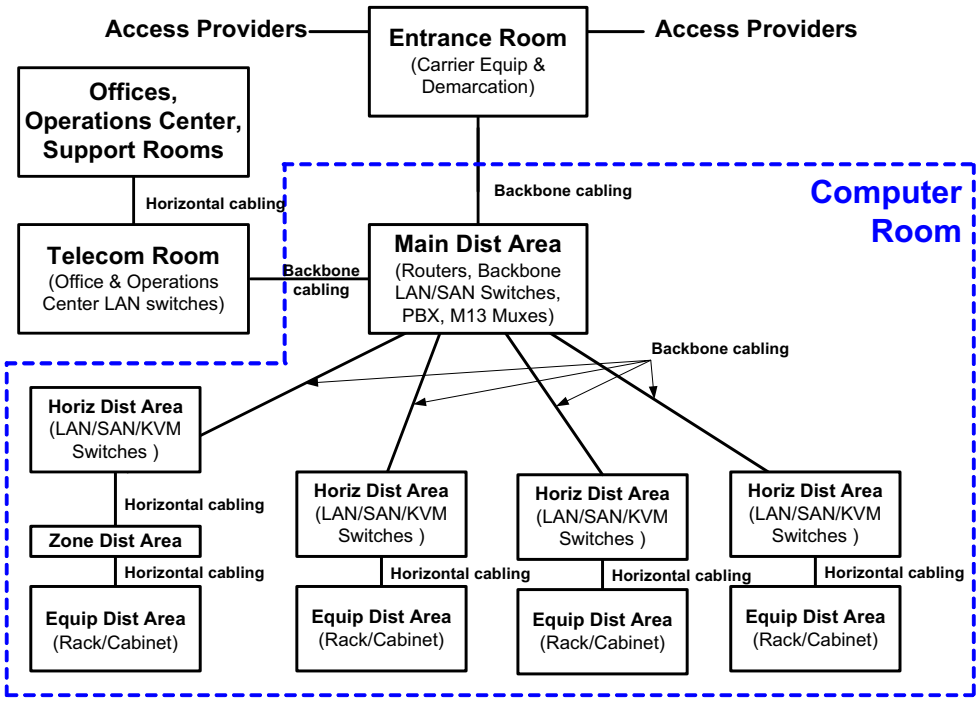


Figure 3: Example of a basic data center topology

5.2.3 Reduced data center topologies

Data center designers can consolidate the main cross-connect, and horizontal cross-connect in a single main distribution area, possibly as small as a single cabinet or rack. The telecommunications room for cabling to the support areas and the entrance room may also be consolidated into the main distribution area in a reduced data center topology. The reduced data center topology for a small data center is illustrated in Figure 4.

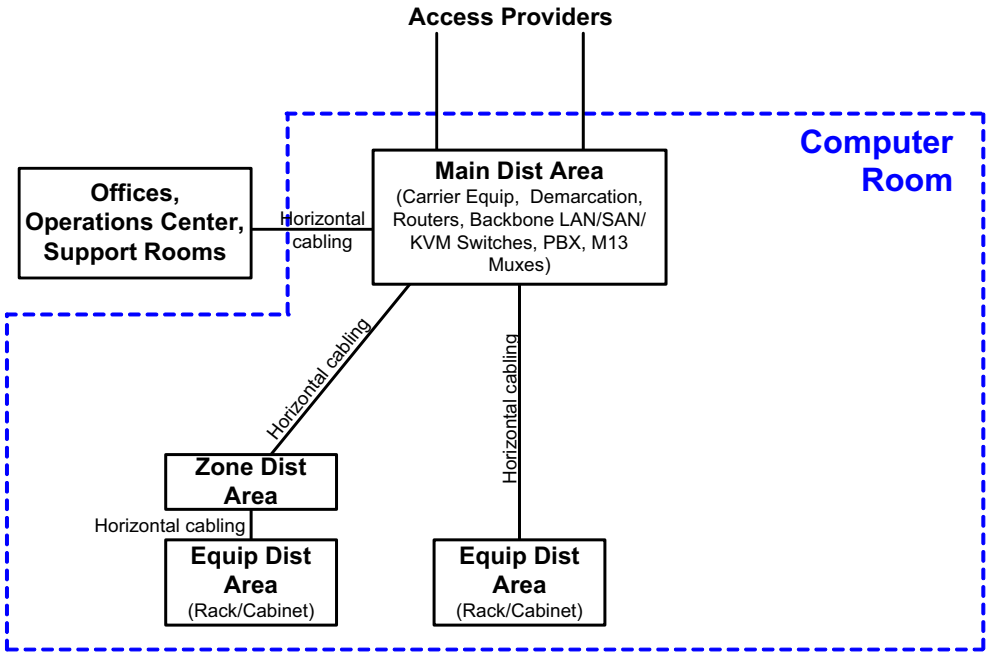


Figure 4: Example of a reduced data center topology

5.2.4 Distributed data center topologies

Multiple telecommunications rooms may be required for data centers with large or widely separated office and support areas.

Circuit distance restrictions may require multiple entrance rooms for very large data centers. Additional entrance rooms may be connected to the main distribution area and horizontal distribution areas that they support using twisted-pair cables, optical fiber cables and coaxial cables. The data center topology with multiple entrance rooms is shown in figure 5. The primary entrance room shall not have direct connections to horizontal distribution areas. Secondary entrance rooms are permitted to have direct cabling to horizontal distribution areas if the secondary entrance rooms were added to avoid exceeding maximum circuit length restrictions. Although cabling from the secondary entrance room directly to the HDAs is not common practice or encouraged, it is allowed to meet certain circuit length limitations and redundancy needs.

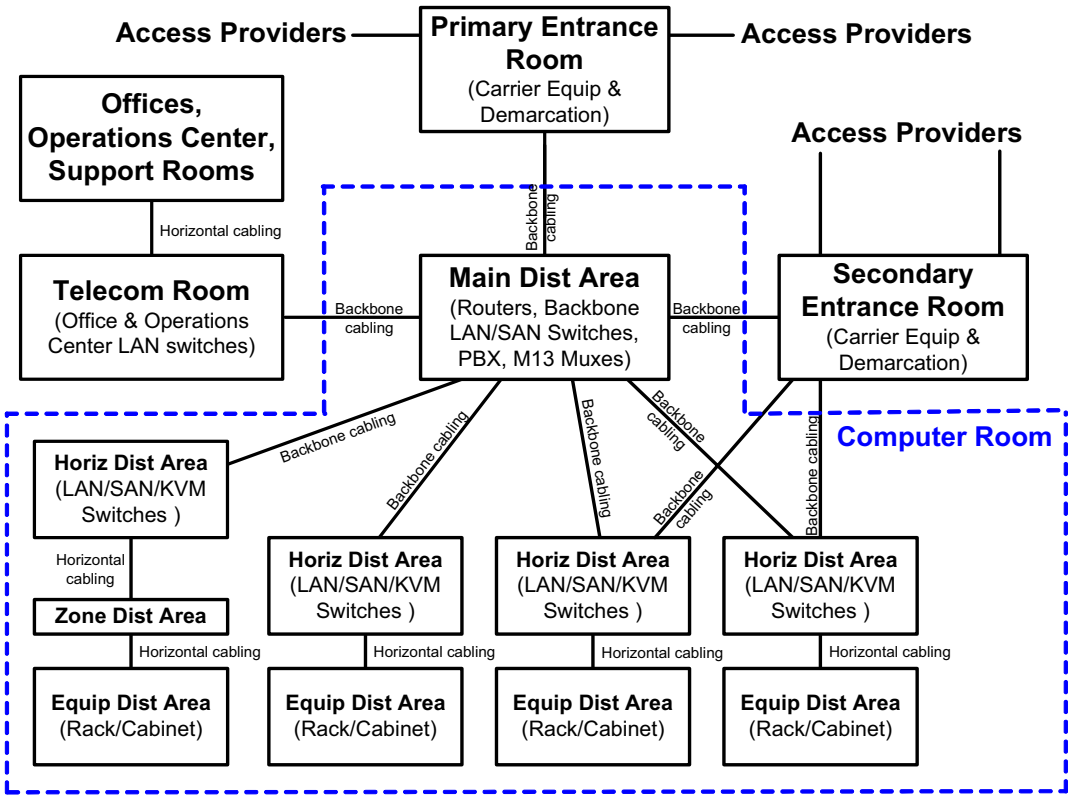


Figure 5: Example of a distributed data center topology with multiple entrance rooms.

5.3 Computer room requirements

5.3.1 General

The computer room is an environmentally controlled space that serves the sole purpose of housing equipment and cabling directly related to the computer systems and other telecommunications systems. The computer room should meet the NFPA 75 standard.

The floor layout should be consistent with equipment and facility providers' requirements, such as:

- floor loading requirements including equipment, cables, patch cords, and media (static concentrated load, static uniform floor load, dynamic rolling load);
- service clearance requirements (clearance requirements on each side of the equipment required for adequate servicing of the equipment);
- air flow requirements;
- mounting requirements;
- DC power requirements and circuit length restrictions;

- equipment connectivity length requirements (for example, maximum channel lengths to peripherals and consoles).

5.3.2 Location

When selecting the computer room site, avoid locations that are restricted by building components that limit expansion such as elevators, core, outside walls, or other fixed building walls. Accessibility for the delivery of large equipment to the equipment room should be provided (see ANSI/TIA-569-B annex B.3).

The room shall be located away from sources of electromagnetic interference. Examples of such noise sources include electrical power supply transformers, motors and generators, x-ray equipment, radio or radar transmitters, and induction sealing devices.

The computer room should not have exterior windows, as exterior windows increase heat load and reduce security.

5.3.3 Access

Computer room doors should provide access to authorized personnel only. Additionally, access to the room shall comply with the requirements of the AHJ. For additional information on monitoring computer room access, see annex G.

5.3.4 Architectural design

5.3.4.1 Size

The computer room shall be sized to meet the known requirements of specific equipment including proper clearances; this information can be obtained from the equipment provider(s). Sizing should include projected future as well as present requirements. See annex E regarding guidelines on sizing of computer rooms.

5.3.4.2 Guidelines for other equipment

Electrical control equipment, such as power distribution or conditioner systems, and UPS up to 100 kVA shall be permitted in the computer room, with the exception of flooded-cell batteries. UPS larger than 100 kVA and any UPS containing flooded-cell batteries should be located in a separate room except as required by the AHJ.

Equipment not related to the support of the computer room (e.g., piping, ductwork, pneumatic tubing, etc.) shall not be installed in, pass through, or enter the computer room.

5.3.4.3 Ceiling height

The minimum height in the computer room shall be 2.6 m (8.5 ft) from the finished floor to any obstruction such as sprinklers, lighting fixtures, or cameras. Cooling requirements or racks/cabinets taller than 2.13 m (7 ft) may dictate higher ceiling heights. A minimum of 460 mm (18 in) clearance shall be maintained from water sprinkler heads.

5.3.4.4 Treatment

Floors, walls, and ceiling shall be sealed, painted, or constructed of a material to minimize dust. Finishes should be light in color to enhance room lighting. Floors shall have anti-static properties in accordance with IEC 61000-4-2.

5.3.4.5 Lighting

Lighting shall be a minimum of 500 lux (50 footcandles) in the horizontal plane and 200 lux (20 footcandles) in the vertical plane, measured 1 m (3 ft) above the finished floor in the middle of all aisles between cabinets.

Lighting fixtures should not be powered from the same electrical distribution panel as the telecommunications equipment in the computer room. Dimmer switches should not be used. Emergency lighting and signs shall be properly placed per authority having jurisdiction (AHJ) such that an absence of primary lighting will not hamper emergency exit.

5.3.4.6 Doors

Doors shall be a minimum of 1 m (3 ft) wide and 2.13 m (7 ft) high, without doorsills, hinged to open outward (code permitting) or slide side-to-side, or be removable. Doors shall be fitted with locks and have either no center posts or removable center posts to facilitate access for large equipment. Exit requirements for the computer room shall meet the requirements of the AHJ.

5.3.4.7 Floor loading

Floor loading capacity in the computer room shall be sufficient to bear both the distributed and concentrated load of the installed equipment with associated cabling and media. The minimum distributed floor loading capacity shall be 7.2 kPA (150 lbf/ ft^2). The recommended distributed floor loading capacity is 12 kPA (250 lbf/ ft^2).

The floor shall also have a minimum of 1.2 kPA (25 lbf/ ft^2) hanging capacity for supporting loads that are suspended from the bottom of the floor (for example, cable ladders suspended from the ceiling of the floor below). The recommended hanging capacity of the floor is 2.4 kPA (50 lbf/ ft^2). Refer to Telcordia specification GR-63-CORE regarding floor loading capacity measurement and test methods.

5.3.4.8 Signage

Signage, if used, should be developed within the security plan of the building. Proper exit signage shall be placed in accordance with the AHJ.

5.3.4.9 Seismic considerations

Specifications for related facilities shall accommodate the applicable seismic zone requirements. Refer to Telcordia specification GR-63-CORE for more information regarding seismic considerations.

5.3.5 Environmental design

5.3.5.1 Contaminants

The room shall be protected from contaminants in accordance with ANSI/TIA-569-B.

5.3.5.2 HVAC

If the computer room does not have a dedicated HVAC system, the computer room shall be located with ready access to the main HVAC delivery system. A computer room is typically not recognized as such by the AHJ unless it has a dedicated HVAC, or utilizes the main building HVAC and has automatic dampers installed.

5.3.5.2.1 Continuous operation

HVAC shall be provided on a 24 hours-per-day, 365 days-per-year basis. If the building system cannot assure continuous operation for large equipment applications, a stand-alone unit shall be provided for the computer room.

5.3.5.2.2 Standby operation

The computer room HVAC system should be supported by the computer room standby generator system, if one is installed. If the computer room does not have a dedicated standby generator system, the computer room HVAC should be connected to the building standby generator system, if one is installed.

5.3.5.3 Operational parameters

The temperature and humidity shall be controlled to provide continuous operating ranges for temperature and humidity:

- dry Bulb Temperature: 20° C (68° F) to 25° C (77° F);
- relative Humidity: 40% to 55%;
- maximum Dew Point: 21° C (69.8° F);
- maximum Rate of Change: 5° C (9° F) per hour;
- humidification and dehumidification equipment may be required depending upon local environmental conditions.

The ambient temperature and humidity shall be measured after the equipment is in operation. Measurements shall be done at a distance of 1.5 m (5 ft) above the floor level every 3 to 6 m (10 to 30 ft) along the center line of the cold aisles and at any location at the air intake of operating equipment. Temperature measurements should be taken at several locations of the air intake of any equipment with potential cooling problems. Refer to ASHRAE for more detailed guidelines for measuring and evaluating computer room temperatures.

A positive pressure differential with respect to surrounding areas should be provided.

5.3.5.4 Batteries

If batteries are used for backup, adequate ventilation and spill containment as required shall be provided. Refer to applicable electrical codes for requirements.

5.3.5.5 Vibration

Mechanical vibration coupled to equipment or the cabling infrastructure can lead to service failures over time. A common example of this type of failure would be loosened connections. Potential vibration problems should be considered in the design of the computer room, since

vibration within the building will exist and will be conveyed to the computer room via the building structure. In these cases, the project structural engineer should be consulted to design safeguards against excessive computer room vibration. Refer to Telcordia specification GR-63-CORE for more information regarding vibration testing.

5.3.6 Electrical design

5.3.6.1 Power

Separate supply circuits serving the computer room shall be provided and terminated in their own electrical panel or panels.

The computer room shall have duplex convenience outlets (120V 20A) for power tools, cleaning equipment, and equipment not suitable to plug into equipment cabinet power strips. The convenience outlets should not be on the same power distribution units (PDUs) or electrical panels as the electrical circuits used for the telecommunications and computer equipment in the room. The convenience outlets shall be spaced 3.65 m (12 ft) apart along the computer room walls, or closer if specified by local ordinances, and reachable by a 4.5m (15 ft) cord (per NEC Articles 210.7(A) and 645.5(B1)).

5.3.6.2 Standby power

The computer room electrical panels should be supported by the computer room standby generator system, if one is installed. Any generators used should be rated for electronic loads. Generators of this capability are often referred to as “Computer Grade”. If the computer room does not have a dedicated standby generator system, the computer room electrical panels should be connected to the building standby generator system, if one is installed. The power shutdown requirements for computer room equipment are mandated by the AHJ and vary by jurisdiction.

5.3.6.3 Bonding and grounding (earthing)

Access shall be made available to the telecommunications grounding system specified by ANSI/TIA/EIA-J-STD-607-A. The computer room should have a common bonding network (CBN) (see subclause G.5.1.6).

5.3.7 Fire protection

The fire protection systems and hand-held fire extinguishers shall comply with NFPA-75.
Sprinkler systems in computer rooms should be pre-action systems.

5.3.8 Water infiltration

Where risk of water ingress exists, a means of evacuating water from the space shall be provided (e.g. a floor drain). Additionally, at least one drain or other means for evacuating water for each 100 m^2 (1000 ft^2) area should be provided. Any water and drain pipes that run through the room should be located away from and not directly above equipment in the room.

5.4 Entrance room requirements

5.4.1 General

The entrance room is a space, preferably a room, in which access provider-owned facilities interface with the data center cabling system. It typically houses telecommunications access provider equipment and is the location where access providers typically hand off circuits to the customer. This hand-off point is called the demarcation point. It is where the telecommunications

access provider's responsibility for the circuit typically ends and the customer's responsibility for the circuit begins.

The entrance room will house entrance pathways, protector blocks for copper-pair entrance cables, termination equipment for access provider cables, access provider equipment, and termination equipment for cabling to the computer room.

5.4.2 Location

The entrance room should be located to ensure that maximum circuit lengths from the access provider demarcation points to the end equipment are not exceeded. The maximum circuit lengths need to include the entire cable route, including patch cords and changes in height between floors and within racks or cabinets. Specific circuit lengths (from demarcation point to end equipment) to consider when planning entrance room locations are provided in annex A.

> NOTE: Repeaters can be used to extend circuits beyond the lengths specified in annex A.

The entrance rooms may either be located inside or outside the computer room space. Security concerns may dictate that the entrance rooms are located outside the computer room to avoid the need for access provider technicians to access the computer room. However, in larger data centers, circuit length concerns may require that the entrance room be located in the computer room.

Cabling in the entrance rooms should use the same cable distribution (overhead or under floor) as used in the computer room; this will minimize cable lengths as it avoids a transition from overhead cable trays to under floor cable trays.

5.4.3 Quantity

Large data centers may require multiple entrance rooms to support some circuit types throughout the computer room space and/or to provide additional redundancy.

The additional entrance rooms may have their own entrance pathways for dedicated service feeds from the access providers. Alternatively, the additional entrance rooms may be subsidiaries of the primary entrance room, in which case the access provider service feeds come from the primary entrance room.

5.4.4 Access

Access to the entrance room shall be controlled by the data center owner or their agent.

5.4.5 Entrance conduit routing under access floor

If the entrance room is located in the computer room space, the entrance conduit runs should be designed to avoid interfering with airflow, chilled water piping and other cable routing under the access floor.

5.4.6 Access provider and service provider spaces

Access provider and service provider spaces for data centers are typically located either in the entrance room or in the computer room. Refer to ANSI/TIA-569-B for information on access provider and service provider spaces.

The access provider and service provider spaces in data center entrance rooms typically do not require partitions because access to the data center entrance rooms is carefully controlled. Access and service providers that lease space in the computer room, however, typically require secure access to their spaces.

5.4.7 Building entrance terminal

5.4.7.1 General

Listed herein are the requirements for building entrance terminals located at the cabling entrance to building facilities where the transition between inside and outside environments occur. Outside terminals are typically used when the entrance connection is located in a closure on an outside wall of a building. Inside terminals are used when the outside cable will be connected to the inside distribution cabling system. Refer to ANSI/TIA/EIA-568-B.1 for additional information on entrance facilities and entrance facility connections.

5.4.8 Architectural design

5.4.8.1 General

The decision whether a room or open area is provided should be based on security (with consideration to both access and incidental contact), the need for wall space for protectors, entrance room size, and physical location.

5.4.8.2 Size

The entrance room shall be sized to meet known and projected maximum requirements for:

- entrance pathways for access provider and campus cabling;
- backboard and frame space for termination of access provider and campus cabling;
- access provider racks;
- customer-owned equipment to be located in the entrance room;
- demarcation racks including termination hardware for cabling to the computer room;
- pathways to the computer room, the main distribution area and possibly horizontal distribution area for secondary entrance rooms;
- pathways to other entrance rooms if there are multiple entrance rooms.

The space required is related more closely to the number of access providers, number of circuits, and type of circuits to be terminated in the room than to the size of the data center. Meet with all access providers to determine their initial and future space requirements. See annex C for more information regarding access provider coordination and access provider demarcation.

Space should also be provided for campus cabling. Cables containing metallic components (copper-pair, coaxial, optical fiber cables with metallic components etc.) shall be terminated with protectors in the entrance room. The protectors may either be wall-mounted or frame-mounted. The space for protectors shall be located as close as practical to the point of entrance of the cables into the building. Optical fiber campus cables may be terminated in the main cross-connect instead of the entrance room if they have no metallic components (for example, cable

sheath or strength member). Refer to applicable codes regarding entrance cable and entrance cable termination requirements.

5.4.8.3 Plywood backboards

Where wall terminations are to be provided for protectors, the wall should be covered with rigidly fixed 20 mm (¾ in) A-C plywood, preferably void free, 2.4 m (8 ft) high, and capable of supporting attached connecting hardware. Plywood should be either fire-rated (fire-retardant) or covered with two coats of fire retardant paint.

If fire-rated (fire-retardant) plywood is to be painted, the paint should not cover the fire-rating stamp until inspection by the fire marshal or other AHJ is complete. To reduce warping, fire-rated (fire-retardant) plywood shall be kiln-dried and shall not exceed moisture content of 15 %.

5.4.8.4 Ceiling height

The minimum height shall be 2.6 m (8.5 ft) from the finished floor to any obstruction such as sprinklers, lighting fixtures, or cameras. Cooling requirements or racks/cabinets taller than 2.13 m (7 ft) may dictate higher ceiling heights. A minimum of 460 mm (18 in) clearance shall be maintained from water sprinkler heads.

5.4.8.5 Treatment

Floors, walls, and ceiling shall be sealed, painted, or constructed of a material to minimize dust. Finishes should be light in color to enhance room lighting. Floors shall have anti-static properties as per IEC 61000-4-2.

5.4.8.6 Lighting

Lighting shall be a minimum of 500 lux (50 footcandles) in the horizontal plane and 200 lux (20 footcandles) in the vertical plane, measured 1 m (3 ft) above the finished floor in middle of all aisles between cabinets.

Lighting fixtures should not be powered from the same electrical distribution panel as the telecommunications equipment in the computer room. Dimmer switches should not be used. Emergency lighting and signs shall be properly placed per AHJ such that an absence of primary lighting will not hamper emergency exit.

5.4.8.7 Doors

Doors shall be a minimum of 1 m (3 ft) wide and 2.13 m (7 ft) high, without doorsill, hinged to open outward (code permitting) or slide side-to-side, or be removable. Doors shall be fitted with a lock and have either no center post or a removable center post to facilitate access for large equipment.

5.4.8.8 Signage

Signage, if used, should be developed within the security plan of the building.

5.4.8.9 Seismic considerations

Specifications for related facilities shall accommodate the applicable seismic zone requirements. Refer to Telcordia specification GR-63-CORE for more information regarding seismic considerations.

5.4.8.10 HVAC

The entrance room shall be located with ready access to the computer room HVAC delivery system. Consider having dedicated air-conditioning for the entrance room. If the entrance room has dedicated air-conditioning, temperature control circuits for the entrance room air-conditioning units should be powered from the same PDUs or panel boards that serve the entrance room racks.

HVAC for the equipment in the entrance room should have the same degree of redundancy and backup as the HVAC and power for the computer room.

5.4.8.10.1 Continuous operation

HVAC shall be provided on a 24 hours-per-day, 365 days-per-year basis. If the building system cannot assure continuous operation, a stand-alone unit shall be provided for the data center entrance room.

5.4.8.10.2 Standby operation

The entrance room HVAC system should be supported by the computer room standby generator system, if one is installed. If the computer room or entrance room does not have a dedicated standby generator system, the entrance room HVAC should be connected to the building standby generator system, if one is installed.

5.4.8.11 Operational parameters

The temperature and humidity shall be controlled to provide continuous operating ranges for temperature and humidity:

- dry Bulb Temperature: 20^{o} C (68^{o} F) to 25^{o} C (77^{o} F);
- relative Humidity: 40% to 55%;
- maximum Dew Point: 21^{o} C (69.8^{o} F);
- maximum Rate of Change: 5^{o} C (9^{o} F) per hour;
- humidification and dehumidification equipment may be required depending upon local environmental conditions.

The ambient temperature and humidity shall be measured after the equipment is in operation. Measurement shall be done at a distance of 1.5 m (5 ft) above the floor level every 3 to 6 m (10 to 30 ft) along the center line of the cold aisles and at any location at the air intake of operating equipment. Temperature measurements should be taken at several locations of the air intake of any equipment with potential cooling problems.

5.4.8.12 Power

Consider having dedicated PDUs and UPS fed power panels for the entrance room. The quantity of electrical circuits for entrance rooms depends on the requirements of the equipment to be located in the room. The entrance rooms shall use the same electrical backup systems (UPS and generators) as that used for the computer room. The degree of redundancy for entrance room mechanical and electrical systems shall be the same as that for the computer room.

The entrance room shall have one or more duplex convenience outlets (120V 20A) for power tools, cleaning equipment, and other equipment not suitable to plug into equipment rack power strips. The convenience outlets should not be on the same PDU or electrical panel as the electrical circuits used for the telecommunications and computer equipment in the room. There shall be at least one duplex outlet on each wall of the room, spaced no more than 4m (12 ft) apart, and in floor boxes, poke through and other delivery systems such that they can be reached by a 4.5 m (15 ft) power cord from any place in the room as per the NFPA 70 article 645.5 (B1) or as per the AHJ.

5.4.8.13 Standby Power

The entrance room electrical panels should be supported by the computer room standby generator system, if one is installed. Any generators used should be rated for electronic loads. Generators of this capability are often referred to as “Computer Grade”. If the computer room or entrance room does not have a dedicated standby generator system, the entrance room electrical panels should be connected to the building standby generator system, if one is installed.

5.4.8.14 Bonding and grounding

Access shall be made available to the telecommunications grounding system specified by ANSI/TIA/EIA-J-STD-607-A.

5.4.9 Fire protection

The fire protection systems and hand-held fire extinguishers shall comply with NFPA-75.
Sprinkler systems in computer rooms should be pre-action systems.

5.4.10 Water infiltration

Where risk of water ingress exists, a means of evacuating water from the space shall be provided (e.g. a floor drain). Any water and drain pipes that run through the room should be located away from and not directly above equipment in the room.

5.5 Main distribution area

5.5.1 General

The main distribution area (MDA) is the central space where the point of distribution for the structured cabling system in the data center is located. The data center shall have at least one main distribution area. The core routers and core switches for the data center networks are often located in or near the main distribution area.

In data centers that are used by multiple organizations, such as Internet data centers and collocation facilities, the main distribution area should be in a secure space.

5.5.2 Location

The main distribution area should be centrally located to avoid exceeding maximum distance restrictions for the applications to be supported, including maximum cable lengths for access provider circuits served out of the entrance room.

5.5.3 Facility requirements

If the main distribution area is in an enclosed room, consider a dedicated HVAC, PDU, and UPS fed power panels for this area.

If the main distribution area has dedicated HVAC, the temperature control circuits for air-conditioning units should be powered and controlled from the same PDUs or power panels that serve the telecommunications equipment in the main distribution area.

The architectural, mechanical, and electrical requirements for the main distribution area are the same as that for the computer room.

5.6 Horizontal distribution area

5.6.1 General

The horizontal distribution area (HDA) is the space that supports cabling to the equipment distribution areas. The LAN, SAN, console, and KVM switches that support the end equipment are also typically located in the horizontal distribution area. The main distribution area may serve as a horizontal distribution area for nearby equipment or for the entire computer room if the computer room is small.

There should be a minimum of one horizontal distribution area per floor. Additional horizontal distribution areas may be required to support equipment beyond the horizontal cable length limitation.

The maximum number of connections per horizontal distribution area should be adjusted based on cable tray capacity, leaving room in the cable trays for future cabling.

In data centers that are used by multiple organizations, such as Internet data centers and collocation facilities, the horizontal distribution areas should be in a secure space.

5.6.2 Location

The horizontal distribution areas should be located to avoid exceeding maximum backbone lengths from the MDA and maximum distances for the media type.

5.6.3 Facility requirements

If the horizontal distribution area is in an enclosed room, consideration regarding a dedicated HVAC, PDUs, and UPS fed power panels for the horizontal distribution area should be taken.

The temperature control circuits and air-conditioning units should be powered from a different PDUs or power panels that serve the telecommunications equipment in the horizontal distribution area.

The architectural, mechanical, and electrical requirements for the horizontal distribution area are the same as that for the computer room.

5.7 Zone distribution area

The zone distribution area should be limited to serving a maximum of 288 coaxial or twisted-pair connections to avoid cable congestion, particularly for enclosures meant to be placed overhead or under 2 ft. x 2 ft. (or 600 mm x 600 mm) access floor tiles.

Cross-connection shall not be used in the zone distribution area. No more than one zone distribution area shall be used within the same horizontal cable run.

There shall be no active equipment in the zone distribution area with the exception of DC powering equipment.

5.8 Equipment distribution areas

The equipment distribution areas are spaces allocated for end equipment, including computer systems and communications equipment. These areas do not include the telecommunications rooms, entrance rooms, main distribution area, and horizontal distribution areas.

The end equipment is typically floor standing equipment or equipment mounted in cabinets or racks.

Horizontal cables are terminated in equipment distribution areas on connecting hardware mounted in the cabinets or racks. Sufficient power receptacles and connecting hardware should be provided for each equipment cabinet and rack to minimize patch cord and power cord lengths.

Point-to-point cabling is permitted between equipment located in the equipment distribution area. Cable lengths for point-to-point cabling between equipment in the equipment distribution area should be no greater than 15 m (49 ft) and should be between equipment in adjacent racks or cabinets in the same row.

5.9 Telecommunications room

In data centers, the telecommunications room (TR) is a space that supports cabling to areas outside the computer room. The TR is normally located outside the computer room but, if necessary, it can be combined with the main distribution area or horizontal distribution areas.

The data center may support more than one telecommunications room if the areas to be served cannot be supported from a single telecommunications room.

The telecommunication rooms shall meet the specifications of ANSI/TIA-569-B.

5.10 Data center support areas

The data center support areas are spaces outside the computer room that are dedicated to supporting the data center facility. These may include the operation center, support personnel offices, security rooms, electrical rooms, mechanical rooms, storage rooms, equipment staging rooms, and loading docks.

The operation center, security room, and support personnel offices shall be cabled similarly to standard office areas, as per ANSI/TIA/EIA-568-B.1. The operation center consoles and security consoles will require larger numbers of cables than standard work area requirements. The quantity should be determined with the assistance of the operations and technical staff. The operation center may also require cabling for large wall-mounted or ceiling-mounted displays (e.g., monitors and televisions).

The electrical rooms, mechanical rooms, storage rooms, equipment staging rooms, and loading docks should have at least one wall phone each. The electrical and mechanical rooms should also have at least one data connection for access to the facility management system.

5.11 Racks and cabinets

5.11.1 General

Racks are equipped with side mounting rails to which equipment and hardware are mounted. Cabinets can be equipped with side mounting rails, side panels, a top, and front and rear doors, and are frequently equipped with locks.

5.11.2 "Hot" and "cold" aisles

Cabinets and racks shall be arranged in an alternating pattern, with fronts of cabinets/racks facing each other in a row to create "hot" and "cold" aisles.

"Cold" aisles are in front of racks and cabinets. If there is an access floor, power distribution cables should be installed here under the access floor on the slab.

"Hot" aisles are behind racks and cabinets. If there is an access floor, cable trays for telecommunications cabling should be located under the access floor in the “hot” aisles.

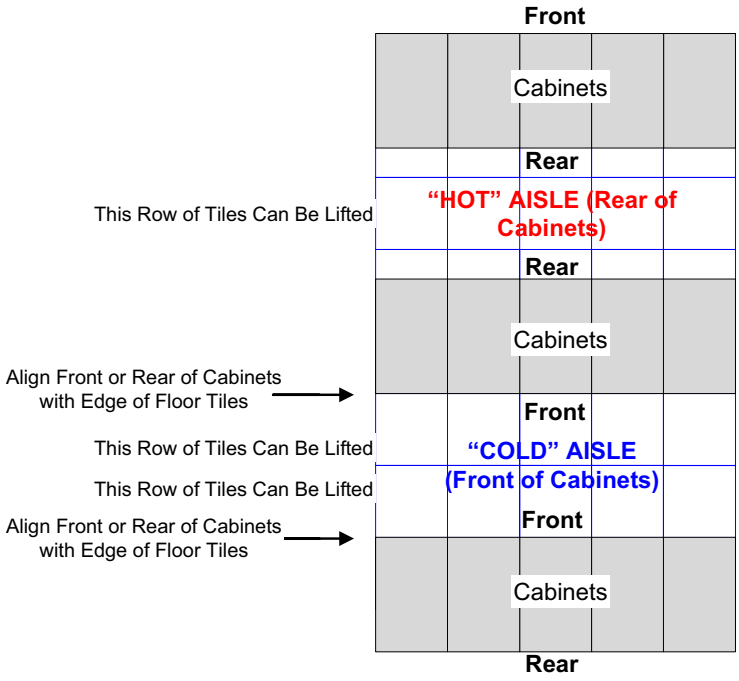


Figure 6: Example of "hot" aisles, "cold" aisles and cabinet placement

5.11.3 Equipment placement

Equipment should be placed in cabinets and racks with “cold” air intake at the front of the cabinet or rack, and “hot” air exhaust out the back. Reversing equipment in the rack will disrupt the proper functioning of “hot” and “cold” aisles. Equipment that uses the front-to-rear cooling scheme should be used so that it does not disrupt the functioning of hot and cold aisles.

Blank panels should be installed in unused rack and cabinet spaces to improve the functioning of "hot" and "cold" aisles. Perforated access floor tiles should be located in the “cold” aisles rather than in the “hot” aisles to improve the functioning of the “hot” and “cold” aisles. Additionally, no cable trays or other obstruction should be placed in the “cold” aisles below the perforated tiles.

See annex D for additional information regarding coordination of equipment plans with other disciplines.

5.11.4 Placement relative to floor tile grid

When placed on access floor, cabinets and racks shall be arranged so that they permit tiles in the front and rear of the cabinets and racks to be lifted. Cabinets should be aligned with either the front or rear edge along the edge of the floor tile. Racks should be placed such that the threaded rods that secure the racks to the slab will not penetrate an access floor stringer.

5.11.5 Access floor tile cuts

Floor tile cuts should be no larger than necessary. Dampers or brushes should be installed on floor tile cuts to minimize air loss through openings in the floor tiles. Floor tile cuts shall have edging or grommets along all cut edges.

Floor tile cuts for cabinets should be placed under the cabinets or other location where the floor tile cut will not create a tripping hazard.

Floor tile cuts for racks should be placed either under the vertical cable managers between the racks or under the rack (at the opening between the bottom angles). Generally, placing the floor tile cut under the vertical cable managers is preferable as it allows equipment to be located at the bottom of the rack.

Cabinets and racks should be placed at the same location on each floor tile so that floor tile cuts can be standardized. Thus, cabinets should be the same width as the floor tiles and the combined width of one rack and one vertical wire manager should be the same width as the floor tile. Additionally, spacers may be employed between cabinets to ensure that each cabinet in a row starts at the edge of a floor tile. Exceptions to this general rule are:

- main distribution area and horizontal distribution area where large vertical cable managers are typically used to provide adequate cable management;

- entrance room access provider racks and cabinets, which are often 585 mm (23 in) rather than 480 mm (19 in) racks;

- cabinets for large servers that do not fit in standard 480 mm (19 in) cabinets.

5.11.6 Installation of racks on access floors

Seismic racks shall either be bolted to a seismic stand or bolted directly to the slab.

Racks that are supported by the access floor shall be bolted to the cement slab or a metal channel secured to the slab by threaded rods that penetrate through the floor tiles.

Sharp edges on the top of the threaded rods shall be covered using domed nuts or other method. Exposed threads under the access floor should be covered using split tubing or other method.

5.11.7 Specifications

5.11.7.1 Clearances

A minimum of 1 m (3 ft) of front clearance shall be provided for installation of equipment. A front clearance of 1.2 m (4 ft) is preferable to accommodate deeper equipment. A minimum of 0.6 m (2 ft) of rear clearance shall be provided for service access at the rear of racks and cabinets. A rear clearance of 1 m (3 ft) is preferable. Some equipment may require service clearances of greater than 1 m (3 ft). See equipment manufacturer requirements

5.11.7.2 Cabinet ventilation

The cabinets shall be selected to provide adequate ventilation for the equipment it will house. Ventilation can be achieved by using:

- forced airflow utilizing fans;

- utilizing natural airflow between hot and cold aisles through ventilation openings in the front and rear doors of the cabinets;

- a combination of both methods.

For moderate heat loads, cabinets can utilize any of the following ventilation practices:

1) Ventilation through slots or perforations of front and rear doors to provide a minimum of 50% open space. Increasing the size and area of ventilation openings can increase the level of ventilation.

2) Ventilation through forced airflow utilizing fans in combination with properly placed door vents, and sufficient space between the equipment and rack doors.

For high heat loads, natural airflow is not sufficient and forced airflow is required to provide adequate cooling for all the equipment in the cabinet. A forced airflow system utilizes a combination of properly placed vents in addition to the cooling fan systems.

If cabinet fans are installed, they should be of the type that is designed to enhance rather than disrupt the functioning of “hot” and “cold” aisles. Airflow from the fans should adequate to dissipate the heat generated in the cabinet.

In data centers where the highest availability is desired, fans should be wired from separate circuits than those fed by the PDUs or UPS fed power panels to avoid disruption to telecommunications and computer equipment when fans fail.

5.11.7.3 Cabinet and rack height

The maximum rack and cabinet height shall be 2.4 m (8 ft). Racks and cabinets should preferably be no taller than 2.1 m (7 ft) for easier access to the equipment or connecting hardware installed at the top.

5.11.7.4 Cabinet depth and width

Cabinets should be of adequate depth to accommodate the planned equipment, including cabling at the front and/or rear, power cords, cable management hardware, and power strips. To ensure adequate airflow and to provide adequate space for power strips and cabling, consider using cabinets that are at least 150 mm (6 in) deeper or wider than the deepest.

5.11.7.5 Adjustable rails

Cabinets should have adjustable front and rear rails. The rails should provide 42 or more rack units (RUs) of mounting space. Rails may optionally have markings at rack unit boundaries to simplify positioning of equipment. Active equipment and connecting hardware should be mounted on the rails on rack unit boundaries to most efficiently utilize cabinet space.

If patch panels are to be installed on the front of cabinets, the front rails should be recessed at least 100 mm (4 in) to provide room for cable management between the patch panels and doors

and to provide space for cabling between cabinets. Similarly, if patch panels are to be installed on the rear of cabinets, the rear rails should be recessed at least 100 mm (4 in).

Patch panels shall not be installed on both the front and rear rails of a cabinet or rack in a manner to prevent service access to the rear of the patch panels.

If power strips are to be installed on the front or rear rail of cabinets, adequate clearance should be provided for power cords and power supplies that may be installed on the power strips.

5.11.7.6 Rack and cabinet finishes

Painted finishes should be powder coat or other scratch-resistant finishes.

5.11.7.7 Power strips

Cabinets and racks with no active equipment do not require power strips.

The typical configuration for power strips in cabinets provides at least one 20A, 120V power strip. The use of two power strips which contain circuits that are fed from diverse power sources should be considered. Power circuits should have dedicated neutral and ground conductors. Power strips with indicators but no on/off switch or breaker reset button should be used to minimize accidental shut-off. A number of power strips should be used to provide enough receptacles and current capacity to support the planned equipment. The plug for the power strip should be a locking plug to prevent accidental disconnection.

Power strips shall be labeled with the PDU/panel identifier and circuit breaker number.

5.11.7.8 Additional cabinet and rack specifications

Refer to ANSI T1.336 for additional specifications for cabinets and racks. In addition to the requirements specified in T1.336, cabinets and racks heights up to 2.4 m (8 ft) and cabinet depths up to 1.1 m (43 in) may be used in data centers.

5.11.8 Racks and cabinets in entrance room, main distribution areas and horizontal distribution areas

The entrance room, main distribution area and horizontal distribution areas should use 480 mm (19 in) racks for patch panels and equipment. Service providers may install their own equipment in the entrance room in either 585 mm (23 in) racks or proprietary cabinets.

In the entrance room, main distribution area, and horizontal distribution areas, a vertical cable manager shall be installed between each pair of racks and at both ends of every row of racks. The vertical cable managers shall be not less than 83 mm (3.25 in) in width. Where single racks are installed, the vertical cable managers should be at least 150 mm (6 in) wide. Where a row of two or more racks is installed, consider mounting 250mm (10 in) wide vertical cable managers between racks, and 150 mm (6 in) wide vertical cable managers at both ends of the row. The cable managers should extend from the floor to the top of the racks.

In the entrance room, main distribution area and horizontal distribution areas, horizontal cable management panels should be installed above and below each patch panel. The preferred ratio of horizontal cable management to patch panels is 1:1.

The vertical cable management, horizontal cable management, and slack storage should be adequate to ensure that the cables can be neatly dressed and that bend radius requirements specified in ANSI/EIA/TIA-568-B.2 and ANSI/EIATIA-568-B.3 are met.

Overhead cable trays should be for management of patch cables between racks.

Overhead cable tray should not be used for structural support for racks. It is recommended that a structural engineer be consulted in determining appropriate mounting for high weight load applications.

6 DATA CENTER CABLING SYSTEMS

6.1 General

The Data Center cabling system is a cabling infrastructure that will support a multi-product, multi-vendor environment.

6.2 Horizontal Cabling

6.2.1 General

The horizontal cabling is the portion of the telecommunications cabling system that extends from the mechanical termination in the equipment distribution area to either the horizontal cross-connect in the horizontal distribution area or the main cross-connect in the main distribution area. The horizontal cabling includes horizontal cables, mechanical terminations, and patch cords or jumpers, and may include a zone outlet or a consolidation point in the zone distribution area.

> NOTE: The term "horizontal" is used since typically the cable in this part of the cabling system runs horizontally along the floor(s) or ceiling(s) of the data center.

The following partial listing of common services and systems should be considered when the horizontal cabling is designed:

- voice, modem, and facsimile telecommunications service;
- premises switching equipment;
- computer and telecommunications management connections;
- keyboard/video/mouse (KVM) connections;
- data communications;
- wide area networks (WAN);
- local area networks (LAN);
- storage area networks (SAN);
- other building signaling systems (building automation systems such as fire, security, power, HVAC, EMS, etc.).

In addition to satisfying today’s telecommunication requirements, the horizontal cabling should be planned to reduce ongoing maintenance and relocation. It should also accommodate future equipment and service changes. Consideration should be given to accommodating a diversity of user applications in order to reduce or eliminate the probability of requiring changes to the horizontal cabling as equipment needs evolve. The horizontal cabling can be accessed for reconfiguration under the access floor or overhead on cable tray systems. However, in a properly planned facility, disturbance of the horizontal cabling should only occur during the addition of new cabling.

6.2.2 Topology

The horizontal cabling shall be installed in a star topology as shown in figure 7. Each mechanical termination in the equipment distribution area shall be connected to a horizontal cross-connect in the horizontal distribution area or main cross-connect in the main distribution area via a horizontal cable.

Horizontal cabling shall contain no more than one consolidation point in the zone distribution area between the horizontal cross-connect in the horizontal distribution area and the mechanical termination in the equipment distribution area. Refer to subclause 5.7 for additional information regarding zone distribution areas.

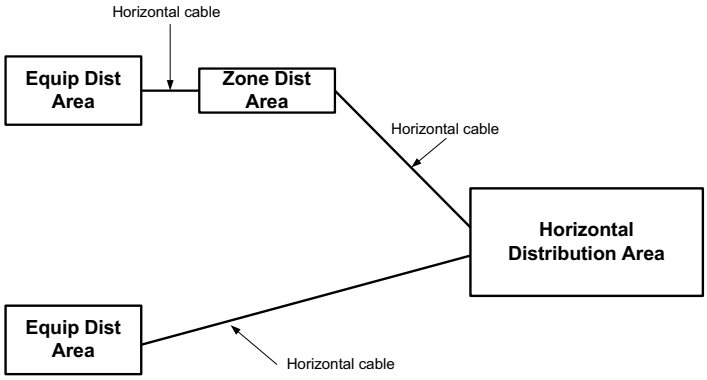


Figure 7: Typical horizontal cabling using a star topology

6.2.3 Horizontal cabling distances

The horizontal cabling distance is the cable length from the mechanical termination of the media at the horizontal cross-connect in the horizontal distribution area or the main distribution area to the mechanical termination of the media in the equipment distribution area. The maximum horizontal distance shall be 90 m (295 ft), independent of media type (see figure 7). The maximum channel distance including equipment cords shall be 100 m (328 ft). The maximum cabling distance in a data center not containing a horizontal distribution area shall be 300 m (984 ft) for an optical fiber channel including equipment cords, 90 m (294 ft) for copper cabling excluding equipment cords and 100 m (328 ft) for copper cabling including equipment cords. If a zone outlet is used, the maximum horizontal distances of copper media shall be reduced in accordance with subclause 6.2.3.1.

Additionally, horizontal cable distances in a computer room may need to be reduced to compensate for longer equipment cords in the data center distribution areas. Therefore, careful considerations to the horizontal cable distance should be made to ensure cabling distances and transmission requirements are not exceeded when the equipment cords are attached. Refer to annex A for additional information on application-based cabling distances.

> NOTE: For copper cabling, in order to reduce the effect of multiple connections in close proximity on NEXT loss and return loss, the zone distribution area termination should be located at least 15 m (49 ft) from the horizontal distribution area termination.

6.2.3.1 Maximum lengths for copper cabling

Copper equipment cables used in the context of zone outlets in the zone distribution area, shall meet the requirements of ANSI/TIA/EIA-568-B.2. Based upon insertion loss considerations, the maximum length shall be determined according to:

$C = (102 - H)/(1+D)$ (1)

$Z = C - T \leq 22$ m (72 ft) for 24 AWG UTP/ScTP or ≤ 17 m (56 ft) for 26 AWG ScTP (2)

Where:

C is the maximum combined length (m) of the zone area cable, equipment cable, and patch cord.

H is the length (m) of the horizontal cable (H + C ≤ 100 m).

D is a de-rating factor for the patch cord type (0.2 for 24 AWG UTP/24 AWG ScTP and 0.5 for 26 AWG ScTP).

Z is the maximum length (m) of the zone area cable.

T is the total length of patch and equipment cords.

Table 1 applies the above formulae assuming that there is a total of 5 m (16 ft) of 24 AWG UTP/24AWG ScTP or 4 m (13 ft) of 26 AWG ScTP patch cords and equipment cables in the main distribution area, or horizontal distribution area. The zone outlet shall be marked with the maximum allowable zone area cable length. One method to accomplish this is to evaluate cable length markings.

Table 1: Maximum length of horizontal and equipment area cables

Length of horizontal cable H m (ft)	24 AWG UTP/24 AWG ScTP patch cords		26 AWG ScTP patch cords	
	Maximum length of zone area cable Z m (ft)	Maximum combined length of zone area cables, patch cords, and equipment cable C m (ft)	Maximum length of zone area cable Z m (ft)	Maximum combined length of zone area cables, patch cords, and equipment cable C m (ft)
90 (295)	5 (16)	10 (33)	4 (13)	8 (26)
85 (279)	9 (30)	14 (46)	7 (23)	11 (35)
80 (262)	13 (44)	18 (59)	11 (35)	15 (49)
75 (246)	17 (57)	22 (72)	14 (46)	18 (59)
70 (230)	22 (72)	27 (89)	17 (56)	21 (70)

6.2.4 Recognized media

Due to the wide range of services and site sizes where horizontal cabling will be used, more than one transmission medium is recognized. This Standard specifies transmission media, which shall be used individually or in combination in the horizontal cabling.

Recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet all applicable requirements specified in ANSI/TIA/EIA-568-B.2 and ANSI/TIA/EIA-568-B.3.

The recognized media are:

- 100-ohm twisted-pair cable (ANSI/TIA/EIA-568-B.2), category 6 recommended (ANSI/TIA/EIA-568-B.2-1);

- multimode optical fiber cable, either 62.5/125 micron or 50/125 micron (ANSI/TIA/EIA-568-B.3), 50/125 micron 850 nm laser optimized multimode fiber is recommended (ANSI/TIA-568-B.3-1);

- single-mode optical fiber cable (ANSI/TIA/EIA-568-B.3).

The recognized coaxial media are 75-ohm (734 and 735 type) coaxial cable (Telcordia Technologies GR-139-CORE) and coaxial connector (ANSI T1.404). These cables and connectors are recommended to support specific applications per annex A.

Channels constructed from recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet the requirements specified in ANSI/TIA/EIA-568-B.1, ANSI/TIA/EIA-568-B.2, ANSI/TIA/EIA-568-B.3 and ANSI T1.404 (DS3).

NOTES

1) Crosstalk between individual, unshielded twisted-pairs may affect the transmission performance of multipair copper cables. Annex B of ANSI/TIA/EIA-568-B.1 provides some shared sheath guidelines for multipair cables.

2) See subclause 6.2.3 for horizontal cabling distance limitations.

6.3 Backbone cabling

6.3.1 General

The function of the backbone cabling is to provide connections between the main distribution area, the horizontal distribution area, and entrance facilities in the data center cabling system. Backbone cabling consists of the backbone cables, main cross-connects, horizontal cross-connects, mechanical terminations, and patch cord or jumpers used for backbone-to-backbone cross-connection.

The backbone cabling is expected to serve the needs of the data center occupants for one or several planning phases, each phase spanning a time scale that may be on the order of days or months. During each planning period, the backbone cabling design should accommodate growth and changes in service requirements without the installation of additional cabling. The length of the planning period is ultimately dependent on the design logistics including material procurement, transportation, installation and specification control.

The backbone cabling shall allow network reconfiguration and future growth without disturbance of the backbone cabling. The backbone cabling should support different connectivity requirements, including both the network and physical console connectivity such as local area networks, wide area networks, storage area networks, computer channels, and equipment console connections.

6.3.2 Topology

6.3.2.1 Star topology

The backbone cabling shall use the hierarchical star topology as illustrated by figure 8 wherein each horizontal cross-connect in the horizontal distribution area is cabled directly to a main cross-connect in the main distribution area. There shall be no more than one hierarchical level of cross-connect in the backbone cabling. From the horizontal cross-connect, no more than one cross-connect shall be passed through to reach another horizontal cross-connect.

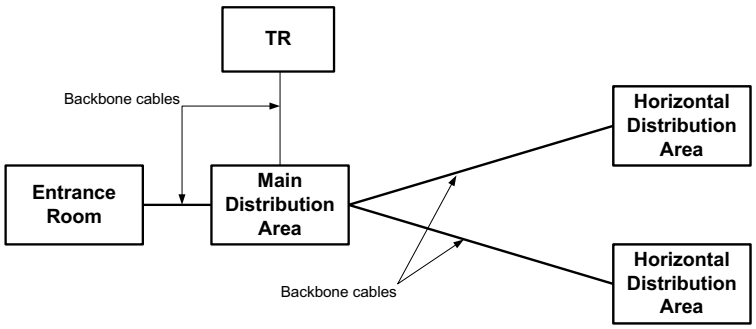


Figure 8: Typical backbone cabling using a star topology

The presence of the horizontal cross-connect is not mandatory. When the horizontal cross-connects are not used, the cabling extending from the main cross-connect to the mechanical termination in the equipment distribution area is considered horizontal cabling. If the horizontal cabling passes through the HDA, sufficient cable slack shall exist in the horizontal distribution area to allow movement of the cables when migrating to a cross-connect.

Backbone cabling cross-connects may be located in telecommunications rooms, equipment rooms, main distribution areas, horizontal distribution areas or at entrance rooms. In the case of multiple entrance rooms, direct backbone cabling to the horizontal cross-connect shall be allowed when distance limitations are encountered.

6.3.2.2 Accommodation of non-star configurations

The topology in figure 8, through the use of appropriate interconnections, electronics, or adapters in data center distribution areas, can often accommodate systems that are designed for non-star configurations such as ring, bus, or tree.

- Cabling between HDAs should be permitted to provide redundancy and to avoid exceeding legacy application distance restrictions.

6.3.3 Redundant cabling topologies

Redundant topologies can include a parallel hierarchy with redundant distribution areas. These topologies are in addition to the star topology specified in subclauses 6.2.2 and 6.3.2. See clause 8 for additional information.

6.3.4 Recognized media

Due to the wide range of services and site sizes where backbone cabling will be used, more than one transmission medium is recognized. This Standard specifies transmission media, which shall be used individually or in combination in the backbone cabling.

Recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet all applicable requirements specified in ANSI/TIA/EIA-568-B.2 and ANSI/TIA/EIA-568-B.3.

The recognized media are:

- 100-ohm twisted-pair cable (ANSI/TIA/EIA-568-B.2), category 6 recommended (ANSI/TIA/EIA-568-B.2-1);

- multimode optical fiber cable, either 62.5/125 micron or 50/125 micron (ANSI/TIA/EIA-568-B.3), 50/125 micron 850 nm laser optimized multimode fiber is recommended (ANSI/TIA-568-B.3-1);

- single-mode optical fiber cable (ANSI/TIA/EIA-568-B.3).

The recognized coaxial media are 75-ohm (734 and 735 type) coaxial cable (Telcordia Technologies GR-139-CORE) and coaxial connector (ANSI T1.404). These cables and connectors are recommended to support specific applications per annex A.

Channels constructed from recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet the requirements specified in ANSI/TIA/EIA-568-B.1, ANSI/TIA/EIA-568-B.2, ANSI/TIA/EIA-568-B.3 and ANSI T1.404 (DS3).

NOTES

1) Crosstalk between individual, unshielded twisted-pairs may affect the transmission performance of multipair copper cables. Annex B of ANSI/TIA/EIA-568-B.1 provides some shared sheath guidelines for multipair cables.

2) Annex C of ANSI/TIA/EIA-568-B.1 provides a brief description of a number of other backbone cables that have been used in telecommunications. These cables, as well as others, may be effective for specific applications. Although these cables are not part of the requirements of this Standard, they may be used in addition to the minimum requirements of this Standard.

3) See subclause 6.3.5 for backbone cabling distance limitations.

6.3.5 Backbone cabling distances

The maximum supportable distances are application and media dependent. The maximum backbone distances in annex A of this document provide application specific guidelines. To minimize cabling distances, it is often advantageous to locate the main cross-connect near the center of a site. Cabling installations that exceed these distance limits may be divided into areas, each of which can be supported by backbone cabling within the scope of this Standard. Interconnections between the individual areas, which are outside the scope of this Standard, may be accomplished by employing equipment and technologies normally used for wide area applications.

The length of category 3 multipair balanced 100 Ohm backbone cabling, that supports applications up to 16 MHz, should be limited to a total of 90 m (295 ft).

The length of category 5e and 6 balanced 100 Ohm backbone cabling should be limited to a total of 90 m (295 ft). The 90 m (295 ft) distance allows for an additional 5 m (16 ft) at each end for equipment cables (cords) connecting to the backbone.

Data centers typically utilize patch cords that are longer than 5 m (16 ft). In data centers that use longer patch cords, the maximum backbone cabling distances shall be reduced accordingly to ensure that the maximum channel lengths are not exceeded. See subclause 6.2.3.1 for maximum lengths for copper patch cord information.

NOTES

1) The 90 m (295 ft) distance limitation assumes uninterrupted cabling runs between cross-connects that serve equipment (i.e., no intermediate cross-connect).

2) Users of this document are advised to consult the specific standards associated with the planned service, or equipment manufacturers and systems integrators to determine the suitability of the cabling described herein for specific applications.

3) For copper cabling, in order to reduce the effect of multiple connections in close proximity on NEXT loss and return loss, the horizontal distribution area termination should be located at least 15 m (50 ft) from the main distribution area termination.

6.4 Choosing media

Cabling specified by this document is applicable to different application requirements within the data center environment. Depending upon the characteristics of the individual application, choices with respect to transmission media should be made. In making this choice, factors to be considered include:

a) flexibility with respect to supported services,

b) required useful life of cabling,

c) facility/site size and occupant population,

d) channel capacity within the cabling system,

e) equipment vendor recommendations or specifications.

Each recognized cable has individual characteristics that make it suitable for a myriad of applications and situations. A single cable may not satisfy all end user requirements. It may be necessary to use more than one medium in the backbone cabling. In those instances, the different media shall use the same facility architecture with the same location for cross-connects, mechanical terminations, interbuilding entrance rooms, etc.

6.5 Centralized optical fiber cabling

6.5.1 Introduction

Many single tenant users of optical fiber are implementing data networks with centralized electronics versus distributed electronics in the building. Centralized optical fiber cabling is designed as an alternative to the optical cross-connection located in the horizontal distribution area when deploying recognized optical fiber cable in the horizontal in support of centralized electronics.

Centralized cabling provides connections from equipment distribution areas to centralized cross-connects by allowing the use of pull-through cables, an interconnect, or splice in the horizontal distribution area.

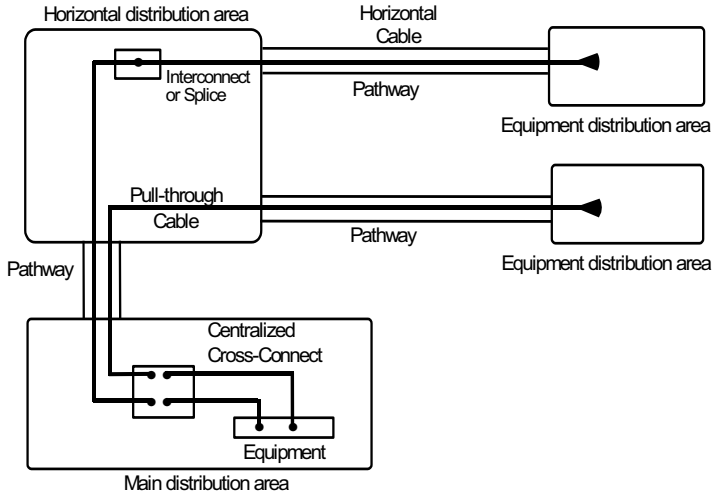


Figure 9: Centralized optical fiber cabling

6.5.2 Guidelines

The specifications of ANSI/TIA/EIA-568-B.1 shall be followed except the pull-through cable length shall be less than or equal to 300 m (984 ft) and, thus, the maximum horizontal cabling distance shall not exceed 300 m (984 ft) when a pull-through cable is used. Centralized cabling implementations shall be located within the same building as the equipment distribution areas served. The administration of moves, adds and changes shall be performed at the centralized cross-connect.

Centralized cabling design shall allow for migration (in part or in total) of the pull-through, interconnect, or splice implementation to a cross-connection implementation. Sufficient space shall be left in the horizontal distribution area to allow for the addition of patch panels needed for the migration of the pull-through, interconnect, or splice to a cross-connection. Sufficient cable slack shall exist in the horizontal distribution area to allow movement of the cables when migrating to a cross-connection.

Slack may be stored as cable or unjacketed fiber (buffered or coated). Slack storage shall provide bend radius control so that cable and fiber bend radius limitations are not violated. Cable slack may be stored within enclosures or on the rack/cabinet of the horizontal distribution area. Fiber slack shall be stored in protective enclosures.

Centralized cabling design shall allow for the addition and removal of horizontal and intrabuilding backbone fibers. The layout of the termination hardware should accommodate modular growth in an orderly manner.

The intrabuilding backbone subsystem should be designed with sufficient spare capacity to service additional outlet/connectors from the centralized cross-connect without the need to pull additional intrabuilding backbone cables. The intrabuilding backbone fiber count should be sized to deliver present and future applications to the maximum equipment distribution areas density within the area served by the horizontal distribution area. Generally, two fibers are required for each application delivered to an equipment distribution area.

Centralized cabling shall comply with the labeling requirements of ANSI/TIA/EIA-606-A and annex B of this Standard. In addition, horizontal distribution area splice and interconnect hardware shall be labeled with unique identifiers on each termination position. Field color-coding is not used at the interconnect or splice. The centralized cross-connect termination positions in the main distribution area shall be labeled as a blue field. The blue field shall move to the horizontal distribution area for each circuit that is converted to a cross-connection in the horizontal distribution area.

Centralized cabling shall be implemented to ensure the correct fiber polarity as specified in subclause 10.3.2 of ANSI/TIA/EIA-568-B.1.

6.6 Cabling transmission performance and test requirements

Transmission performance depends on cable characteristics, connecting hardware, patch cords and cross-connect wiring, the total number of connections, and the care with which they are installed and maintained. See ANSI/TIA/EIA-568-B.1, Clause 11 for field test specifications for post-installation performance measurements of cabling designed in accordance with this Standard.

7 DATA CENTER CABLING PATHWAYS

7.1 General

Except where otherwise specified, data center cabling pathways shall adhere to the specifications of ANSI/TIA-569-B.

7.2 Security for data center cabling

Telecommunications cabling for data centers shall not be routed through spaces accessible by the public or by other tenants of the building unless the cables are in enclosed conduit or other secure pathways. Any maintenance holes, pull boxes, and splice boxes shall be equipped with a lock.

Telecommunications entrance cabling for data centers should not be routed through a common equipment room (CER).

Any maintenance holes on building property or under control of the data center owner should be locked and monitored by the data center security system using a camera, remote alarm or both.

Access to pull boxes for data center cabling (entrance cabling or cabling between portions of the data center) that are located in public spaces or shared tenant spaces should be controlled. The pull boxes should also be monitored by the data center security system using a camera, remote alarm or both.

Any splice boxes for data center cabling that are located in public spaces or shared tenant spaces should be locked and monitored by the data center security system using a camera, remote alarm or both.

Entrance to utility tunnels used for telecommunications entrance rooms and other data center cabling should be locked. If the tunnels are used by multiple tenants or cannot be locked, telecommunications cabling for data centers shall be in rigid conduit or other secure pathway.

7.3 Separation of power and telecommunications cables

To minimize longitudinal coupling between power cables and twisted-pair copper cables, the separation distances outlined in this clause shall be provided. This separation is specified to accommodate the wide variety of equipment that may be present in a data center, but are not found in a typical office environment or telecommunications room.

7.3.1 Separation between electrical power and twisted-pair cables

The distances in table 2 shall be maintained between electrical power cables and twisted-pair cables. Electrical codes may require a barrier or greater separation than specified in table 2. Refer to NFPA 70, article 800 or applicable electrical code for additional information.

Table 2: Data center separation between twisted-pair and shielded power cables

Quantity of circuits	Electrical Circuit Type	Separation Distance (mm)	Separation Distance (in)
1 -15	20A 110/240V 1-phase shielded or unshielded	Refer to 569B annex C	Refer to 569B annex C
16 - 30	20A 110/240V 1-phase shielded	50 mm	2 in
31 - 60	20A 110/240V 1-phase shielded	100 mm	4 in
61-90	20A 110/240V 1-phase shielded	150 mm	6 in
91+	20A 110/240V 1-phase shielded	300 mm	12 in
1+	100A 415V 3-phase shielded feeder	300 mm	12 in

If the power cables are unshielded, then the separation distances provided in table 2 shall be doubled. However, these distances can apply to unshielded power cables if either the power cables or data cables are installed in bonded and grounded metal tray. The side or the bottom of the metal tray shall separate the power cables from the twisted-pair cables, this separation surface should be solid metal. Refer to NEMA VE 2-2001 for additional information on cable tray installation guidelines.

The shielding shall completely surround the cable (except at the receptacle) and shall be properly bonded and grounded in accordance with the applicable electrical codes.

There are no requirements for separation of power and telecommunications cabling crossing at right angles, except the separation requirements mandated by applicable electrical codes.

No separation distance is required when either the data cables or the power cables are enclosed in metallic raceway or conduit that meets the following requirements:

- the metallic raceway or conduit shall completely enclose the cables and be continuous;

- the metallic raceway or conduit shall be properly bonded and grounded in accordance with the applicable electrical codes;

- the raceway or conduit shall be at least 1 mm (0.04 in) thick if made of galvanized (low carbon) steel or 2 mm (0.08 in) thick if made of aluminum.

7.3.2 Practices to accommodate power separation requirements

It is normally possible to meet the recommended separation distances through thoughtful design and installation practices.

Branch circuits in data centers should be in watertight flexible metal conduit. Feeder circuits to power distribution units and panels should be installed in solid metal conduit. If the feeder circuits are not in solid metal conduit, they should be in watertight flexible metal conduit.

In data centers that use overhead cable trays, the normal separation distances provided by standard practices provides adequate separation. As specified in ANSI/TIA-569-B, a minimum of 300 mm (12 in) access headroom between the top of a tray or runway and the bottom of the tray or runway above shall be provided and maintained. This provides adequate separation if the electrical cables are shielded or if the power cable tray meets the specifications of the subclause 7.3.1 and is above the telecommunications cable tray or runway.

In data centers that employ access floor systems, adequate separation of power and telecommunications cabling can be accommodated through the following measures:

- in the main aisles, allocate separate aisles for power and telecommunications cabling, if possible;

- where it is not possible to allocate separate aisles for power and telecommunications cabling in the main aisles, then provide both horizontal and vertical separation of power and telecommunications cables. Provide horizontal separation by allocating different rows of tiles in the main aisles for power and telecommunications cabling, with the power and telecommunications cables as far apart from each other as possible. Additionally, provide vertical separation by placing the telecommunications cabling in cable trays or baskets as far above the power cables as possible, preferably with the top of the cable tray or basket 20 mm (0.75 in) below the bottom of the access floor tile;

- in the equipment cabinet aisles, allocate separate aisles for power and telecommunications cabling. Refer to subclause 5.11.2 for additional information on “hot” and “cold” aisles.

7.3.3 Separation of fiber and copper cabling

Fiber and copper cabling in cable trays and other jointly used pathways should be separated so that it improves administration, operation, and minimize damage to smaller diameter fiber cables. Physical barriers between the two types of cables are not necessary.

Where it is not practical to separate fiber and copper cables, fiber cables should be on top of copper cables.

7.4 Telecommunications entrance pathways

7.4.1 Entrance pathway types

Telecommunications entrance pathways for data centers should be located underground. Aerial entrance pathways for telecommunications service entrance pathways are not recommended because of their vulnerability due to physical exposure.

7.4.2 Diversity

Refer to ANSI/TIA-569-B for information regarding entrance pathway diversity.

7.4.3 Sizing

The number of entrance conduits required depends on the number of access providers that will provide service to the data center, and the number and type of circuits that the access providers will provide. The entrance pathways should also have adequate capacity to handle growth and additional access providers.

Each access provider should have at least one 100 mm (4 in) trade size conduit at each entrance point. Additional conduits may be required for campus. Conduits used for optical fiber entrance cables should have three innerducts [two 38 mm (1.5 in) and one 25 mm (1.0 in) or three 33 mm (1.25 in)].

7.5 Access floor systems

7.5.1 General

Access floor systems, also known as raised floor systems, should be used in data centers that support equipment that is designed to be cabled from below.

Cables shall not be left abandoned under the access floor. Cables shall be terminated on at least one end in the main distribution area or a horizontal distribution area, or shall be removed.

For additional information on rack and cabinet installation with access flooring systems, refer to subclause 5.11.

7.5.2 Cable trays for telecommunications cabling

Telecommunications cabling under the access floor shall be in ventilated cable trays that do not block airflow. See ANSI/TIA-569-B for further cable tray design considerations. Under floor cable trays may be installed in multiple layers to provide additional capacity. Metallic cable tray shall be bonded to the data center grounding infrastructure. The cable tray should have a maximum depth of 150 mm (6 in).

Under-floor cable tray routing should be coordinated with other under floor systems during the planning stages of the building. Refer to NEMA VE 2-2001 for recommendations regarding installation of cable trays.

7.5.3 Access floor performance requirements

Access flooring shall meet the performance requirements of ANSI/TIA-569-B subclause 8.5 and annex B.2.

Access floors for data centers should use a bolted stringer understructure, as they are more stable over time than stringerless systems. Additionally, access floor stringers should be 1.2 m (4 ft) long installed in a “herringbone” pattern to improve stability. Pedestals should be bolted to the subfloor for added stability.

7.5.4 Floor tile cut edging

Access floor tile cuts should have edging or grommets along all cut edges. If the edging or grommets are higher than the surface of the access floor, they shall be installed as not to interfere with placement of racks and cabinets. The edging or grommets shall not be placed where the racks and cabinets normally contact the surface of the access floor.

In the case of floor discharge HVAC systems, floor tile cuts should be limited in both size and quantity to ensure proper airflow. It is recommended that the HVAC system be properly balanced once all equipment racks, cabinets, etc are in-place. The HVAC system should be re-balanced with the addition of floor cuts, equipment racks, cabinets, etc.

7.5.5 Cable types under access floors

In some jurisdictions, plenum cable is the minimum requirement for telecommunications cabling under computer room access floors. Consult the AHJ before deciding on the type of cable to use under access floors.

> NOTE – This standard references applicable requirements relating to fire, health and safety. In addition, consider the selection of cable types and fire suppression practices that minimize damage in the event of fire.

7.6 Overhead cable trays

7.6.1 General

Overhead cable tray systems may alleviate the need for access floors in data centers that do not employ floor-standing systems that are cabled from below.

Overhead cable trays may be installed in several layers to provide additional capacity. Typical installations include two or three layers of cable trays, one for power cables and one or two for telecommunications cabling. One of the cable tray layers typically has brackets on one side that hold the data center grounding infrastructure. These overhead cable trays are often supplemented by a duct or tray system for fiber patch cables. The fiber duct or tray may be secured to the same hanging rods used to support the cable trays.

Cables shall not be left abandoned in overhead cable trays. Cables shall be terminated on at least one end in the main distribution area or a horizontal distribution area, or shall be removed.

In aisles and other common spaces in internet date centers, co-location facilities, and other shared tenant data centers, overhead cable trays should have solid bottoms or be placed at least 2.7 m (9 ft) above the finished floor to limit accessibility or be protected through alternate means from accidental and/or intentional damage.

The maximum recommended depth of any cable tray is 150 mm (6 in).

7.6.2 Cable tray support

Overhead cable trays should be suspended from the ceiling. If all racks and cabinets are of uniform height, the cable trays may be attached to the top of racks and cabinets, but this is not a recommended practice because suspended cable trays provide more flexibility for supporting cabinets and racks of various heights, and provide more flexibility for adding and removing cabinets and racks.

Typical cable tray types for overhead cable installation include telco-type cable ladders, center spine cable tray, or wire basket cable tray. If required by prevailing code, adjacent sections of cable tray shall be bonded together and grounded per AHJ, and shall be listed by a nationally recognized testing laboratory (NRTL) for this purpose. The cable tray system should be bonded to the data center grounding infrastructure.

7.6.3 Coordination of cable tray routes

Planning of overhead cable trays for telecommunications cabling should be coordinated with architects mechanical engineers, and electrical engineers that are designing lighting, plumbing, air ducts, power, and fire protection systems. Lighting fixtures and sprinkler heads should be placed between cable trays, not directly above cable trays.

8 DATA CENTER REDUNDANCY

8.1 Introduction

Data Centers that are equipped with diverse telecommunications facilities may be able to continue their function under catastrophic conditions that would otherwise interrupt the data center's telecommunications service. This Standard includes four tiers relating to various levels of availability of the data center facility infrastructure. Information on infrastructure tiers can be found in annex G. The Figure 10 illustrates various redundant telecommunications infrastructure components that can be added to the basic infrastructure.

The reliability of the communications infrastructure can be increased by providing redundant cross-connect areas and pathways that are physically separated. It is common for data centers to have multiple access providers providing services, redundant routers, redundant core distribution and edge switches. Although this network topology provides a certain level of redundancy, the duplication in services and hardware alone does not ensure that single points of failure have been eliminated.

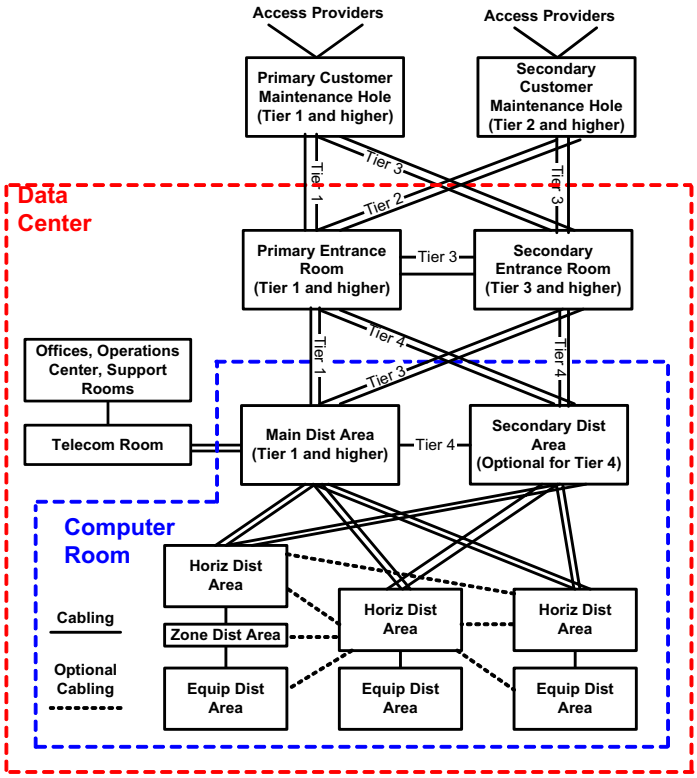


Figure 10: Telecommunications infrastructure redundancy

8.2 Redundant maintenance holes and entrance pathways

Multiple entrance pathways from the property line to the entrance room(s) eliminate a single point of failure for access provider services entering the building. These pathways will include customer-owned maintenance holes where the access provider conduits do not terminate at the building wall. The maintenance holes and entrance pathways should be on opposite sides of the building and be at least 20 m (66 ft) apart.

In data centers with two entrance rooms and two maintenance holes, it is not necessary to install conduits from each entrance room to each of the two maintenance holes. In such a configuration, each access provider is typically requested to install two entrance cables, one to the primary entrance room through the primary maintenance hole, and one to the secondary entrance room through the secondary maintenance hole. Conduits from the primary maintenance hole to the secondary entrance room and from the secondary maintenance hole to the primary maintenance hole provide flexibility, but are not required.

In data centers with two entrance rooms, conduits may be installed between the two entrance rooms to provide a direct path for access provider cabling between these two rooms (for example, to complete a SONET or SDH ring).

8.3 Redundant access provider services

Continuity of telecommunications access provider services to the data center can be ensured by using multiple access providers, multiple access provider central offices, and multiple diverse pathways from the access provider central offices to the data center.

Utilizing multiple access providers ensures that service continues in the event of a access provider-wide outage or access provider financial failure that impacts service.

Utilizing multiple access providers alone does not ensure continuity of service, because access providers often share space in central offices and share rights-of-way.

The customer should ensure that its services are provisioned from different access provider central offices and the pathways to these central offices are diversely routed. These diversely routed pathways should be physically separated by at least 20 m (66 ft) at all points along their routes.

8.4 Redundant entrance room

Multiple entrance rooms may be installed for redundancy rather than simply to alleviate maximum circuit distance restrictions. Multiple entrance rooms improve redundancy, but complicate administration. Care should be taken to distribute circuits between entrance rooms.

Access providers should install circuit provisioning equipment in both entrance rooms so that circuits of all required types can be provisioned from either room. The access provider provisioning equipment in one entrance room should not be subsidiary to the equipment in the other entrance room. The access provider equipment in each entrance room should be able to operate in the event of a failure in the other entrance room.

The two entrance rooms should be at least 20 m (66 ft) apart and be in separated fire protection zones. The two entrance rooms should not share power distribution units or air conditioning equipment.

8.5 Redundant main distribution area

A secondary distribution area provides additional redundancy, but at the cost of complicating administration. Core routers and switches should be distributed between the main distribution area and secondary distribution area. Circuits should also be distributed between the two spaces.

A secondary distribution area may not make sense if the computer room is one continuous space, as a fire in one portion of the data center will likely require that the entire data center be shut down. The secondary distribution area and main distribution area should be in different fire

protection zones, be served by different power distribution units, and be served by different air conditioning equipment.

8.6 Redundant backbone cabling

Redundant backbone cabling protects against an outage caused by damage to backbone cabling. Redundant backbone cabling may be provided in several ways depending on the degree of protection desired.

Backbone cabling between two spaces, for example, a horizontal distribution area and a main distribution area, can be provided by running two cables between these spaces, preferably along different routes. If the data center has both a main distribution area and a secondary distribution area, redundant backbone cabling to the horizontal distribution area is not necessary, though the routing of cables to the main distribution area and secondary distribution area should follow different routes.

Some degree of redundancy can also be provided by installing backbone cabling between horizontal distribution areas. If the backbone cabling from the main distribution area to horizontal distribution area is damaged, connections can be patched through another horizontal distribution area.

8.7 Redundant horizontal cabling

Horizontal cabling to critical systems can be diversely routed to improved redundancy. Care should be taken not to exceed maximum horizontal cable lengths when selecting paths.

Critical systems can be supported by two different horizontal distribution areas as long as maximum cable length restrictions are not exceeded. This degree of redundancy may not provide much more protection than diversely routing the horizontal cabling if the two horizontal distribution areas are in the same fire protection zone.

ANNEX A (INFORMATIVE) CABLING DESIGN CONSIDERATIONS

This annex is informative only and is not part of this Standard.

A.1 Cabling application distances

The cabling distances presented here are informative only.

The maximum supportable distances proposed in this annex are application and media dependent.

The use of 100-Ohm twisted-pair cable (4-pair category 6 is recommended) is based on the following applications:

- 1000 Mb/s LAN connections;
- termination of T1 and lower speed circuits in the end equipment area;
- facilities management and monitoring;
- out-of-band management;
- power management;
- security systems.

The use of 75-ohm coaxial (734 type) cable is based on the provisioning of T-3 circuits from the access provider to the end equipment area.

The use of current 62.5/125 μm multimode fiber (160/500 MHz•km) is based on the following applications:

- 1000 Mb/s Ethernet (1000BASE-SX);
- 100 Mb/s (133 MBaud) Fibre Channel (100-M6-SN-I);
- 200 Mbps (266 MBaud) Fibre Channel (200-M6-SN-I).

The use of current 50/125 μm multimode fiber (500/500 MHz•km) is based on the following applications:

- 1000 Mb/s Ethernet (1000BASE-SX);
- 100 Mb/s (133 MBaud) Fibre Channel (100-M5-SN-I);
- 200 Mbps (266 MBaud) Fibre Channel (200-M5-SN-I).

The use of 850-nm laser-optimized 50/125 μm multimode fiber (1500/500 MHz•km; 2000 MHz•km effective modal bandwidth) is based on the following applications:

- 1000 Mb/s Ethernet (1000BASE-SX);

- 10 Gb/s Ethernet (10GBASE-S);

- 100 Mb/s (133 MBaud) Fibre Channel (100-M5-SN-I);

- 200 Mbps (266 MBaud) Fibre Channel (200-M5-SN-I);

- 1200 Mbps (1062 MBaud) Fibre Channel (1200-M5E-SN-I).

The use of single-mode fiber, as per ANSI/TIA/EIA-568-B.3, is based on the following applications:

- 10 Gb/s and higher LAN & SAN connections;

- distances in excess of those recommended for 850-nm laser-optimized 50/125 μm multimode fiber.

A.1.1 T-1, E-1, T-3 and E-3 circuit distances

The following table 3 provides the maximum circuit distances for T-1, T-3, E-1, and E-3 circuits with no adjustments for intermediate patch panels or outlets between the circuit demarcation point and the end equipment. These calculations assume that there is no customer DSX panel between the access provider demarcation point (which may be a DSX) and the end equipment. The access provider DSX panel is not counted in determining maximum circuit lengths.

Table 3: Maximum circuit distances with no customer DSX panel

Circuit type	Category 3 UTP	Category 5e & 6 UTP	734 Type Coaxial	735 Type Coaxial
T-1	170 m (557 ft)	206 m (677 ft)	-	-
CEPT-1 (E-1)	126 m (412 ft)	158m (517 ft)	395m (1297 ft)	177 m (580 ft)
T-3	-	-	160 m (524 ft)	82 m (268 ft)
CEPT-3 (E-3)	-	-	175 m (574 ft)	90 m (294 ft)

NOTE: The distances shown in table 3 are for the specific applications used in data centers and may be different from the distances supported for various applications in TIA-568-B.

Repeaters can be used to extend circuits beyond the lengths specified above.

These circuit distances should be adjusted for attenuation losses caused by a DSX panel between the access provider demarcation point (which may be a DSX panel) and the end equipment. The following table 4 provides the reduction caused by DSX panels in maximum circuit distances for T-1, T-3, E-1, and E-3 circuits over the recognized media type.

Table 4: Reduction in circuit distances for customer DSX panel

Circuit type	Category 3 UTP	Category 5e & 6 UTP	734 Type Coaxial	735 Type Coaxial
T-1	11 m (37 ft)	14 m (45 ft)	-	-
CEPT-1 (E-1)	10 m (32 ft)	12 m (40 ft)	64 m (209 ft)	28 m (93 ft)
T-3	-	-	13 m (44 ft)	7 m (23 ft)
CEPT-3 (E-3)	-	-	15 m (50 ft)	8 m (26 ft)

Maximum circuit distances should be adjusted for attenuation losses caused by intermediate patch panels and outlets. The following table 5 provides the reduction in maximum circuit distances for T-1, T-3, E-1, and E-3 circuits over the recognized media type.

Table 5: Reduction in circuit distances per patch panel or outlet

Circuit type	Category 3 UTP	Category 5e & 6 UTP	734 Type Coaxial	735 Type Coaxial
T-1	4.0 m (13.0 ft)	1.9 m (6.4 ft)	-	-
CEPT-1 (E-1)	3.9 m (12.8 ft)	2.0 m (6.4 ft)	22.1 m (72.5 ft)	9.9 m (32.4 ft)
T-3	-	-	4.7 m (15.3 ft)	2.4 m (7.8 ft)
CEPT-3 (E-3)	-	-	5.3 m (17.5 ft)	2.7 m (8.9 ft)

In the typical data center, there are a total of 3 connections in the backbone cabling, 3 connections in the horizontal cabling and no DSX panels between the access provider demarcation point and the end equipment:

Backbone cabling:

- one connection in the entrance room,
- two connections in the main cross-connect,

Horizontal cabling:

- two connections in the horizontal cross-connect, and
- an outlet connection at the equipment distribution area.

This ‘typical’ configuration corresponds to the typical data center with an entrance room, main distribution area, one or more horizontal distribution areas, and no zone distribution areas. Maximum circuit lengths for the typical data center configuration are in the following table 6. These maximum circuit lengths include backbone cabling, horizontal cabling, and all patch cords or jumpers between the access provider demarcation point and the end equipment.

Table 6: Maximum circuit distances for the typical data center configuration

Circuit type	Category 3 UTP	Category 5e & 6 UTP	734 Type Coaxial	735 Type Coaxial
T-1	146 m (479 ft)	198 m (648 ft)	-	-
CEPT-1 (E-1)	102 m (335 ft)	146 m (478 ft)	263 m (862 ft)	117m (385 ft)
T-3	-	-	132 m (432 ft)	67 m (221 ft)
CEPT-3 (E-3)	-	-	143 m (469 ft)	73 m (240 ft)

With maximum horizontal cable lengths, maximum patch cord lengths, no customer DSX, and no zone outlets, the maximum backbone cable lengths for a 'typical' data center where T-1, E-1, T-3, or E-3 circuits can be provisioned to equipment anywhere in the data center are shown in the following table 7. This 'typical' configuration assumes that the entrance room, main distribution area, and horizontal distribution areas are separate rather than combined. The maximum backbone cabling distance is the sum of the length of cabling from the entrance room to the main distribution area and from the main distribution area to the horizontal distribution area.

Table 7: Maximum backbone for the typical data center configuration

Circuit type	Category 3 UTP	Category 5e & 6 UTP	734 Type Coaxial	735 Type Coaxial
T-1	8 m (27 ft)	60 m (196 ft)	-	-
CEPT-1 (E-1)	0 m (0 ft)	8 m (26 ft)	148 m (484 ft)	10m (33 ft)
T-3	-	-	17 m (55 ft)	0 m (0 ft)
CEPT-3 (E-3)	-	-	28 m (92 ft)	0 m (0 ft)

These calculations assume the following maximum patch cord lengths in the 'typical' data center:

- 10 m (32.8 ft) for UTP and fiber in the entrance room, main distribution area, and horizontal distribution area;

- 5 m (16.4 ft) for 734-type coaxial cable in the entrance room, main distribution area, and horizontal distribution area;

- 2.5 m (8.2 ft) for 735-type coaxial cable in the entrance room, main distribution area, and horizontal distribution area.

Due to the very short distances permitted by category 3 UTP cabling and 735 type coaxial cable for T-1, T-3, E-1, and E-3 circuits, category 3 UTP and 735-type coaxial cables are not recommended for supporting these types of circuits.

Backbone cabling distances can be increased by limiting the locations where T-1, E-1, T-3, and E-3 circuits will be located (for example only in the main distribution area or locations served by horizontal cabling terminated in the main distribution area).

Other options include provisioning circuits from equipment located in the main distribution area or horizontal distribution area.

A.1.2 EIA/TIA-232 and EIA/TIA-561 console connections

The recommended maximum distances for EIA-TIA-232-F and EIA/TIA-561/562 console connections up to 20 kb/s are:

- 23.2 m (76.2 ft) over category 3 unshielded twisted-pair cable;

- 27.4 m (89.8 ft) over category 5e or category 6 unshielded twisted-pair cable.

The recommended maximum distances for EIA-TIA-232-F and EIA/TIA-561/562 console connections up to 64 kb/s are:

- 8.1 m (26.5 ft) over category 3 unshielded twisted-pair cable;

- 9.5 m (31.2 ft) over category 5e or category 6 unshielded twisted-pair cable.

Recommended maximum distances over shielded twisted-pair cables are one half of the distances permitted over unshielded twisted-pair cables.

A.1.3 Other application distances

As 1 and 10 Gigabit fiber applications are introduced into networks the physical limitations and properties of optical fiber introduce new challenges for a network designer. Due to the increased data rate, fiber effects, such as dispersion, become a factor in the achievable distances and numbers of connectors used in fiber optic link designs. This leaves the network designer with new decisions and trade-offs that they must understand and overcome. Refer to the information provided in ANSI/TIA/EIA-568-B.1 and Addendum 3 to ANSI/TIA/EIA-568-B.1 regarding supportable distances and channel attenuation for optical fiber applications by fiber type.

A.2 Cross-connections

In the entrance room, main distribution area and horizontal distribution area, jumper and patch cord lengths used for cross-connection to backbone cabling should not exceed 20 m (66 ft).

The only exception to these length restrictions should be in the case of 75-ohm coaxial cables, for DS-3 patching, the maximum length should be 5 m (16.4 ft) for type 734 coaxial and 2.5 m (8.2 ft) for type 735 coaxial in the entrance room, main cross-connect, and horizontal cross-connects.

A.3 Separation of functions in the main distribution area

The main distribution area should have separate racks for copper-pair, coaxial cable, and optical fiber distribution unless the data center is small and the main cross-connect can fit in one or two racks. Separate patching bays for copper-pair cables, coaxial cables, and optical fiber cables simplify management and serves to minimize the size of each type of patching bay. Arrange patching bays and equipment in close proximity to minimize patch cord lengths.

A.3.1 Twisted-pair main cross-connect

The twisted-pair main cross-connect (MC) supports twisted-pair cable for a wide range of applications including low speed circuits, T-1, E-1, consoles, out-of-band management, KVM, and LANs.

Consider installing category 6 twisted-pair cabling for all copper-pair cabling from the MC to the intermediate cross-connects (ICs) and HCs, as this will provide maximum flexibility for supporting a wide variety of applications. High pair count (25-pair or higher) category 3 twisted-pair

backbone is satisfactory for cabling from the MC to the HC and low-speed circuit demarcation area in the entrance room. Cabling from the E-1/T-1 demarcation area in the entrance room should be 4-pair category 5e or category 6 twisted-pair cable.

The type of terminations in the MC (IDC connecting hardware or patch panels) depends on the desired density and where the conversion from 1- and 2-pair access provider cabling to 4-pair computer room structured cabling occurs:

- if the conversion from 1- and 2-pair access provider cabling occurs in the entrance room, then copper-pair cable terminations in the MC are typically on patch panels. This is the recommended configuration;

- if the conversion from 1- and 2-pair access provider cabling occurs in the MC, then copper-pair cable terminations in the MC should be on IDC connecting hardware.

A.3.2 Coaxial main cross-connect

The coaxial MC supports coaxial cable for T-3 and E-3 cabling (two coaxial cables per circuit). All coaxial cabling should be 734-type coaxial cable.

Termination of coaxial cables should be on patch panels with 75-ohm BNC connectors. The BNC connectors should be female-BNC on both the front and back of the patch panels.

A.3.3 Optical fiber main cross-connect

The fiber MC supports optical fiber cable for local area networks, storage area networks, metropolitan area networks, computer channels, and SONET circuits.

Termination of fiber cables should be on fiber patch panels.

A.4 Separation of functions in the horizontal distribution area

Horizontal distribution areas should have separate cabinets or racks for copper-pair, coaxial cable, and optical fiber distribution unless the horizontal cross-connect is small and only requires one or two racks. Separate patching bays for copper-pair cables, coaxial cables, and optical fiber cables simplify management and minimize the size of each type of patching bay. Arrange patching bays and equipment in close proximity to minimize patch cord lengths.

The use of a single type of cable simplifies management and improves flexibility to support new applications. Consider installing only one type of twisted-pair cable for horizontal cabling, (for example all category 5e or all category 6 UTP), rather than installing different types of twisted-pair cables for different applications.

A.5 Cabling to telecommunications equipment

The length of the cable used to connect voice telecommunications equipment (such as PBX’s) directly to the main distribution area should not exceed 30 m (98 ft).

The length of the cable used to connect voice telecommunications equipment (such as PBX’s) directly to the horizontal distribution area should not exceed 30 m (98 ft).

A.6 Cabling to end equipment

Equipment cord lengths from the ZDA should be limited to a maximum of 22 m (72 ft) in the case of copper or fiber optic cabling.

If individual telecommunications outlets are located on the same equipment rack or cabinet as the equipment served in lieu of a ZDA, equipment cord lengths should be limited to 5 m (16 ft).

A.7 Fiber design consideration

High termination density can be achieved using multi-fiber increments and the use of multi-fiber connectors. If cable lengths can be accurately pre-calculated, pre-terminated multi-fiber ribbon assemblies can reduce installation time. In these cases, consideration of the effects of additional connections should be considered to ensure overall fiber system performance. High data-rate end equipment may accommodate multi-fiber connectors directly.

A.8 Copper design consideration

The patch panels should provide adequate space for labeling of each patch panel with its identifier as well as labeling each port as per annex B and ANSI/TIA/EIA-606-A requirements.

ANNEX B (INFORMATIVE) TELECOMMUNICATIONS INFRASTRUCTURE ADMINISTRATION

This annex is informative only and is not part of this Standard.

B.1 General

Data centers should adhere to ANSI/TIA/EIA-606-A with the exceptions noted in this Standard.

B.2 Identification scheme for floor space

Floor space should track the data center grid. Most data centers will require at least two letters and two numeric digits to identify every 600 mm x 600 mm (or 2 ft x 2 ft) floor tile. In such data centers, the letters will be AA, AB, AC… AZ, BA, BB, BC… and so on. For an example, see figure 11.

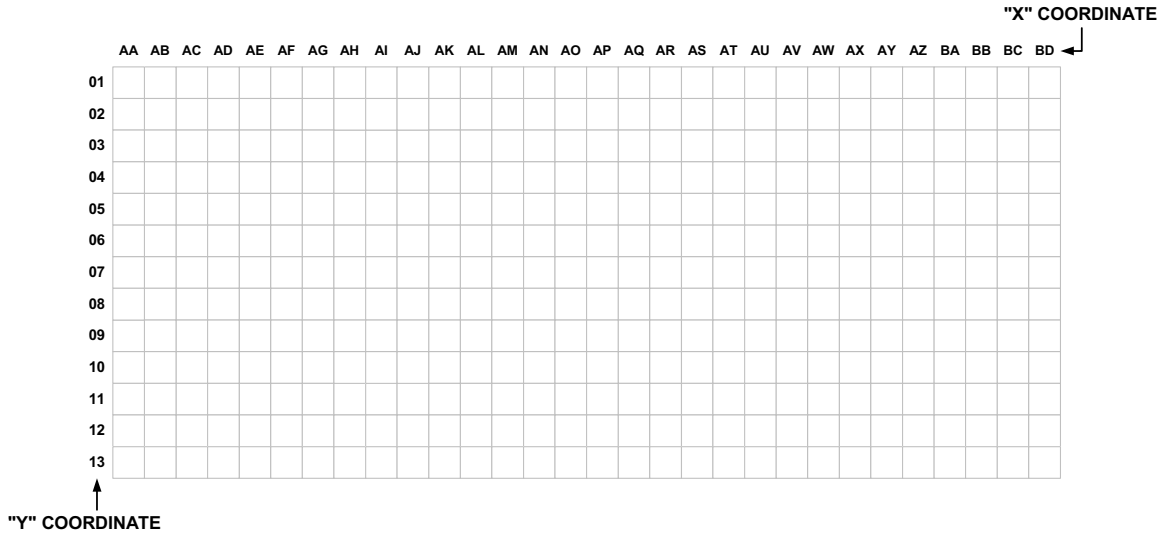


Figure 11: Sample floor space identifiers

B.3 Identification scheme for racks and cabinets

All racks and cabinets should be labeled in the front and back.

In computer rooms with access floors, label cabinets and racks using the data center grid. Each rack and cabinet should have a unique identifier based on floor tile coordinates. If cabinets rest on more than one tile, the grid location for the cabinets can be determined by using the same corner on every cabinet (e.g., the right front corner).

The cabinet or rack ID should consist of one or more letters followed by one or more numbers. The numeric portion of the ID will include leading 0's. So the cabinet whose front right corner is at tile AJ05 will be named AJ05.

In data centers with multiple floors, the floor number should be added as a prefix to the cabinet number. For example, 3AJ05 for the cabinet whose front right corner is at tile AJ05 on the 3rd floor of the data center. A sample floor space administration schema follows:

nx_1y_1

Where:

n = Where data center space is present in more than one floor in a building, one or more numeric characters designating the floor on which the space is located.

x_1y_1 = One or two alphanumeric characters followed by two alphanumeric characters designating the location on the floor space grid where the right front corner of the rack or cabinet is located. In figure 12, the Sample Cabinet is located at AJ05.

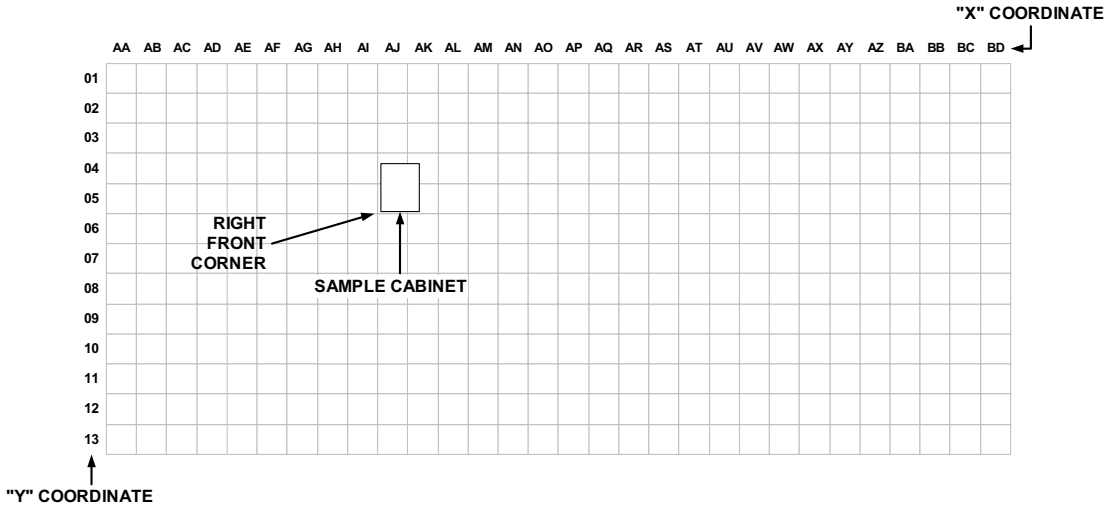


Figure 12: Sample rack/cabinet identifier

In computer rooms without access floors, use row number and position within the row to identify each rack and cabinet.

In Internet data centers and co-location facilities, where the computer room is subdivided into customer cages and rooms, the identification scheme can use cage/room names and cabinet or rack number within the cage/room.

B.4 Identification scheme for patch panels

1) Patch Panel Identifier

The identification scheme for patch panels should include cabinet or rack name and one or more characters that indicate the patch panel position in the cabinet or rack. Horizontal wire management panels do not count when determining patch panel position. If a rack has more than 26 panels, then two characters will be required to identify the patch panel. A sample patch panel administration schema follows:

x_1y_1-a

Where:

a = One to two characters designating the patch panel location within cabinet or rack x_1y_1, beginning at the top of the cabinet or rack. See figure 13 for typical copper patch panel designation.

2) Patch Panel Port Identifier

Two or three characters are used to specify the port number on the patch panel. Thus, the 4th port on the 2nd panel in cabinet 3AJ05 may be named 3AJ05-B04. A sample patch panel port administration schema follows:

x_1y_1-an

Where:

n = One to three characters designating the port on a patch panel. For copper patch panels, two to three numeric characters. For fiber patch panels, one alpha character, which identifies the connector panel located within the patch panel, starting sequentially from "A" excluding "I" and "O," followed by one or two numeric characters designating a fiber strand.

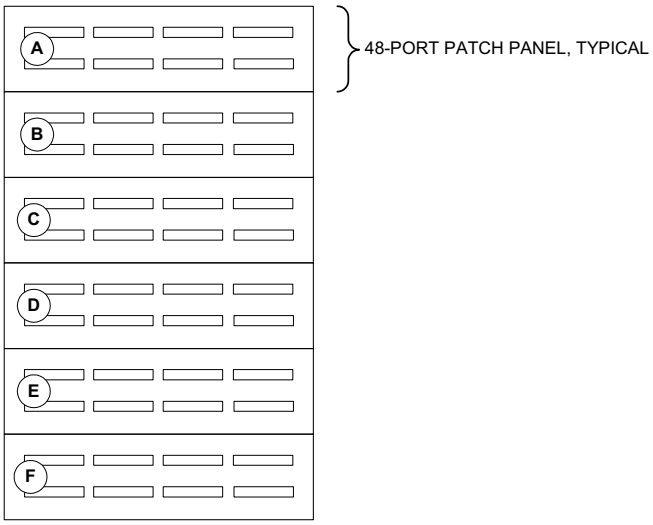


Figure 13: Sample copper patch panel identification schema

3) Patch panel connectivity identifier

Patch panels should be labeled with the patch panel identifier and patch panel port identifiers of the patch panel followed by the patch panel identifier and patch panel port identifiers of the patch panels or outlets at the other end of the cables. A sample patch panel connectivity administration schema follows:

p_1 to p_2

Where:

p_1 = Near end rack or cabinet, patch panel sequence, and port number range.

p_2 = Far end rack or cabinet, patch panel sequence, and port number range.

Consider supplementing ANSI/TIA/EIA-606-A cable labels with sequence numbers or other identifiers to simplify troubleshooting. For example, the 24-port patch panel with 24 category 6 cables from the MDA to HDA1 could include the label above, but could also include the label 'MDA to HDA1 Cat 6 UTP 1 – 24'.

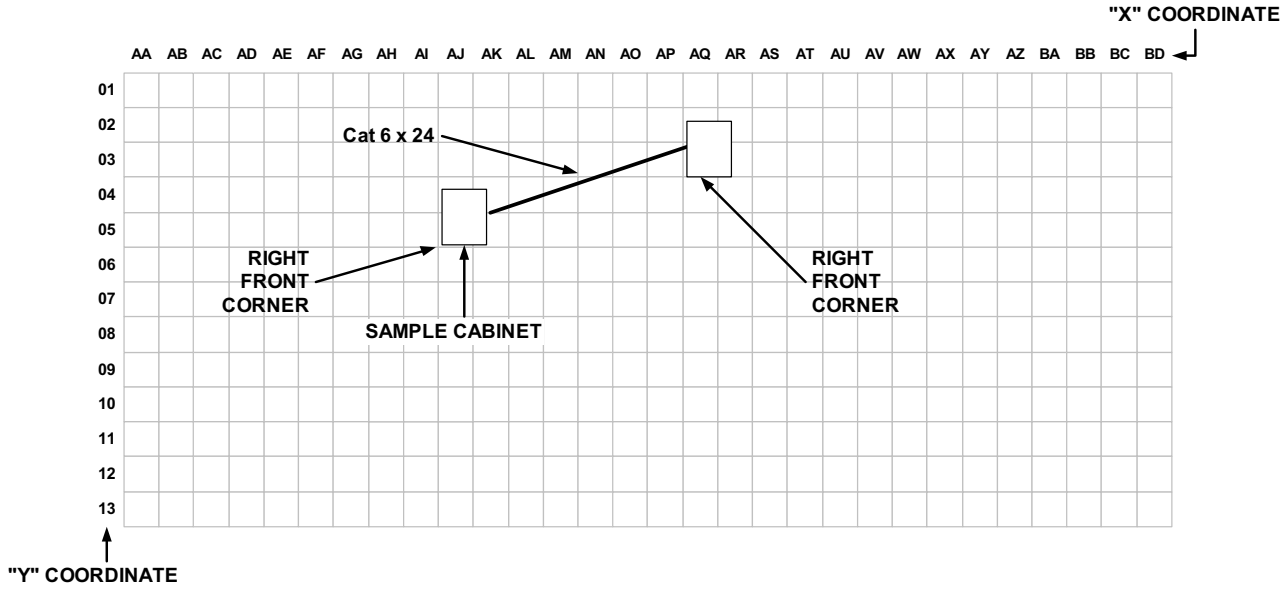


Figure 14: Sample 8-position modular patch panel labeling – Part I

For example, figure 15 shows a label for a 24-position modular patch panel with 24 category 6 cables interconnecting cabinet AJ05 to AQ03 as shown in figure 14.

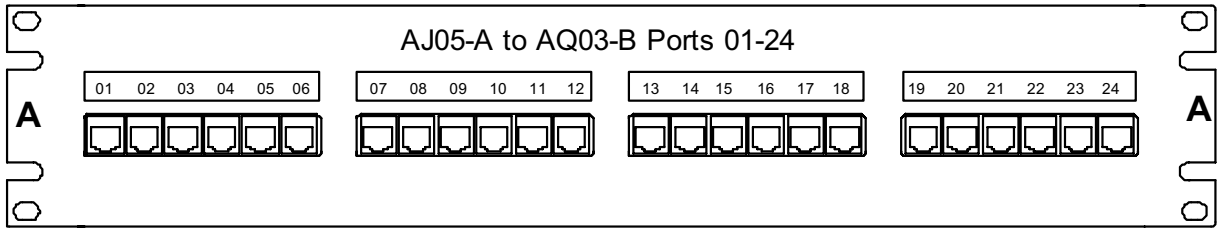


Figure 15: Sample 8-position modular patch panel labeling – Part II

B.5 Cable and patch cord identifier

Cables and patch cords should be labeled on both ends with the name of the connection at both ends of the cable.

Consider color-coding patch cables by application and type. A sample cable and patch cord administration schema follows:

p_{1n} / p_{2n}

Where:

p_{1n} = The near end rack or cabinet, patch panel sequence, and port designator assigned to that cable.

p_{2n} = The far end rack or cabinet, patch panel sequence, and port designator assigned to that cable.

For example, the cable connected to first position of the patch panel shown in figure 15 may contain the following label:

AJ05-A01 / AQ03-B01

and the same cable at cabinet AQ03 would contain the following label:

AQ03-B01 / AJ05-A01

ANNEX C (INFORMATIVE) ACCESS PROVIDER INFORMATION

This annex is informative only and is not part of this Standard.

C.1 Access provider coordination

C.1.1 General

Data center designers should coordinate with local access providers to determine the access providers' requirements and to ensure that the data center requirements are provided to the access providers.

C.1.2 Information to provide to access providers

Access providers will typically require the following information for planning entrance rooms for a data center:

- address of the building;
- general information concerning other uses of the building, including other tenants;
- plans of telecommunications entrance conduits from the property line to the entrance room, including location of maintenance holes, hand holes, and pull boxes;
- assignment of conduits and innerducts to the access provider;
- floor plans for the entrance facilities;
- assigned location of the access providers protectors, racks, and cabinets;
- routing of cables within entrance room (under access floor, overhead cable ladders, other);
- expected quantity and type of circuits to be provisioned by the access provider;
- date that the access provider will be able to install entrance cables and equipment in the entrance room;
- requested location and interface for demarcation of each type of circuit to be provided by the access provider;
- requested service date;
- name, telephone number, and email address of primary customer contact and local site contact.

C.1.3 Information that the access providers should provide

The access provider should provide the following information:

- space and mounting requirements for protectors on copper-pair cables;
- quantity and dimensions of access provider racks and cabinets;

- power requirements for equipment, including receptacle types;

- service clearances;

- installation and service schedule.

C.2 Access provider demarcation in the entrance room

C.2.1 Organization

The entrance room will have up to four separate areas for access provider demarcation:

- demarcation for low-speed copper-pair circuits, including DS-0, ISDN BRI, and telephone lines;

- demarcation for high-speed DS-1 (T-1 or fractional T-1, ISDN PRI) or CEPT-1 (E-1) copper-pair circuits;

- demarcation for circuits delivered on coaxial cable including DS-3 (T-3) and CEPT-3 (E-3);

- demarcation for optical fiber circuits (for example, SONET OC-x, SDH STM-x, FDDI, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet).

Ideally, all access providers provide demarcation for their circuits in the same location rather than in their own racks. This simplifies cross-connects and management of circuits. The centralized location for demarcation to all access providers is often called meet-me areas or meet-me racks. There should be separate meet-me or demarcation areas or racks for each type of circuit; low speed, E-1/T-1, E-3/T-3, and optical fiber. Cabling from the computer room to the entrance room should terminate in the demarcation areas.

If an access provider prefers to demarcate their services in their racks, the customer can install tie-cables from that access provider’s demarcation point to the desired meet-me/demarcation area.

C.2.2 Demarcation of low-speed circuits

Access providers should be asked to provide demarcation of low-speed circuits on IDC connecting hardware. While service providers may prefer a specific type of IDC connecting hardware (e.g. 66 block), they may be willing to hand off circuits on another type of IDC connecting hardware upon request.

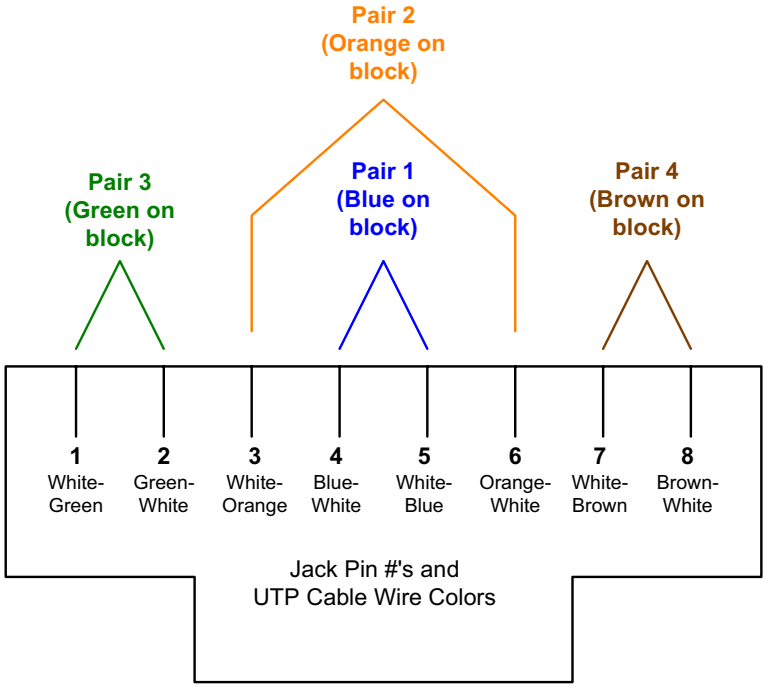
Cabling from the low-speed circuit demarcation area to the main distribution area should be terminated on IDC connecting hardware near the access provider IDC connecting hardware.

Circuits from access providers are terminated either in one or two pairs on the access provider IDC connecting hardware. Different circuits have different termination sequences, as illustrated in figure 16 and figure 17.

Each 4-pair cable should be terminated in an eight-position modular jack at the work area. The 100 ohm UTP and ScTP telecommunications outlet/connector should meet the modular interface requirements specified in IEC 60603-7. In addition, the telecommunications outlet/connector for 100 ohm UTP and ScTP cable should meet the requirements of ANSI/TIA/EIA-568-B.2 and the terminal marking and mounting requirements specified in ANSI/TIA-570-B.

Pin/pair assignments should be as shown in figure 16 or, optionally, per figure 17 if necessary to accommodate certain 8-pin cabling systems. The colors shown are associated with the horizontal

distribution cable. These illustrations depict the front view of the telecommunications outlet/connector and provide the list of the pair position for various circuit types.



(View from Front of Jack or Back of Plug)

1) **Phone Lines**:1-pair cross-connect to Pair 1**(Blue**)

2) **ISDN BRI U-Interface (U.S.)**: 1-pair cross-connect to Pair 1 (**Blue)**

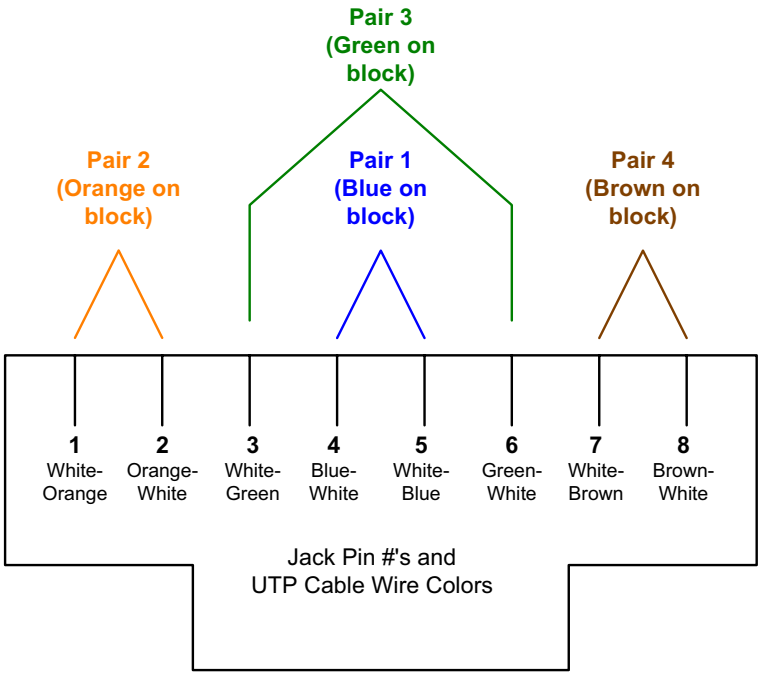
3) **ISDN BRI S/T-Intf (Intl)**: 2-pair cross-connect to Pairs 1 & 2 (**Blue** & **Orange**)

4) **56k/64k Leased Line**: 2-pair cross-connect to Pairs 3 & 4 (**Green** & **Brown**)

5) **E1/T1**: 2-pair cross-connect to Pairs 1 & 3 (**Blue** & **Green**)

6) **10Base-T/100Base-T**: 2-pair cross-connect to Pairs 2 & 3 (**Orange** & **Green**)

Figure 16: Cross-connection circuits to IDC connecting hardware cabled to modular jacks in the T568A 8-pin sequence



(View from Front of Jack or Back of Plug)

1) **Phone Lines**:1-pair cross-connect to Pair 1**(Blue**)

2) **ISDN BRI U-Interface (U.S.)**: 1-pair cross-connect to Pair 1 (**Blue)**

3) **ISDN BRI S/T-Intf (Intl)**: 2-pair cross-connect to Pairs 1 & 3 (**Blue** & **Green**)

4) **56k/64k Leased Line**: 2-pair cross-connect to Pairs 2 & 4 (**Orange** & **Brown**)

5) **E1/T1**: 2-pair cross-connect to Pairs 1 & 2 (**Blue** & **Orange**)

6) **10Base-T/100Base-T**: 2-pair cross-connect to Pairs 2 & 3 (**Orange** & **Green**)

Figure 17: Cross-connection circuits to IDC connecting hardware cabled to modular jacks in the T568B 8-pin sequence

The conversion from access provider 1-pair and 2-pair cabling to 4-pair cabling used by the data center structured cabling system can occur either in the low-speed circuit demarcation area or in the main distribution area.

The access provider and customer IDC connecting hardware can be mounted on a plywood backboard, frame, rack, or cabinet. Dual-sided frames should be used for mounting large numbers of IDC connecting hardware (3000+ pairs).

C.2.3 Demarcation of T-1 circuits

Access providers should be asked to hand-off T-1 circuits on RJ48X jacks (individual 8-position modular jacks with loop back), preferably on a DSX-1 patch panel mounted on a customer-owned rack installed in the DS-1 demarcation area. Patch panels from multiple access providers and the customer may occupy the same rack.

For example, in the United States and Canada, access providers typically use DSX-1 patch panels that fit 585 mm (23 in) racks. Thus, the DS-1 demarcation area should use one or more 585 mm (23 in) racks for access provider DS-1 patch panels. These same racks or adjacent 480 mm (19 in) racks can accommodate patch panels for cabling to the main distribution area. Outside the United States and Canada, access providers typically use DSX-1 panels that fit in 480 mm (19 in) racks.

The DSX-1 patch panels may require power for indicator lights. Thus, racks supporting access provider DSX-1 patch panels should, at minimum have one 20A 120V circuit and a multi-outlet power strip.

Allocate rack space for access provider and customer patch panels including growth. Access providers may require rack space for rectifiers to power DSX-1 patch panels.

Access providers can alternatively hand off DS-1 circuits on IDC connecting hardware. These IDC connecting hardware can be placed on the same frame, backboard, rack, or cabinet as the IDC connecting hardware for low-speed circuits.

A single 4-pair cable can accommodate one T1 transmit and receive pair. When multiple T1 signals are placed over multi-pair unshielded twisted-pair cable, the transmitted signals should be placed in one cable and the receive signals placed in a separate cable.

If the data center support staff has the test equipment and knowledge to troubleshoot T-1 circuits, the DS-1 demarcation area can use DSX-1 panels to terminate T-1 cabling to the main distribution area. These DSX-1 panels should have either modular jacks or IDC terminations at the rear.

The IDC connecting hardware, modular jack patch panels, or DSX-1 panels for cabling to the main distribution area can be on the same or separate racks, frames, or cabinets as the ones used for access provider DSX-1 patch panels. If they are separate, they should be adjacent to the racks assigned to the access providers.

The customer (data center owner) may decide to provide its own multiplexers (M13 or similar multiplexer) to demultiplex access provider T-3 circuits to individual T-1 circuits. T-1 circuits from a customer-provided multiplexer should not be terminated in the T-1 demarcation area.

C.2.4 Demarcation of E-3 & T-3 circuits

Access providers should be asked to hand-off E-3 or T-3 circuits on pairs of female BNC connectors, preferably on a DSX-3 patch panel on a customer-owned rack installed in the E-3/T-3

demarcation area. Patch panels from multiple access providers and the customer may occupy the same rack.

In the United States and Canada, access providers typically use DSX-3 patch panels that fit 585 mm (23 in) racks. Thus, the E-3/T-3 demarcation area should use one or more 585 mm (23 in) racks for access provider DSX-3 patch panels. These same racks or adjacent 480 mm (19 in) racks can accommodate patch panels for cabling to the main distribution area. Outside North America, access providers typically use DSX-3 panels that fit 480 mm (19 in) racks.

If the data center support staff has the test equipment and knowledge to troubleshoot E-3 or T-3 circuits, the E-3/T-3 demarcation area can use DSX-3 panels to terminate 734-type coaxial cabling to the main distribution area. These DSX-3 panels should have BNC connectors at the rear.

The DSX-3 patch panels may require power for indicator lights. Thus, racks supporting access provider DSX-3 patch panels should, at minimum have one 20A 120V circuit and a multi-outlet power strip.

Allocate rack space for access provider and customer patch panels including growth. Access providers may require rack space for rectifiers to power DSX-3 patch panels.

Cabling from the E-3/T-3 demarcation area to the main distribution area should be 734-type coaxial cable. Cables in the E-3/T-3 demarcation area can be terminated on a customer patch panel with 75-ohm BNC connectors, or directly on an access provider DSX-3 patch panel. Access provider DSX-3 patch panels typically have the BNC connectors on the rear of the panels. Thus, BNC patch panels for cabling to the main distribution area should be oriented with the front of the patch panels on the same side of the rack as the rear of the access provider DSX-3 panels.

All connectors and patch panels for E-3 and T-3 cabling should use 75-ohm BNC connectors.

C.2.5 Demarcation of optical fiber circuits

Access providers should be asked to hand-off optical fiber circuits on fiber patch panels installed on racks in the fiber demarcation area. Fiber patch panels from multiple access providers and the customer may occupy the same rack. If requested, access providers may be able to use the same connector to simplify patch cable requirements.

In the United States and Canada, access providers typically use fiber patch panels that fit 585 mm (23 in) racks, but may be able to provide patch panels that fit 480 mm (19 in) racks, if requested. In the United States, it is usually prudent to use 585 mm (23 in) racks for access provider fiber patch panels in the fiber demarcation area. These same racks or adjacent 480 mm (19 in) racks can accommodate patch panels for cabling to the main distribution area. Outside North America, access providers typically use fiber patch panels that fit 480 mm (19 in) racks.

The racks in the fiber demarcation area do not require power except possibly utility outlets for access provider and customer test equipment.

Cabling from the fiber demarcation area to the main cross-connect in the main distribution area should be single-mode optical fiber cable. If the access providers provide services terminated in multimode optical fiber cable, the cabling from the fiber demarcation area to the main cross-connect (MC) in the main distribution area can also include multimode optical fiber cable.

ANNEX D (INFORMATIVE) COORDINATION OF EQUIPMENT PLANS WITH OTHER ENGINEERS

This annex is informative only and is not part of this Standard.

D.1 General

Coordinate placement of equipment and lighting in the data centers so that lighting fixtures are placed in aisles between cabinets and racks instead of directly over equipment rows.

Coordinate placement of equipment and sprinklers in the data centers so that tall cabinets or overhead cable trays do not block water dispersal from the sprinklers – the minimum clearance by Code is 460 mm (18 in). Electrical engineers will need to know placement and power requirements for equipment cabinets and racks. Coordinate routing of power cabling and receptacles with routing of telecommunications cabling and placement of equipment.

Mechanical engineers will need to know cooling requirements for equipment cabinets and racks. Coordinate placement of cable trays and telecommunications cabling to ensure that adequate airflow is maintained to all parts of the computer room. Airflow from cooling equipment should be parallel to rows of cabinets and racks. Perforated tiles should be placed in “cold” aisles, not “hot” aisles.

Plan telecommunications cabling routes to maintain a minimum separation of unshielded twisted pair cabling from fluorescent lights by 125 mm (5 in).

ANNEX E (INFORMATIVE) DATA CENTER SPACE CONSIDERATIONS

This annex is informative only and is not part of this Standard.

E.1 General

The data center should have an adequately sized storage room so that boxed equipment, spare air filters, spare floor tiles, spare cables, spare equipment, spare media, and spare paper can be stored outside the computer room. The data center should also have a staging area for unpacking and possibly for testing new equipment before deploying them in the computer room. It is possible to dramatically reduce the amount of airborne dust particles in the data center by having a policy of un-packaging all equipment in the build/storage room.

The required square footage of space is intimately related to the layout of the space, including not only equipment racks and/or cabinets, but also cable management and other supporting systems such as electrical power, HVAC and fire suppression. These supporting systems have space requirements that depend upon the required level of redundancy.

If the new data center replaces one or more existing data centers, one way to estimate the size of the data center is to inventory the equipment to be moved into the new data center and create a floor plan of the new data center with this equipment and expected future equipment with desired equipment adjacencies and desired clearances. The layout should assume that the cabinets and racks are efficiently filled with equipment. The floor plan should also take into account any planned technology changes that might affect the size of the equipment to be located in the new data center. The new computer room floor plan will need to include electrical and HVAC support equipment.

Often an operations center and a printer room are spaces with data center adjacency requirements, and are best designed together with the data center. The printer room should be separated from the main computer room and have a separate HVAC system because the printers generate paper and toner dust, which are detrimental to computer equipment. NFPA 75 specifies separate rooms for storage of spare media and forms. Additionally, it is a good practice to have a separate tape room for tape drives, automated tape libraries, and tape libraries because of the toxicity of smoke from burning tape.

Consider separate spaces or rooms outside the computer room for electrical, HVAC, and fire suppression system equipment, although space is not used as efficiently, security is improved because vendors and staff that service this equipment don’t need to enter the computer room. Also, separate spaces for support equipment may not be possible in large data centers that are wider than the throw distance of computer room air conditioners (CRAC), which is about 12 m (40 ft).

ANNEX F (INFORMATIVE) SITE SELECTION

This annex is informative only and is not part of this Standard.

F.1 General

Some of the considerations in this annex apply to higher tier data centers, considerations that are particularly important to a specific tier level are provided in the tiering chart in annex G.

The building should conform to all applicable national, state, and local codes.

The building and site should meet all current applicable local, state, and federal accessibility guidelines and standards.

The building should conform to the seismic standards applicable to the International Building Code Seismic Zone of the site.

The building should be free of asbestos, lead-containing paint, PCB's, and other environmental hazards.

Consideration should be given to zoning ordinances and environmental laws governing land use, fuel storage, sound generation, and hydrocarbon emissions that may restrict fuel storage and generator operation.

The difficulty in properly cooling equipment increases with altitude, thus data centers should be located below 3050 m (10,000 ft) elevation as recommended by ASHRAE.

F.2 Architectural site selection considerations

The need for redundant access to the building from separate roads should be considered.

Where practical, the building should be a single story dedicated data center building.

Buildings with large clear spans between columns that maximize usable space for equipment are preferred.

The building materials should be non-combustible. Exterior walls should be constructed of concrete or masonry to provide security, particularly in areas where brush fires may cause service outages or threaten the structure.

For one or two story buildings, the building construction should be International Building Code Type V-N, fully sprinklered with 18 m (60 ft) of clear side yards on all sides. For buildings with three or more stories, the building construction should be International Building Code Type I or II.

Where the building is not dedicated to the data center, other tenant spaces should be non-industrial, International Building Code type 'B' offices, and non-intrusive to the data center. Avoid buildings with restaurants and cafeterias to minimize fire risk.

If the data center is to be on an upper floor of a multi-tenant building, then there should be adequate shaft and conduit space for generator, security, telecommunications, and electrical conduits as well as supplemental HVAC, grounding conductors and cabling to antennas, as needed.

The building should meet the structural requirements of the installation. Consider floor loading for UPS batteries and transformers as well as vibration isolation from rotary equipment on the adjacent floors.

The height from the floor to the underside of the building should be considered. Heights of 4 m (13 ft) or more may be required to accommodate access flooring, equipment, and cabling.

The building should be provided with sufficient parking to meet all applicable codes. Consideration should be given to “exit strategies” which may require additional parking.

Sufficient space should be provided for all mechanical and electrical support equipment, including indoor, outdoor, and rooftop equipment. Consideration should be given to future equipment requirements.

The building should have a sufficiently large loading dock, freight elevator, and pathway to handle all anticipated deliveries of supplies and equipment.

The computer room should be located away from sources of EMI and RFI such as x-ray equipment, radio transmitters, and transformers. Sources of EMI & RFI should be at a distance that will reduce the interference to 3.0 volts/meter throughout the frequency spectrum.

The data center and all support equipment should be located above the highest expected floodwater levels. No critical electronic, mechanical or electrical equipment should be located in basement levels.

Avoid locating computer room below plumbed areas such as rest rooms, janitor closets, kitchens, laboratories, and mechanical rooms.

The computer room should have no exterior windows. If there are windows in a proposed computer room space, they should be covered for security reasons and to minimize any solar heat gain.

F.3 Electrical site selection considerations

The local utility company should be able to provide adequate power to supply all initial and future power requirements for the data center. The availability and economics of redundant utility feeders possibly from separate utility substations should be considered where applicable. If the local utility cannot provide adequate power, the site should be able to support self-generation, co-generation or distributed generation equipment. Underground utility feeders are preferable to overhead feeders to minimize exposure to lightning, trees, traffic accidents, and vandalism.

F.4 Mechanical site selection considerations

A multi-tenant building will require a location designated by the landlord either on the roof or on grade for air conditioning heat rejection equipment (condensing units, cooling towers, or dry fluid coolers).

If the building has an existing fire suppression system it should be easily modified to a pre-action sprinkler system dedicated to the data center. If the building has an existing air conditioning system serving the data center space it should be a system and type applicable for data centers based on a minimum 10 sq m (100 sq ft) per ton, including both the computer room space and support areas.

F.5 Telecommunications site selection considerations

The building should be served by at least two diversely routed optical fiber entrance rooms. These entrance rooms should be fed from different local access provider offices. If the building is only served by a single local central office, then the service feed from the second local central office should be capable of being added without major construction or delays in obtaining permits.

Multiple telecommunications access providers should provide service or be able to provide service to the building without major construction or delays in obtaining permits.

The data center should be served by dedicated access provider equipment located in the data center space and not in shared tenant space. The access provider entrance cables should be enclosed in conduit within the building and be inaccessible to other tenants where routed through shared pathways. The building should have dedicated conduits serving the data center space for telecommunications service.

F.6 Security site selection considerations

If cooling equipment, generators, fuel tanks, or access provider equipment is situated outside the customer space, then this equipment should be adequately secured.

Also, the data center owner will need access to this space 24 hrs/day, 7 days/week.

Common areas should be monitored by cameras, including parking lots, loading docks, and building entrances.

The computer room should not be located directly in close proximity to a parking garage.

The building should not be located in a 100-year flood plain, near an earthquake fault, on a hill subject to slide risk, or down stream from a dam or water tower. Additionally there should be no nearby buildings that could create falling debris during an earthquake.

The building should not be in the flight path of any nearby airports.

The building should be no closer than 0.8 km (½ mile) from a railroad or major interstate highway to minimize risk of chemical spills.

The building should not be within 0.4 km (¼ mile) of an airport, research lab, chemical plant, landfill, river, coastline, or dam.

The building should not be within 0.8 km (½ mile) of a military base.

The building should not be within 1.6 km (1 mile) of a nuclear, munitions, or defense plant.

The building should not be located adjacent to a foreign embassy.

The building should not be located in high crime areas.

F.7 Other site selection considerations

Other data center site selection criteria to consider are:

- risk of contamination;

- proximity of police stations, fire stations, and hospitals;

- general access;
- zoning ordinances;
- vibration;
- environmental issues;
- alternate uses of the building after it is no longer needed as a data center (exit strategies).

ANNEX G (INFORMATIVE) DATA CENTER INFRASTRUCTURE TIERS

This annex is informative only and is not part of this Standard.

G.1 General

G.1.1 Redundancy overview

Single points of failure should be eliminated to improve redundancy and reliability, both within the data center and support infrastructure as well as in the external services and utility supplies. Redundancy increases both fault tolerance and maintainability. Redundancy should be separately addressed at each level of each system, and is typically described using the nomenclature in clause 8.

This Standard includes four tiers relating to various level of availability of the data center facility infrastructure. The tier ratings correspond to the industry data center tier ratings as defined by The Uptime Institute, but the definitions of each tier have been expanded in this Standard.

G.1.2 Tiering overview

This Standard includes four tiers relating to various levels of availability of the data center facility infrastructure. Higher tiers not only correspond to higher availability, but also lead to higher construction costs. In all cases, higher rated tiers are inclusive of lower level tier requirements unless otherwise specified.

A data center may have different tier ratings for different portions of its infrastructure. For example, a data center may be rated tier 3 for electrical, but tier 2 for mechanical. However, the data center's overall tier rating is equal to the lowest rating across all portions of its infrastructure. Thus, a data center that is rated tier 4 for all portions of its infrastructure except electrical, where it is rated tier 2, is rated tier 2 overall. The overall rating for the data center is based on its weakest component.

Care should be taken to maintain mechanical and electrical system capacity to the correct tier level as the data center load increases over time. A data center may be degraded from tier 3 or tier 4 to tier 1 or tier 2 as redundant capacity is utilized to support new computer and telecommunications equipment.

A data center should meet the requirements specified in this Standard to be rated at any tier level. While the concept of tiers is useful for stratifying the levels of redundancy within various data center systems, it is quite possible that circumstances might call for some systems to be of higher tiers than others. For example, a data center located where utility electric power is less reliable than average might be designed with a tier 3 electrical system but only tier 2 mechanical systems. The mechanical systems might be enhanced with spare parts to help ensure a low MTTR (mean time to repair).

It should also be noted that human factors and operating procedures can also be very important. Hence the actual reliability of two tier 3 data centers might be quite different.

G.2 Redundancy

G.2.1 N - Base requirement

System meets base requirements and has no redundancy.

G.2.2 N+1 redundancy

N+1 redundancy provides one additional unit, module, path, or system in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any single unit, module, or path will not disrupt operations.

G.2.3 N+2 redundancy

N+2 redundancy provides two additional units, modules, paths, or systems in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any two single units, modules, or paths will not disrupt operations.

G.2.4 2N redundancy

2N redundancy provides two complete units, modules, paths, or systems for every one required for a base system. ”Failure or maintenance of one entire unit, module, path, or system will not disrupt operations.

G.2.5 2(N+1) redundancy

2 (N+1) redundancy provides two complete (N+1) units, modules, paths, or systems. Even in the event of failure or maintenance of one unit, module, path, or system, some redundancy will be provided and operations will not be disrupted.

G.2.6 Concurrent maintainability and testing capability

The facilities should be capable of being maintained, upgraded, and tested without interruption of operations.

G.2.7 Capacity and scalability

Data centers and support infrastructure should be designed to accommodate future growth with little or no disruption to services.

G.2.8 Isolation

Data centers should (where practical) be used solely for the purposes for which they were intended and should be isolated from non-essential operations.

G.2.9 Data center tiering

G.2.9.1 General

The four data center tiers as originally defined by The Uptime Institute in its white paper ‘Industry Standard Tier Classifications Define Site Infrastructure Performance’ are:

Tier I Data Center: Basic

A Tier I data center is susceptible to disruptions from both planned and unplanned activity. It has computer power distribution and cooling, but it may or may not have a raised floor, a UPS, or an engine generator. If it does have UPS or generators, they are single-module systems and have many single points of failure. The infrastructure should be completely shut down on an annual basis to perform preventive maintenance and repair work. Urgent situations may require more frequent shutdowns. Operation errors or spontaneous failures of site infrastructure components will cause a data center disruption.

Tier II Data Center: Redundant Components

Tier II facilities with redundant components are slightly less susceptible to disruptions from both planned and unplanned activity than a basic data center. They have a raised floor, UPS, and engine generators, but their capacity design is “Need plus One” (N+1), which has a single-threaded distribution path throughout. Maintenance of the critical power path and other parts of the site infrastructure will require a processing shutdown.

Tier III Data Center: Concurrently Maintainable

Tier III level capability allows for any planned site infrastructure activity without disrupting the computer hardware operation in any way. Planned activities include preventive and programmable maintenance, repair and replacement of components, addition or removal of capacity components, testing of components and systems, and more. For large sites using chilled water, this means two independent sets of pipes. Sufficient capacity and distribution must be available to simultaneously carry the load on one path while performing maintenance or testing on the other path. Unplanned activities such as errors in operation or spontaneous failures of facility infrastructure components will still cause a data center disruption. Tier III sites are often designed to be upgraded to Tier IV when the client’s business case justifies the cost of additional protection.

Tier IV Data Center: Fault Tolerant

Tier IV provides site infrastructure capacity and capability to permit any planned activity without disruption to the critical load. Fault-tolerant functionality also provides the ability of the site infrastructure to sustain at least one worst-case unplanned failure or event with no critical load impact. This requires simultaneously active distribution paths, typically in a System+System configuration. Electrically, this means two separate UPS systems in which each system has N+1 redundancy. Because of fire and electrical safety codes, there will still be downtime exposure due to fire alarms or people initiating an Emergency Power Off (EPO). Tier IV requires all computer hardware to have dual power inputs as defined by the Institute’s Fault-Tolerant Power Compliance Specification.

Tier IV site infrastructures are the most compatible with high availability IT concepts that employ CPU clustering, RAID DASD, and redundant communications to achieve reliability, availability, and serviceability.

G.2.9.2 Tier 1 data center – basic

A tier 1 data center is a basic data center with no redundancy. It has a single path for power and cooling distribution with no redundant components.

A tier 1 data center is susceptible to disruptions from both planned and unplanned activity. It has computer power distribution and cooling, UPS and generators are single module systems and have many single points of failure. Critical loads may be exposed to outages during preventive

maintenance and repair work. Operation errors or spontaneous failures of site infrastructure components will cause a data center disruption.

G.2.9.3 Tier 2 data center – redundant components

A tier 2 data center has redundant components, but only a single path. It has a single path for power and cooling distribution, but it has redundant components on this distribution path.

Tier 2 facilities with redundant components are slightly less susceptible to disruptions from both planned and unplanned activity than a basic tier 1 data center. The UPS and engine generators design capacity is “Need plus One” (N+1), which has a single threaded distribution path throughout. Maintenance of the critical power path and other parts of the infrastructure will require a processing shutdown.

G.2.9.4 Tier 3 data center - concurrently maintainable

A tier 3 data center has multiple power and cooling distribution paths, but only one path active. Because redundant components are not on a single distribution path, the system is concurrently maintainable.

Tier 3 level capability allows for any planned data center infrastructure activity without disrupting the computer hardware operation in any way. Planned activities include preventive and programmable maintenance, repair and replacement of components, addition or removal of capacity components, testing of components and systems, and more. For data centers using chilled water, this means two independent sets of pipes. Sufficient capacity and distribution should be available to simultaneously carry the load on one path while performing maintenance or testing on the other path. Unplanned activities such as errors in operation or spontaneous failures of facility infrastructure components will still cause a data center disruption. Tier 3 data centers are often designed to be upgraded to tier 4 when the business case justifies the cost of additional protection.

The site should be manned 24 hours per day.

G.2.9.5 Tier 4 data center - fault tolerant

A tier 4 data center has multiple active power and cooling distribution paths. Because at least two paths are normally active in a tier 4 data center, the infrastructure provides a higher degree of fault tolerance.

Tier 4 data centers provide multiple power feeds to all computer and telecommunications equipment. Tier 4 requires all computer and telecommunications equipment to have multiple power inputs. The equipment should be able to continue functioning with one of these power inputs shut down. Equipment that is not built with multiple power inputs will require automatic transfer switches.

Tier 4 provides data center infrastructure capacity and capability to permit any planned activity without disruption to the critical load. Fault-tolerant functionality also provides the ability of the data center infrastructure to sustain at least one worst-case unplanned failure or event with no critical load impact. This requires simultaneously active distribution paths, typically in a System + System configuration. Electrically, this means two separate UPS systems in which each system has N+1 redundancy. Because of fire and electrical safety codes, there will still be downtime exposure due to fire alarms or people initiating an Emergency Power Off (EPO). Tier 4 data center infrastructures are the most compatible with high availability information technology concepts that employ CPU clustering, Redundant Array of Independent Disk/Direct Access

Storage Device (RAID/DASD), and redundant communications to achieve reliability, availability, and serviceability.

G.3 Telecommunications systems requirements

G.3.1 Telecommunications tiering

G.3.1.1 Tier 1 (telecommunications)

The telecommunications infrastructure should meet the requirements of this Standard to be rated at least tier 1.

A tier 1 facility will have one customer owned maintenance hole and entrance pathway to the facility. The access provider services will be terminated within one entrance room. The communications infrastructure will be distributed from the entrance room to the main distribution and horizontal distribution areas throughout the data center via a single pathway. Although logical redundancy may be built into the network topology, there would be no physical redundancy or diversification provided within a tier 1 facility.

Label all patch panels, outlets, and cables as described in ANSI/TIA/EIA-606-A and annex B of this Standard. Label all cabinets and racks with their identifier at the front and rear.

Some potential single points of failure of a tier 1 facility are:

- access provider outage, central office outage, or disruption along a access provider right-of-way;

- access provider equipment failure;

- router or switch failure, if they are not redundant;

- any catastrophic event within the entrance room, main distribution area, or maintenance hole may disrupt all telecommunications services to the data center;

- damage to backbone or horizontal cabling.

G.3.1.2 Tier 2 (telecommunications)

The telecommunications infrastructure should meet the requirements of tier 1.

Critical telecommunications equipment, access provider provisioning equipment, production routers, production LAN switches, and production SAN switches, should have redundant components (power supplies, processors).

Intra-data center LAN and SAN backbone cabling from switches in the horizontal distribution areas to backbone switches in the main distribution area should have redundant fiber or wire pairs within the overall star configuration. The redundant connections may be in the same or different cable sheathes.

Logical configurations are possible and may be in a ring or mesh topology superimposed onto the physical star configuration.

A tier 2 facility addresses vulnerability of telecommunications services entering the building.

A tier 2 facility should have two customer owned maintenance holes and entrance pathways to the facility. The two redundant entrance pathways will be terminated within one entrance room. The physical separation of the pathways from the redundant maintenance holes to the entrance room is recommended to be a minimum of 20 m (66 ft) along the entire pathway route. The entrance pathways are recommended to enter at opposite ends of the entrance room. It is not recommended that the redundant entrance pathways enter the facility in the same area as this will not provide the recommended separation along the entire route.

All patch cords and jumpers should be labeled at both ends of the cable with the name of the connection at both ends of the cable for a data center to be rated tier 2.

Some potential single points of failure of a tier 2 facility are:

- access provider equipment located in the entrance room connected to same electrical distribution and supported by single HVAC components or systems;

- redundant routing and core switching hardware located in the main distribution area connected to same electrical distribution and supported by single HVAC components or systems;

- redundant distribution switching hardware located in the horizontal distribution area connected to same electrical distribution and supported by single HVAC components or systems;

- any catastrophic event within the entrance room or main distribution area may disrupt all telecommunications services to the data center.

G.3.1.3 Tier 3 (telecommunications)

The telecommunications infrastructure should meet the requirements of tier 2.

The data center should be served by at least two access providers. Service should be provided from at least two different access provider central offices or points-of-presences. Access provider cabling from their central offices or points-of-presences should be separated by at least 20 m (66 ft) along their entire route for the routes to be considered diversely routed.

The data center should have two entrance rooms preferably at opposite ends of the data center but a minimum of 20 m (66 ft) physical separation between the two rooms. Do not share access provider provisioning equipment, fire protection zones, power distribution units, and air conditioning equipment between the two entrance rooms. The access provider provisioning equipment in each entrance room should be able to continue operating if the equipment in the other entrance room fails.

The data center should have redundant backbone pathways between the entrance rooms, main distribution area, and horizontal distribution areas.

Intra-data center LAN and SAN backbone cabling from switches in the horizontal distribution areas to backbone switches in the main distribution area should have redundant fiber or wire pairs within the overall star configuration. The redundant connections should be in diversely routed cable sheathes.

There should be a “hot” standby backup for all critical telecommunications equipment, access provider provisioning equipment, core layer production routers and core layer production LAN/SAN switches.

All cabling, cross-connects and patch cords should be documented using spreadsheets, databases, or programs designed to perform cable administration. Cabling system documentation is a requirement for a data center to be rated tier 3.

Some potential single points of failure of a tier 3 facility are:

- any catastrophic event within the main distribution area may disrupt all telecommunications services to the data center;

- any catastrophic event within a horizontal distribution area may disrupt all services to the area it servers.

G.3.1.4 Tier 4 (telecommunications)

The telecommunications infrastructure should meet the requirements of tier 3.

Data center backbone cabling should be redundant. Cabling between two spaces should follow physically separate routes, with common paths only inside the two end spaces. Backbone cabling should be protected by routing through conduit or by use of cables with interlocking armor.

There should be automatic backup for all critical telecommunications equipment, access provider provisioning equipment, core layer production routers and core layer production LAN/SAN switches. Sessions/connections should switch automatically to the backup equipment.

The data center should have a main distribution area and secondary distribution area preferably at opposite ends of the data center but a minimum of 20 m (66 ft) physical separation between the two spaces. Do not share fire protection zones, power distribution units, and air conditioning equipment between the main distribution area and secondary distribution area. The secondary distribution area is optional, if the computer room is a single continuous space, there is probably little to be gained by implementing a secondary distribution area.

The main distribution area and the secondary distribution area will each have a pathway to each entrance room. There should also be pathway between the main distribution area and secondary distribution area.

The redundant distribution routers and switches should be distributed between the main distribution area and secondary distribution area in such a manner that the data center networks can continue operation if the main distribution area, secondary distribution area, or one of the entrance rooms has a total failure.

Each of the horizontal distribution areas should be provided with connectivity to both the main distribution area and secondary distribution area.

Critical systems should have horizontal cabling to two horizontal distribution areas. Redundant horizontal cabling is optional even for tier 4 facilities.

Some potential single points of failure of a tier 4 facility are:

- the main distribution area (if the secondary distribution area is not implemented);

- at the horizontal distribution area and horizontal cabling (if redundant horizontal cabling is not installed).

G.4 Architectural and structural requirements

G.4.1 General

The building structural system should be either steel or concrete. At a minimum, the building frame should be designed to withstand wind loads in accordance with the applicable building codes for the location under consideration and in accordance with provisions for structures designated as essential facilities (for example, Building Classification III from the International Building Code).

Slabs on grade should be a minimum of 127 mm (5 in) and have a bearing capacity of 12 kPa (250 lbf/ft^2). Elevated slabs should be of hard rock concrete and have a 100 mm (4 in) minimum cover over the tops of metal deck flutes in seismic zones 3 and 4 to allow for adequate embedment of epoxy or KB-II anchors. Floors within UPS areas should be designed for a minimum loading of 12 to 24 kPa (250 to 500 lbf/ ft^2) deck and joists, 19.2 kPa (400 lbf/ ft^2) girders, columns and footings. Local building codes may dictate final requirements, which may necessitate structural modifications to increase the load carrying capacity of the floor system. Battery racks will typically require supplemental supports in order to properly distribute the applied loads.

Roofs should be designed for actual mechanical equipment weights plus an additional 1.2 kPa (25 lbf/ ft^2) for suspended loads. Roof areas over UPS rooms should be designed to accommodate a suspended load of 1.4 kPa (30 lbf/ ft^2).

All mechanical equipment should be positively anchored to the supporting element. Equipment is often vibration sensitive, and precautions should be taken to ensure that sources of vibration are carefully controlled. Vibrating equipment should be mounted on vibration isolators to the extent possible. Also, the vibration characteristics of the floor structure should be carefully reviewed.

All yard equipment should be anchored in a manner consistent with the Code. All pipe racks should be designed and detailed to limit the lateral drift to 1/2 that allowed by Code, but should not exceed 25 mm (1 in) elastic or 64 mm (2.5 in) inelastic deformation. All equipment screens should meet Code-mandated allowable deformation. However, should any equipment or piping be attached to the equipment screen, supports should be designed and deflections limited.

All interior partitions should have a minimum one hour fire rating (two hours is preferred) and extend from the floor to the underside of the structure above.

Truck loading docks should be provided as required to handle anticipated deliveries, and should be provided with a level of security similar to the other building entrances. Consideration should be given to areas for equipment staging, secured storage for valuable equipment, and for equipment burn-in and testing. Access floor spaces may require higher load ratings or additional understructure support in areas of heavy delivery traffic.

Sufficient storage space should be provided for all anticipated items such as paper, tapes, cabling, and hardware. Large paper rolls for roll-fed printers require larger clearances, storage spaces, and floor loading than boxed paper.

All penetrations at computer room perimeter walls, floors and ceilings will require sealing.

A clean-room ceiling system should be considered in all computer room areas, particularly where flaking and dust from fireproofing materials might contaminate equipment. Suspended ceilings can also reduce the volume of gas required for gaseous fire suppression systems.

Special design considerations should be given to mounting satellite dishes and wireless communications towers.

A command center, operations center, or network operations center (NOC) is often required in larger data centers. The command center is sometimes large, housing 20 or more workstations, and is often located in a secure and separate room. It often requires a door for direct access to the computer room space to meet operational needs. Where command center operations are critical, consideration should be given to backing-up the command center with a redundant remote command center.

G.4.2 Architectural tiering

G.4.2.1 Tier 1 (architectural)

Architecturally, a tier 1 data center is a data center with no requirements for protection against physical events, either intentional or accidental, natural or man made, which could cause the data center to fail.

Minimum floor loading for equipment areas should be 7.2 kPa (150 lbf/ft^2) live load with 1.2 kPa (25 lbf/ ft^2) for loads hanging from the bottom of the floor. Refer to Telcordia specification GR-63-CORE regarding floor loading capacity measurement and test methods.

G.4.2.2 Tier 2 (architectural)

Tier 2 installations should meet all requirements of tier 1. In addition, tier 2 installations should meet the additional requirements specified in this annex. A tier 2 data center includes additional minimal protections against physical events, either intentional or accidental, natural or man made, which could cause the data center to fail.

Vapor barriers should be provided for the walls and ceiling of the computer room to ensure the mechanical equipment can maintain humidification limits.

All security doors should be solid wood with metal frames. Doors to security equipment and monitoring rooms should also be provided with 180-degree peepholes.

All security walls should be full height (floor to ceiling). Additionally, walls to the security equipment and monitoring rooms should be hardened by installing not less than 16 mm (5/8 in) plywood to the interior of the room with adhesive and screws every 300 mm (12 in).

Minimum floor loading for equipment areas should be 8.4 kPa (175 lbf/ ft^2) live load with 1.2 kPa (25 lbf/ ft^2) for loads hanging from the bottom of the floor. Refer to Telcordia specification GR-63-CORE regarding floor loading capacity measurement and test methods.

G.4.2.3 Tier 3 (architectural)

Tier 3 installations should meet all requirements of tier 2. In addition, tier 2 installations should meet the additional requirements specified in this annex. A tier 3 data center has set in place specific protections against most physical events, either intentional or accidental, natural or man made, which could cause the data center to fail.

Redundant entrances and security checkpoints should be provided.

Redundant access roads with security checkpoints should be provided to ensure access in the event of road flooding or other problems and/or to enable separation of access of employees and vendors.

There should be no windows on the exterior perimeter walls of the computer room.

The construction of the buildings should provide protection against electromagnetic radiation. Steel construction can provide this shielding. Alternately, a special-purpose Faraday cage can be embedded in the walls, consisting of aluminum foil, foil-backed gypsum board, or chicken wire.

Mantraps at all entrances to the computer room should provide measures that reduce the potential for piggybacking or for intentionally letting more than one person in by the use of only one credential. Single person security interlocks, turnstiles, portals or other hardware designed to prevent piggybacking or pass-back of credentials should be employed to control access from the main entrance to the computer room.

Physical separation or other protection should be provided to segregate redundant equipment and services to eliminate the likelihood of concurrent outages.

A security fence should be considered, with controlled, secured access points. The perimeter of the site should be protected by a microwave intruder detection system and monitored by visible or infrared Closed Circuit Television (CCTV) systems.

Access to the site should be secured by identification and authentication systems. Additional access control should be provided for crucial areas such as the computer room, entrance rooms, and electrical and mechanical areas. Data centers should be provided with a dedicated security room to provide central monitoring for all security systems associated with the data center.

Minimum floor loading for equipment areas should be 12 kPa (250 lbf/ ft^2) live load with 2.4 kPa (50 lbf/ ft^2) loads hanging from the bottom of the floor. Refer to Telcordia specification GR-63-CORE regarding floor loading capacity measurement and test methods.

G.4.2.4 Tier 4 (architectural)

Tier 4 installations should meet all requirements of tier 3. In addition, tier 3 installations should meet the additional requirements specified in this annex.

A tier 4 data center has considered all potential physical events, either intentional or accidental, natural or man made, which could cause the data center to fail. A tier 4 data center has provided specific and in some cases redundant protections against such events. Tier 4 data centers consider the potential problems with natural disasters such as seismic events, floods, fire, hurricanes, and storms, as well as potential problems with terrorism and disgruntled employees. Tier 4 data centers have control over all aspects of their facility.

There should be an area located in a separate building or outdoor enclosure for a secured generator pad.

There should also be a designated area outside the building as close as possible to the generator for fuel storage tanks.

Facilities located within seismic zones 0, 1, & 2 should be designed in accordance with seismic zone 3 requirements. Facilities located within seismic zones 3 & 4 should be designed in accordance with seismic zone 4 requirements. All facilities should be designed with an Importance Factor I = 1.5. Equipment and data racks in seismic zones 3 & 4 should be base attached and top braced to resist seismic loads.

Minimum floor loading for equipment areas should be 12 kPa (250 lbf/ ft^2) live load with 2.4 kPa (50 lbf/ ft^2) loads hanging from the bottom of the floor. Refer to Telcordia specification GR-63-CORE regarding floor loading capacity measurement and test methods.

G.5 Electrical systems requirements

G.5.1 General electrical requirements

G.5.1.1 Utility service entrance and primary distribution

Consideration should be given to other utility customers served by the same utility feeder. Hospitals are preferred as they typically receive high priority during outages. Industrial users sharing incoming electrical supplies are not preferred due to the transients and harmonics they often impose on the feeders.

Underground utility feeders are preferable to overhead feeders to minimize exposure to lightning, trees, traffic accidents, and vandalism.

The primary switchgear should be designed for growth, maintenance, and redundancy. A double-ended (main-tie-main) or isolated redundant configuration should be provided. The switchgear bus should be oversized as this system is the least expandable once operations begin. Breakers should be interchangeable where possible between spaces and switchgear lineups. Design should allow for maintenance of switchgear, bus, and/or breakers. The system should allow flexibility of switching to satisfy total maintainability. Transient Voltage Surge Suppression (TVSS) should be installed at each level of the distribution system, and be properly sized to suppress transient energy that is likely to occur.

G.5.1.2 Standby generation

The standby generation system is the most crucial single resilience factor and should be capable of providing a supply of reasonable quality and resilience directly to the computer and telecommunications equipment if there is a utility failure.

Generators should be designed to supply the harmonic current imposed by the UPS system or computer equipment loads. Motor starting requirements should be analyzed to ensure the generator system is capable of supplying required motor starting currents with a maximum voltage drop of 15% at the motor. Interactions between the UPS and generator may cause problems unless the generator is specified properly; exact requirements should be coordinated between the generator and UPS vendors. A variety of solutions are available to address these requirements, including harmonic filters, line reactors, specially wound generators, time-delayed motor starting, staged transfer, and generator de-rating.

Where a generator system is provided, standby power should be provided to all air-conditioning equipment to avoid thermal overload and shutdown. Generators provide little or no benefit to the overall continuity of operations if they do not support the mechanical systems.

Paralleled generators should be capable of manual synchronization in the event of failure of automatic synchronization controls. Consideration should be given to manual bypass of each generator to directly feed individual loads in the event of failure or maintenance of the paralleling switchgear.

Transient voltage surge suppression (TVSS) should be provided for each generator output.

Generator fuel should be diesel for faster starting rather than natural gas. It will avoid dependence on the gas utility and on-site storage of propane. Consideration should be given to the quantity of on-site diesel storage required, which can range from 4 hours to 60 days. A remote fuel monitoring and alarming system should be provided for all fuel storage systems. As microbial growth is the most common failure mode of diesel fuel, consideration should be given to portable or permanently installed fuel clarification systems. In “cold” climates, consideration

should be given to heating or circulating the fuel system to avoid gelling of the diesel fuel. The response time of fuel vendors during emergency situations should be considered when sizing the on-site fuel-storage system.

Noise and other environmental regulations should be observed.

Lighting powered from the UPS, an emergency lighting inverter, or individual batteries should be provided around generators to provide illumination in the event of a concurrent generator and utility failure. Similarly, UPS-fed receptacles should also be provided around the generators.

Permanent load banks or accommodations to facilitate connection of portable load banks are strongly recommended for any generator system.

In addition to individual testing of components, the standby generation system, UPS systems, and automatic transfer switches should be tested together as a system. At minimum, the tests should simulate a utility failure and restoration of normal power. Failure of individual components should be tested in redundant systems designed to continue functioning during the failure of a component. The systems should be tested under load using load banks. Additionally, once the data center is in operation, the systems should be tested periodically to ensure that they will continue to function properly.

The standby generator system may be used for emergency lighting and other life-safety loads in addition to the data center loads if allowed by local authorities. The National Electrical Code (NEC) requires that a separate transfer switch and distribution system be provided to serve life-safety loads. Battery-powered emergency lighting equipment may be less expensive than a separate automatic transfer switch and distribution system.

Isolation/bypass is required by the NEC for life-safety transfer switches to facilitate maintenance. Similarly, automatic transfer switches with bypass isolation should be provided to serve data center equipment. Transfer circuit breakers can also be used to transfer loads from utility to generator however, bypass isolation of circuit breakers should be added in case of circuit breaker failure during operation.

See IEEE Standard 1100 and IEEE Standard 446 for recommendations on standby generation.

G.5.1.3 Uninterruptible power supply (UPS)

UPS systems can be static, rotary or hybrid type and can either be online, offline or line interactive with sufficient backup time for the standby generator system to come online without interruption of power. Static UPS systems have been used almost exclusively in the United States for the last several years, and are the only systems described in detail herein; the redundancy concepts described are generally applicable to rotary or hybrid systems as well, however.

UPS systems may consist of individual UPS modules or a group of several paralleled modules. Each module should be provided with a means of individual isolation without affecting the integrity of operation or redundancy. The system should be capable of automatic and manual internal by-pass and should be provided with external means to bypass the system and avoid interruption of power in the event of system failure or maintenance.

Individual battery systems may be provided for each module; multiple battery strings may be provided for each module for additional capacity or redundancy. It is also possible to serve several UPS modules from a single battery system, although this is typically not recommended due to the very low expected reliability of such a system.

When a generator system is installed, the primary function of the UPS system is to provide ride-through during a power outage until the generators start and come on-line or the utility returns. Theoretically, this would imply a required battery capacity of only a few seconds. However, in practice, the batteries should be specified for a minimum of 5 to 30 minute capacity at full-rated UPS load due to the unpredictable nature of battery output curves and to provide redundant battery strings or to allow for sufficient orderly shutdown should the generator system fail. If no generator is installed, sufficient batteries should be provided, at a minimum, for that time required for an orderly shutdown of computer equipment; that will typically range from 30 minutes to 8 hours. Greater battery capacities are often specified for specific installations. For example, telephone companies have traditionally mandated a run-time of 4 hours where generator backup is provided, and 8 hours where no generator is installed; telecommunications companies and collocation facilities often adhere to these telephone company requirements.

Consideration should be given to a battery monitoring system capable of recording and trending individual battery cell voltage and impedance or resistance. Many UPS modules provide a basic level of monitoring of the overall battery system, and this should be sufficient if redundant modules with individual redundant battery strings have been installed. However, UPS battery monitoring systems are not capable of detecting individual battery jar failure, which can greatly impact battery system runtime and reliability. A standalone battery monitoring system, capable of monitoring the impedance of each individual battery jar as well as predicting and alarming on impending battery failure, provides much greater detail on the actual battery status. Such battery monitoring systems are strongly recommended where a single, non-redundant battery system has been provided. They are also required where the highest possible level of system reliability is desired (tier 4).

Heating ventilation and air conditioning, hydrogen monitoring, spill control, eye wash and safety showers should be considered on a case by case basis.

There are two primary battery technologies that can be considered: valve-regulated lead-acid (VRLA), which are also known as sealed-cell or immobilized-electrolyte; and flooded-cell batteries. Valve-regulated lead-acid (VRLA) batteries have a smaller footprint than flooded-cell batteries as they can be mounted in cabinets or racks, are virtually maintenance free, and usually require less ventilation than flooded-cell batteries, as they tend to produce less hydrogen. Flooded-cell batteries typically have lower life-cycle costs and a much longer expected lifespan than valve-regulated lead-acid (VRLA) batteries, but require periodic maintenance, take up more floor space as they cannot be mounted in cabinets, and typically have additional acid-containment and ventilation requirements.

Typical design criteria may specify a required power density of anywhere from 0.38 to 2.7 kilowatts per square meter (35 to 250 watts per square foot). The UPS system selection therefore should be based on a UPS system kW rating which meets the design criteria, which is typically exceeded prior to the UPS system kVA rating. This is due to the relatively low power factor ratings of UPS modules compared to the computer equipment requirements: UPS modules are typically rated at 80% or 90%, or unity power factor, versus modern computer equipment which typically has a power factor of 98% or higher. In addition, a minimum 20% allowance in UPS capacity should be provided above that power density requirement for future growth and to ensure the UPS rating is not exceeded during periods of peak demand.

Precision Air Conditioning (PAC) units should be provided for the UPS and battery rooms. Battery life spans are severely affected by temperature; a five-degree higher temperature deviation can shorten the battery life by a year or more. Lower temperature can cause the batteries to deliver less than its capacity.

Redundant UPS systems can be arranged in different configuration. The three main configurations are isolated redundant, parallel redundant and distributed isolated redundant. The reliability of the configurations varies with distributed isolated redundant being the most reliable.

Stand alone UPS systems should not be used on circuits already supported by a centralized UPS, unless the stand alone UPS systems are tied to the centralized UPS system and configured to work in concert with it. Stand alone UPS systems on circuits served by a centralized UPS system may reduce rather than improve availability if they function completely independently from the centralized UPS.

Any UPS systems located in the computer room should be tied to the computer room EPO (Emergency Power Off) system so that the UPS systems do not continue to provide power if the EPO is activated.

Additional information on UPS system design is available in IEEE Standard 1100.

G.5.1.4 Computer power distribution

Power Distribution Units (PDUs) should be considered for distribution to critical electronic equipment in any data center installation as they combine the functionality of several devices into one enclosure, which is often smaller, and more effective than the installation of several discrete panel boards and transformers. If the computer room space is subdivided into different rooms or spaces each supported by its own emergency power off (EPO) system, then each of these spaces should have its own horizontal distribution area.

PDUs should be provided complete with an isolation transformer, Transient voltage surge suppression (TVSS), output panels, and power monitoring. Such packages offer several advantages over traditional transformer and panel installations.

A typical PDU will include all of the following:

- transformer disconnect. Dual input circuit breakers should be considered to allow connection of a temporary feeder for maintenance or source relocation without shutting down the critical loads;

- transformer: This should be located as close to the load as possible to minimize common-mode noise between ground and neutral and to minimize differences between the voltage source ground and signal ground. The closest possible location is achieved when the transformer is located within the PDU enclosure. The isolation transformer is usually configured as a 480:208V/120 volt step-down transformer to reduce the feeder size from the UPS to the PDU. To withstand the heating effects of harmonic currents, K-rated transformers should be used. To reduce harmonic currents and voltages, a zigzag harmonic canceling transformer or transformer with an active harmonic filter can be used. Minimizing harmonics in the transformer improves the efficiency of the transformer and reduces the heat load produced by the transformer;

- transient voltage surge suppression (TVSS): Similarly, the effectiveness of Transient voltage surge suppression (TVSS) devices is greatly increased when the lead lengths are kept as short as possible, preferably less than 200 mm (8 in). This is facilitated by providing the Transient voltage surge suppression (TVSS) within the same enclosure as the distribution panel boards;

- distribution panel boards: Panel boards can be mounted in the same cabinet as the transformer or in cases where more panel boards are needed, a remote power panel can be used;

- metering, monitoring, alarming, and provisions for remote communications: such features would typically imply substantially space requirements when provided with a traditional panel board system;

- emergency Power Off (EPO) controls;

- single-point ground bus;

- conduit landing plate: In most data centers, each equipment rack is powered from at least one dedicated circuit, and each circuit is provided with a separate, dedicated conduit. Most panel board enclosures do not have the physical space to land up to 42 separate conduits. PDU conduit landing plates are designed to accommodate up to 42 conduits per output panel, greatly facilitating the original installation as well as later changes.

PDU features may also include dual input breakers, static transfer switches, input filters, and redundant transformers. PDUs may also be specified to be provided complete with input junction boxes to facilitate under floor connections.

Emergency Power Off (EPO) systems should be provided as required by National Electrical Code (NEC) Article 645. Emergency Power Off (EPO) stations should be located at each exit from each data center space, and should be provided with protective covers to avoid accidental operation. A telephone and list of emergency contacts should be located adjacent to each Emergency Power Off (EPO) station. An Emergency Power Off (EPO) maintenance bypass system should be considered to minimize the risk of accidental power outages during Emergency Power Off (EPO) system maintenance or expansion. An abort switch should be considered to inhibit shutdown of power upon accidental activation. Emergency Power Off (EPO) system control power should be supervised by the fire alarm control panel per National Fire Protection Association (NFPA) 75. The power to all electronic equipment should be automatically disconnected upon activation of a gaseous agent total flooding suppression system. Automatic disconnection is recommended, but not required, on sprinkler activation.

Under floor power distribution is most commonly accomplished using factory-assembled PVC-coated flexible cable assemblies, although in some jurisdictions this may not be permitted and hard conduit may instead be required. To accommodate future power requirements, consideration should be given to the installation of three-phase cabling at ampacities of up to 50 or 60 amps even if such power is not currently required.

Every computer room, entrance room, access provider room, and service provider room circuit should be labeled at the receptacle with the PDU or panel board identifier and circuit breaker number.

Additional information on computer power distribution design for data centers is available in IEEE Standard 1100.

G.5.1.5 Building grounding and lightning protection systems

A building perimeter ground loop should be provided, consisting of #4/0 AWG (minimum) bare copper wire buried 1 m (3 ft) deep and 1 m (3 ft) from the building wall, with 3 m x 19 mm (10 ft x ¾ in) copper-clad steel ground rods spaced every 6 to 12 m (20 to 40 ft) along the ground loop. Test wells should be provided at the four corners of the loop. Building steel should be bonded to the system at every other column. This building grounding system should be directly bonded to all major power distribution equipment, including all switchgear, generators, UPS systems, transformers, etc., as well as to the telecommunications systems and lightning protection system. Ground busses are recommended to facilitate bonding and visual inspection.

No portion of the grounding systems should exceed 5 ohms to true earth ground as measured by the four-point fall-of-potential method.

A UL Master-Labeled lightning protection system should be considered for all data centers. The Risk Analysis Guide provided in NFPA 780, which takes into account geographical location and building construction among other factors, can be very useful in determining the suitability of a lightning protection system. If a lightning protection system is installed, it should be bonded to the building grounding system as required by code and as required for maximum equipment protection.

Aditional information on building grounding and lightning protection system design is available in IEEE Standard 1100.

G.5.1.6 Data center grounding infrastructure.

IEEE Standard 1100 provides recommendations for the electrical design of bonding and grounding. Consideration should be given to installing a common bonding network (CBN) such as a signal reference structure as described in IEEE Standard 1100 for the bonding of telecommunications and computer equipment.

The computer room grounding infrastructure creates an equipotential ground reference for computer room and reduces stray high frequency signals. The data center grounding infrastructure consists of a copper conductor grid on 0.6 to 3 m (2 to 10 ft) centers that covers the entire computer room space. The conductor should be no smaller than #6 AWG or equivalent. Such a grid can use either bare or insulated copper conductors. The preferred solution is to use insulated copper, which is stripped where connections should be made. The insulation prevents intermittent or unintended contact points. The industry standard color of the insulation is green or marked with a distinctive green color as in ANSI-J-STD-607-A.

Other acceptable solutions include a prefabricated grid of copper strips welded into a grid pattern on 200 mm (8 in) centers which is rolled out onto the floor in sections, or chicken wire, which is similarly installed, or an electrically continuous access-floor system which has been designed to function as a data center grounding infrastructure and which is bonded to the building grounding system.

The data center grounding infrastructure should have the following connections:

- 1 AWG or larger bonding conductor to Telecommunications Grounding Busbar (TGB) in the computer room. Refer to ANSI/TIA/EIA-J-STD-607-A Commercial Building Grounding and Bonding Requirements for Telecommunications for the design of the Telecommunications Grounding and Bonding Infrastructure;

- a bonding conductor to the ground bus for each PDU or panel board serving the room, sized per NEC 250.122 and per manufacturers' recommendations;

- 6 AWG or larger bonding conductor to HVAC equipment;

- 4 AWG or larger bonding conductor to each column in the computer room;

- 6 AWG or larger bonding conductor to each cable ladder, cable tray, and cable wireway entering room;

- 6 AWG or larger bonding conductor to each conduit, water pipe, and duct entering room;

- 6 AWG or larger bonding conductor to every 6th access floor pedestal in each direction;

- 6 AWG or larger bonding conductor to each computer or telecommunications cabinet, rack, or frame. Do not bond racks, cabinets, and frames serially.

IEEE Standard 1100 provides recommendations for the electrical design of bonding and grounding. Consideration should be giving to installing a common bonding network (CBN) such as a signal reference structure as described in IEEE Standard 1100 for the bonding of telecommunications and computer equipment.

G.5.1.7 Computer or telecommunications rack or frame grounding

G.5.1.7.1 The rack framework grounding conductor

Each equipment cabinet and equipment rack requires its own grounding connection to the data center grounding infrastructure. A minimum of a # 6 AWG copper conductor should be used for this purpose. The recommended conductor types are:

- Bare copper

- Insulated green, UL VW1 flame rated

- Code or Flex Cable is acceptable

G.5.1.7.2 Rack grounding connection point

Each cabinet or rack should have a suitable connection point to which the rack framework grounding conductor can be bonded. Options for this connection point are:

- Rack ground bus: Attach a dedicated copper ground bar or copper strip to the rack. A bond between the ground bar or strip and the rack should exist. The mounting screws should be of the thread-forming type, not self-tapping or sheet metal screws. Thread-forming screws are tri-lobular and create threads by the displacement of metal without creating chips or curls, which could damage adjacent equipment.

- Direct connection to the rack: If dedicated copper ground bars or strips and associated thread-forming screws are not used, then paint should be removed from the rack at the connection point, and the surface should be brought to a shiny gloss for proper bonding using an approved antioxidant.

G.5.1.7.3 Bonding to the rack

When bonding the rack framework grounding conductor to the connection point on the cabinet or rack, it is desirable to use two-hole lugs. The use of two-hole lugs helps to insure that the ground connection does not become loose due to excessive vibration or movement of the attaching cable. The connection to the rack should have the following characteristics:

- Bare metal-to-metal contact

- Antioxidant recommended

G.5.1.7.4 Bonding to the data center grounding infrastructure

Attach the opposite end of the rack framework grounding conductor to the data center grounding infrastructure. The connection should use a compression type copper tap that is UL / CSA listed.

G.5.1.7.5 Rack continuity

Every structural member of the cabinet or rack should be grounded. This is achieved by assembling the cabinet or rack in such a way that there is electrical continuity throughout its structural members, as described below:

- For welded racks: the welded construction serves as the method of bonding the structural members of the rack together.

- Bolt together racks: special consideration should be taken while assembling bolted racks. Ground continuity cannot be assumed through the use of normal frame bolts used to build or stabilize equipment racks and cabinets. Bolts, nuts and screws used for rack assembly are not specifically designed for grounding purposes. Additionally, most racks and cabinets are painted. Since paint is not a conductor of electrical current, paint can become an insulator and negate any attempt to accomplish desired grounding. Most power is routed over the top or bottom of the rack. Without a reliable bond of all four sides of the rack, a safety hazard in case of contact with live feeds exists. Removing paint at the point of contact with assembly hardware is an acceptable method of bonding. This method is labor intensive but effective. An alternate method is the use of aggressive Type “B” internal-external tooth lock washers, as shown in figure 18. With the bolts torqued, an acceptable bond can be made. Two washers are necessary to accomplish this: one under the bolt head contacting and cutting paint and one under the nut, as shown in Figure 18.

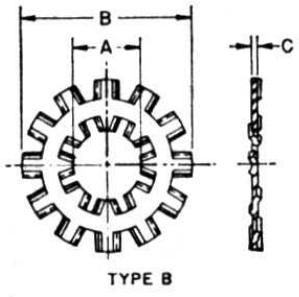


Figure 18: American standard internal-external tooth lock washer (ASA B27.1-1965), Type B

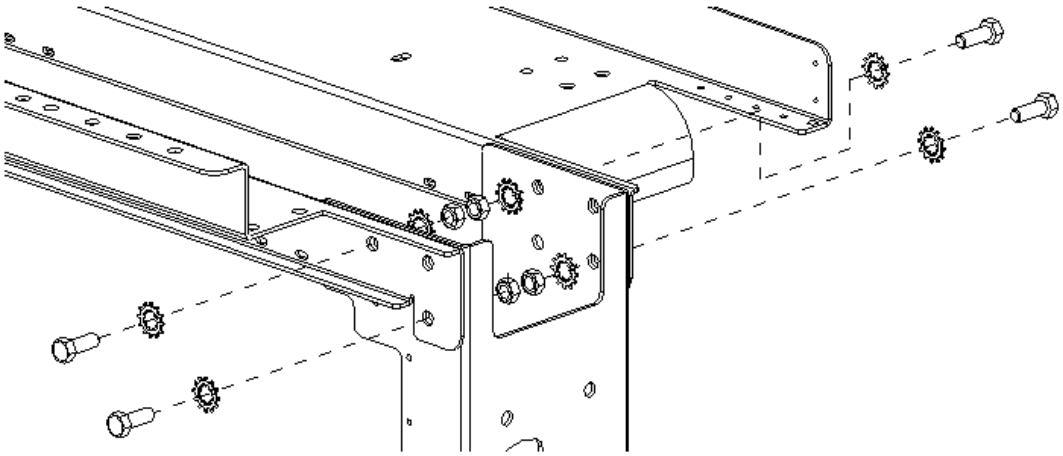


Figure 19: Typical rack assembly hardware

G.5.1.8 Rack-mounted equipment grounding

G.5.1.8.1 Grounding the equipment chassis

It is recommended that rack-mounted equipment be bonded and grounded via the chassis, in accordance with the manufacturer's instructions. Provided the rack is bonded and grounded according to G.5.1.7, the equipment chassis should be bonded to the rack using one of the following methods:

To meet the chassis grounding requirements; the manufacturer may supply a separate grounding hole or stud. This should be used with a conductor of proper size to handle any fault currents up to the limit of the circuit protection device feeding power to the equipment unit. One end of this chassis grounding conductor will be bonded to the chassis hole or stud, and the other end will be properly bonded to the copper ground bar or strip. In some instances, it may be preferable to bypass the copper ground bar or strip and bond the chassis grounding conductor directly to the data center grounding infrastructure.

If the equipment manufacturer suggests grounding via the chassis mounting flanges and the mounting flanges are not painted, the use of thread-forming tri-lobular screws and normal washers will provide an acceptable bond to the rack.

If the equipment mounting flanges are painted, the paint can be removed, or the use of the same thread-forming screws and aggressive internal-external tooth lock washers, designed for this application, will supply an acceptable bond to safety ground through the rack.

G.5.1.8.2 Grounding through the equipment ac (alternating current) power cables

Although ac powered equipment typically has a power cord that contains a ground wire, the integrity of this path to ground cannot be easily verified. Rather than relying on the ac power cord ground wire, it is desirable that equipment be grounded in a verifiable manner such as the methods described above in G.5.1.8.

G.5.1.9 Electro static discharge wrist straps

The use of static discharge wrist straps when working on or installing network or computer hardware is specified in most manufacturers' installation guidelines. Wrist strap ports should be attached to the rack by a means that ensures electrical continuity to ground.

G.5.1.10 Building management system

A building management system (BMS) may be provided to monitor and control the operation of the mechanical and electrical system. Analog or digital meters locally mounted at the equipment being monitored achieve monitoring of power. The UPS system is equipped with battery string monitoring system to provide an indication of the discharge.

G.5.2 Electrical tiering

G.5.2.1 Tier 1 (electrical)

A tier 1 facility provides the minimum level of power distribution to meet the electrical load requirements, with little or no redundancy. The electrical systems are single path, whereby a failure of or maintenance to a panel or feeder will cause partial or total interruption of operations. No redundancy is required in the utility service entrance.

Generators may be installed as single units or paralleled for capacity, but there is no redundancy requirement. One or more automatic transfer switches are typically used to sense loss of normal power, initiation of generator start and transfer of loads to the generator system. Isolation-bypass automatic transfer switches (ATSs) or automatic transfer circuit breakers are used for this purpose but not required. Permanently installed load banks for generator and UPS testing are not required. Provision to attach portable load banks is required.

The uninterruptible power supply system can be installed as a single unit or paralleled for capacity. Static, rotary or hybrid UPS technologies can be utilized, with either double conversion or line interactive designs. Compatibility of the UPS system with the generator system is required. The UPS system should have a maintenance bypass feature to allow continuous operation during maintenance of the UPS system.

Separate transformers and panel boards are acceptable for the distribution of power to the critical electronic loads in tier 1 data centers. The transformers should be designed to handle the non-linear load that they are intended to feed. Harmonic canceling transformers can also be used in lieu of K-rated transformers.

Power distribution units (PDU) or discrete transformers and panel boards may be used to distribute power to the critical electronic loads. Any code compliant wiring method may be utilized. Redundancy is not required in the distribution system. Grounding system should conform to minimum code requirements.

A data center grounding infrastructure is not required, but may be desirable as an economical method to satisfy equipment manufacturers' grounding requirements. The decision to install lightning protection should be based on a lightning risk analysis per NFPA 780 and insurance requirements. If the data center is classified as an Information Technology Equipment Room per NEC 645, an Emergency Power Off (EPO) system should be provided.

Monitoring of electrical and mechanical systems is optional.

G.5.2.2 Tier 2 (electrical)

Tier 2 installations should meet all requirements of tier 1. In addition, tier 2 installations should meet the additional requirements specified in this annex.

A tier 2 facility provides for N+1 redundant UPS modules. A generator system sized to handle all data center loads is required, although redundant generator sets are not required. No redundancy is required in the utility service entrance or power distribution system.

Provisions to connect portable load banks should be provided for generator and UPS testing.

Power distribution units (PDUs) should be used to distribute power to the critical electronic loads. Panel boards or PDU “sidecars” may be sub-fed from PDUs where additional branch circuits are required. Two redundant PDUs, each preferably fed from a separate UPS system, should be provided to serve each computer equipment rack; single cord and three cord computer equipment should be provided with a rack-mount fast-transfer switch or static switch fed from each PDU. Alternatively, dual-fed static-switch PDUs fed from separate UPS systems can be provided for single cord and three-cord equipment, although this arrangement offers somewhat less redundancy and flexibility. Color-coding of nameplates and feeder cables to differentiate A and B distribution should be considered, for example, all A-side white, all B-side blue.

A circuit should not serve more than one rack to prevent a circuit fault from affecting more than one rack. To provide redundancy, racks and cabinets should each have two dedicated 20-amp 120-volt electrical circuits fed from two different Power Distribution Units (PDUs) or electrical panels. For most installations, the electrical receptacles should be locking NEMA L5-20R receptacles. Higher ampacities may be required for high-density racks, and some new-technology servers may possibly require one or more single or three phase 208-volt receptacles rated for 50 amps or more. Each receptacle should be identified with the PDU and circuit number, which serves it. Redundant feeder to mechanical system distribution board is recommended but not required.

The building grounding system should be designed and tested to provide an impedance to earth ground of less than five ohms. A common bonding network should be provided (see subclause G.5.1.6). An Emergency Power Off (EPO) system should be provided.

G.5.2.3 Tier 3 (electrical)

Tier 3 installations should meet all requirements of tier 2. In addition, tier 3 installations should meet the additional requirements specified in this annex.

All systems of a tier 3 facility should be provided with at least N+1 redundancy at the module, pathway, and system level, including the generator and UPS systems, the distribution system, and all distribution feeders. The configuration of mechanical systems should be considered when designing the electrical system to ensure that N+1 redundancy is provided in the combined electrical-mechanical system. This level of redundancy can be obtained by either furnishing two sources of power to each air conditioning unit, or dividing the air conditioning equipment among multiple sources of power. Feeders and distribution boards are dual path, whereby a failure of or maintenance to a cable or panel will not cause interruption of operations. Sufficient redundancy should be provided to enable isolation of any item of mechanical or electrical equipment as required for essential maintenance without affecting the services being provided with cooling. By employing a distributed redundant configuration, single points of failure are virtually eliminated from the utility service entrance down to the mechanical equipment, and down to the PDU or computer equipment.

At least two utility feeders should be provided to serve the data center at medium or high voltage (above 600 volts). The configuration of the utility feeder should be primary selective, utilizing

automatic transfer circuit breakers or automatic isolation-bypass transfer switches. Alternately, an automatic main-tie-main configuration can be used. Padmounted, substation, or dry-type distribution transformers can be utilized. The transformers should be configured for N+1 or 2N redundancy and should be sized based on open-air ratings. A standby generator system is used to provide power to the uninterruptible power supply system and mechanical system. On-site fuel storage should be sized to provide a minimum of 72 hours of generator operation at the design loading condition.

Isolation-bypass automatic transfer switches or automatic transfer breakers should be provided to sense loss of normal power, initiate generator start and transfer loads to the generator system. Duplex pumping systems should be provided with automatic and manual control, with each pump fed from separate electrical sources. Isolated, redundant fuel tanks and piping systems should be provided to ensure that fuel system contamination or mechanical fuel system failure does not affect the entire generator system. Dual redundant starters and batteries should be provided for each generator engine. Where paralleling systems are employed, they should be provided with redundant control systems.

To increase the availability of power to the critical load, the distribution system is configured in a distributed isolated redundant (dual path) topology. This topology requires the use of automatic static transfer switches (ASTS) placed either on the primary or secondary side of the PDU transformer. Automatic static transfer switches (ASTS) requirements are for single cord load only. For dual cord (or more) load design, affording continuous operation with only one cord energized, no automatic static transfer switches (ASTS) is used, provided the cords are fed from different UPS sources. The automatic static transfer switches (ASTS) will have a bypass circuit and a single output circuit breaker.

A data center grounding infrastructure and lightning protection system should be provided. Transient voltage surge suppression (TVSS) should be installed at all levels of the power distribution system that serve the critical electronic loads.

A central power and environmental monitoring and control system (PEMCS) should be provided to monitor all major electrical equipment such as main switchgears, generator systems, UPS systems, automatic static transfer switches (ASTS), power distribution units, automatic transfer switches, motor control centers, transient voltage surge suppression systems, and mechanical systems. A separate programmable logic control system should be provided, programmed to manage the mechanical system, optimize efficiency, cycle usage of equipment and indicate alarm condition.

Redundant server is provided to ensure continuous monitoring and control in the event of a server failure.

G.5.2.4 Tier 4 (electrical)

Tier 4 installations should meet all requirements of tier 3. In addition, tier 4 installations should meet the additional requirements specified in this annex.

Tier 4 facilities should be designed in a ‘2(N+1)’ configuration in all modules, systems, and pathways. All feeders and equipment should be capable of manual bypass for maintenance or in the event of failure. Any failure will automatically transfer power to critical load from failed system to alternate system without disruption of power to the critical electronic loads.

A battery monitoring system capable of individually monitoring the impedance or resistance of each cell and temperature of each battery jar and alarming on impending battery failure should be provided to ensure adequate battery operation.

The utility service entrances should be dedicated to the data center and isolated from all non-critical facilities.

The building should have at least two utility feeders from different utility substations for redundancy.

G.6 Mechanical systems requirements

G.6.1 General mechanical requirements

G.6.1.1 Environmental air

The mechanical system should be capable of achieving the following computer room environmental parameters:

Temperature: 20°C to 25°C (68°F to 77°F)

Normal set points:

22°C (72°F)

Control ± 1°C (2°F)

Relative Humidity: 40%to 55%

Normal set points:

45% RH

Control ± 5%

Coordinate cooling system design and equipment floor plans so that airflow from cooling equipment travels in a direction parallel to the rows of cabinets/racks.

Print rooms should be isolated rooms with separate air conditioning system so as not to introduce contaminants such as paper and toner dust into the remainder of the data center.

G.6.1.2 Ventilation air

The computer room should receive outside air ventilation for occupants. The ventilation air should be introduced at the ceiling level, near the computer room air conditioning units when those units are located inside the computer room.

The computer room should receive supply air for ventilation and positive pressurization purposes. Return and exhaust air for the computer room is not required.

G.6.1.3 Computer room air conditioning

The air-conditioning system should be designed to provide the design temperature and humidity conditions recommended by the manufacturers of the servers to be installed within the data center.

Chilled-water systems are often more suitable for larger data centers. DX units may be more convenient for smaller data centers and do not require water piping to be installed in the computer and telecommunications equipment areas.

Equipment with high heat loads may require air ducts or access floors to provide adequate cooling.

G.6.1.4 Leak detection system

A leak detection system consisting of both distributed-type cable sensors and point sensors should be considered wherever the threat of water exists. Cable sensors offer greater coverage and increase the chances that a leak will be accurately detected. Point sensors are less expensive, require less frequent replacement, and are very suitable when low spots in the floor can be determined. A framed plan indicating cable routing and periodically indicating cable lengths calibrated to the system should be provided adjacent to the system alarm panel.

G.6.1.5 Building management system

A Building Management System (BMS) should monitor all mechanical, electrical, and other facilities equipment and systems. The system should be capable of local and remote monitoring and operation. Individual systems should remain in operation upon failure of the central Building Management System (BMS) or head end. Consideration should be given to systems capable of controlling (not just monitoring) building systems as well as historical trending. 24-hour monitoring of the Building Management System (BMS) should be provided by facilities personnel, security personnel, paging systems, or a combination of these. Emergency plans should be developed to enable quick response to alarm conditions.

G.6.1.6 Plumbing systems

No water or drain piping should be routed through the data center that is not associated with data center equipment. Water or drain piping that should be routed within the data center should be either encased or provided with a leak protection jacket. A leak detection system should be provided to notify building operators in the event of a water leak. Tier 3 and 4 data centers should only have water or drain piping that supports data center equipment routed through the computer room space.

G.6.1.7 Emergency fixtures

An emergency eye wash/shower should be located in battery rooms that have wet cell batteries.

G.6.1.8 HVAC make-up water

Domestic “cold” water make-up should be provided for all the computer room air conditioning units containing a humidifier.

Provide the required backflow preventer on the domestic “cold” water piping; coordinate with the local code authority.

Piping material should be type “L” copper with soldered joints. Combustible piping should not be used.

G.6.1.9 Drainage piping

Provide floor drain(s) within the computer room to collect and drain the pre-action sprinkler water after a discharge. The floor drain(s) should receive the condensate drain water and humidifier flush water from the computer room air conditioning units.

Piping material should be type “L” copper with soldered joints. Combustible piping should not be used.

G.6.1.10 Fire protection systems

The risk factors to be considered when selecting a protection scheme for the data center can be categorized into four main areas. The first is the matter of the safety of individuals or property affected by the operation (e.g., life support systems, telecommunications, transportation system controls, process controls). The next is the fire threat to the occupants in confined areas or the threat to exposed property (e.g., records, disk storage). The next is the economic loss from business interruption due to downtime and lastly is the loss from the value of the equipment. These four areas should be carefully evaluated to determine the appropriate level of protection for the facility in consideration.

The following describes the various levels of protection that can be provided for the data center. The minimum level of protection required by code includes an ordinary sprinkler system along with the appropriate clean-agent fire extinguishers. This Standard specifies that any sprinkler systems be pre-action sprinklers.

Advanced detection and suppression systems beyond minimum code requirements include air sampling smoke detection systems, pre-action sprinkler systems and clean agent suppression systems.

Fire Detection and Alarm, Air Sampling Smoke Detection, significant equipment damage can occur solely due to smoke or other products of combustion attacking electronic equipment. Therefore, early warning detection systems are essential to avoid the damage and loss that can occur during the incipient stages of a fire. An air sampling smoke detection system provides another level of protection for the computer room and associated entrance facilities, mechanical rooms, and electrical rooms. This system is provided in lieu of ordinary smoke detectors, as its sensitivity and detection capability are far beyond that of conventional detectors. The less sensitive detection mechanism used by conventional detectors requires a much larger quantity of smoke before they even detect a fire. In a data center, this difference and time delay is especially pronounced due to the high airflow through the room, which tends to dilute smoke and further delay ordinary detectors.

There are, however, some various early warning systems that air sampling detection systems that utilize conventional ionization or photoelectric detectors. There are also laser-based smoke detectors that do not use air sampling and do not provide an equivalent level of early warning detection to standard air sampling detection systems. The same is also true for beam detectors as well as conventional ionization and photoelectric smoke detectors. These alternate smoke detection systems may be appropriate in data centers where the loss potential and adverse consequences of system downtime are not considered critical. Where conventional smoke detection is chosen, a combination of ionization and photoelectric should be used.

The recommended smoke detection system for critical data centers where high airflow is present is one that will provide early warning via continuous air sampling and particle counting and have a range up to that of conventional smoke detectors. These features will enable it to also function as the primary detection system and thus eliminate the need for a redundant conventional detection system to activate suppression systems.

The most widely used type of air-sampling system consists of a network of piping in the ceiling and below the access floor that continuously draws air from the room into a laser based detector. Any release of smoke or other particles (even from an overheated piece of equipment) into the room air can be detected in its very early stages due to the high sensitivity of the laser. The early response capability affords the occupants an opportunity to assess a situation and respond before the event causes significant damage or evacuation. In addition, the system has four levels of alarm that range from detecting smoke in the invisible range up to that detected by conventional detectors. The system at its highest alarm level would be the means to activate the pre-action system valve. Designs may call for two or more systems. One system would be at the

ceiling level of the computer room, entrance facilities, electrical rooms, and mechanical rooms as well as at the intake to the computer room air-handling units. A second system would cover the area under the access floor in the computer room, entrance facilities, electrical rooms, and mechanical rooms. A third system is also recommended for the operations center and printer room to provide a consistent level of detection for these areas. The separate systems allow separate thresholds and separate baseline readings of normalcy, to optimize early detection while minimizing false alarms. These units can if desired be connected into the network for remote monitoring.

G.6.1.11 Water suppression – pre-action suppression

A pre-action sprinkler system provides the next level of protection for the data center as it affords a higher level of reliability and risk mitigation. The pre-action system is normally air filled and will only allow water in the piping above the data center when the smoke detection system indicates there is an event in progress. Once the water is released into the piping, it still requires a sprinkler to activate before water is released into the room. This system addresses a common concern regarding leakage from accidental damage or malfunction. Pre-action sprinklers should protect the operations center, printer room, and electrical rooms, and mechanical rooms, since they are also considered essential to the continuity of operations. In retro-fit situations, any existing wet-pipe sprinkler mains and branch pipes should be relocated outside the boundaries of the data center to eliminate any water filled piping above the space.

Sprinkler protection under access floors is sometimes an issue that is queried on for data centers. However, in general, such protection should be avoided whenever possible as its effectiveness is usually limited to certain applications where the floor is over 410 mm (16 in) high and the combustible loading under the floor is significant. This protection can usually be omitted where the following favorable conditions are present.

The cable space is used as an air plenum, the cables are FM group 2 or 3, the signal cables outnumber the power cables by 10 to 1, the cable has not been subject to significant deterioration due to thermal degradation or mechanical damage, the access floor is noncombustible, the subfloor space is accessible, and there are no power cables unrelated to the data center or steam lines or any other significant sources of heat in the subfloor space. Where a need for a suppression system in a subfloor space is deemed appropriate, consideration should also be given to clean agent systems as an alternate means to accomplish this protection.

G.6.1.12 Gaseous suppression - clean agent fire suppression

A clean agent fire suppression system provides the highest level of protection for the computer room and the associated electrical and mechanical rooms. This system would be installed in addition to the pre-action suppression and smoke detection systems. The fire suppression system is designed, upon activation, to have the clean agent gas fully flood the room and the under floor area. This system consists of a nontoxic gas that is superior to sprinkler protection in several ways. Firstly, the agent can penetrate computer equipment to extinguish deep-seated fires in electronic and related equipment. Secondly, unlike sprinklers there is no residual from the gas to be removed after the system is activated. Lastly, this agent allows the fire to be extinguished without adversely affecting the other equipment not involved in the fire. Therefore, by using gaseous suppression the data center could readily return to operation after an event with minimal delay and the loss would be limited to the affected items only.

Effective room sealing is required to contain the clean agent so that effective concentrations are achieved and maintained long enough to extinguish the fire.

NFPA recommends that the electronic and HVAC equipment be automatically shut down in the event of any suppression system discharge, although the reasoning behind this is different for water-based and clean agent systems. Electronic equipment can often be salvaged after contact

with water so long as it has been de-energized prior to contact, the automatic shutdown is recommended primarily to save the equipment. With clean-agent systems, the concern is that an arcing fault could re-ignite a fire after the clean agent has dissipated. In either case, however, the decision to provide for automatic shutdown is ultimately the owner's, who may determine that continuity of operations outweighs either of these concerns.

Owners need to carefully assess their risks to determine if the data center should include a clean agent gas suppression system.

Local codes may dictate the type of clean agent suppression system that may be used. Additional information on clean Agent Fire Extinguishing Systems is available in NFPA 2001.

G.6.1.13 Hand held fire extinguishers

A clean agent fire extinguisher is recommended for the computer room as it avoids the dry chemical powder of ordinary ABC fire extinguishers, which can impact associated equipment. This impact goes beyond that of the fire and usually requires a significant clean up effort. See NFPA 75 for guidance regarding hand held fire extinguishers.

G.6.2 Mechanical tiering

G.6.2.1 Tier 1 (mechanical)

The HVAC system of a tier 1 facility includes single or multiple air conditioning units with the combined cooling capacity to maintain critical space temperature and relative humidity at design conditions with no redundant units. If these air conditioning units are served by a water-side heat rejection system, such as a chilled water or condenser water system, the components of these systems are likewise sized to maintain design conditions, with no redundant units. The piping system or systems are single path, whereby a failure of or maintenance to a section of pipe will cause partial or total interruption of the air conditioning system.

If a generator is provided, all air-conditioning equipment should be powered by the standby generator system.

G.6.2.2 Tier 2 (mechanical)

The HVAC system of a tier 2 facility includes multiple air conditioning units with the combined cooling capacity to maintain critical space temperature and relative humidity at design conditions, with one redundant unit (N+1). If these air conditioning units are served by a water system, the components of these systems are likewise sized to maintain design conditions, with one redundant unit(s). The piping system or systems are single path, whereby a failure of or maintenance to a section of pipe will cause partial or total interruption of the air conditioning system.

Air-conditioning systems should be designed for continuous operation 7 days/24 hours/365 days/year, and incorporate a minimum of N+1 redundancy in the Computer Room Air Conditioning (CRAC) units.

The computer room air conditioners (CRAC) system should be provided with N+1 redundancy, with a minimum of one redundant unit for every three or four required units.

The computer rooms and other associated spaces should be maintained at positive pressure to rooms unrelated to the data center as well as to the outdoors.

All air-conditioning equipment should be powered by the standby generator system.

Power circuits to the air-conditioning equipment should be distributed among a number of power panels/distribution boards to minimize the effects of electrical system failures on the air-conditioning system.

All temperature control systems should be powered through redundant dedicated circuits from the UPS.

Air supply to the data center should be coordinated with the types and layouts of the server racks to be installed. The air handling plant should have sufficient capacity to support the total projected heat load from equipment, lighting, the environment, etc., and maintain constant relative humidity levels within the data center. The required cooling capacity should be calculated based on the kW (not kVA) supply available from the UPS system.

The conditioned air should be distributed to the equipment via the access floor space through perforated floor panels with balancing dampers.

A diesel-fired standby generator system should be installed to provide power to the uninterruptible power supply system and mechanical equipment. On-site fuel storage tanks should be sized to provide a minimum of 24 hours of generator operation at the design loading condition. Duplex pumping systems should be provided with automatic and manual control, with each pump fed from separate electrical sources. Redundancy and isolation should be provided in the fuel storage system to ensure that fuel system contamination or a mechanical fuel system failure does not affect the entire generator system.

G.6.2.3 Tier 3 (mechanical)

The HVAC system of a tier 3 facility includes multiple air conditioning units with the combined cooling capacity to maintain critical space temperature and relative humidity at design conditions, with sufficient redundant units to allow failure of or service to one electrical switchboard. If these air conditioning units are served by a water-side heat rejection system, such as a chilled water or condenser water system, the components of these systems are likewise sized to maintain design conditions, with one electrical switchboard removed from service. This level of redundancy can be obtained by either furnishing two sources of power to each air conditioning unit, or dividing the air conditioning equipment among multiple sources of power. The piping system or systems are dual path, whereby a failure of or maintenance to a section of pipe will not cause interruption of the air conditioning system.

Electrical supply should be provided with alternate Computer Room Air Conditioning (CRAC) units served from separate panels to provide electrical redundancy. All computer room air conditioners (CRAC) units should be backed up by generator power.

Refrigeration equipment with N+1, N+2, 2N, or 2(N+1) redundancy should be dedicated to the data center. Sufficient redundancy should be provided to enable isolation of any item of equipment as required for essential maintenance without affecting the services being provided with cooling.

Subject to the number of Precision Air Conditioners (PAC’s) installed, and consideration of the maintainability and redundancy factors, cooling circuits to the Precision Air Conditioners (PAC's) should be sub-divided. If chilled water or water-cooled systems are used, each data center dedicated sub-circuit should have independent pumps supplied from a central water ring circuit. A water loop should be located at the perimeter of the data center and be located in a sub floor trough to contain water leaks to the trough area. Leak detection sensors should be installed in the trough. Consideration should be given to fully isolated and redundant chilled water loops.

G.6.2.4 Tier 4 (mechanical)

The HVAC system of a tier 4 facility includes multiple air conditioning units with the combined cooling capacity to maintain critical space temperature and relative humidity at design conditions, with sufficient redundant units to allow failure of or service to one electrical switchboard. If these air conditioning units are served by a water-side heat rejection system, such as a chilled water or condenser water system, the components of these systems are likewise sized to maintain design conditions, with one electrical switchboard removed from service. This level of redundancy can be obtained by either furnishing two sources of power to each air conditioning unit, or dividing the air conditioning equipment among multiple sources of power. The piping system or systems are dual path, whereby a failure of or maintenance to a section of pipe will not cause interruption of the air conditioning system. Alternative resources of water storage are to be considered when evaporative systems are in place for a tier 4 system.

Table 8: Tiering reference guide (telecommunications)

	TIER 1	TIER 2	TIER 3	TIER 4
TELECOMMUNICATIONS				
General				
Cabling, racks, cabinets, & pathways meet TIA specs.	yes	yes	yes	yes
Diversely routed access provider entrances and maintenance holes with minimum 20 m separation	no	yes	yes	yes
Redundant access provider services – multiple access providers, central offices, access provider right-of-ways	no	no	yes	yes
Secondary Entrance Room	no	no	yes	yes
Secondary Distribution Area	no	no	no	optional
Redundant Backbone Pathways	no	no	yes	yes
Redundant Horizontal Cabling	no	no	no	optional
Routers and switches have redundant power supplies and processors	no	yes	yes	yes
Multiple routers and switches for redundancy	no	no	yes	yes
Patch panels, outlets, and cabling to be labeled per ANSI/TIA/EIA-606-A and annex B of this Standard. Cabinets and racks to be labeled on front and rear.	yes	yes	yes	yes
Patch cords and jumpers to be labeled on both ends with the name of the connection at both ends of the cable	no	yes	yes	yes
Patch panel and patch cable documentation compliant with ANSI/TIA/EIA-606-A and annex B of this Standard.	no	no	yes	yes

Table 9: Tiering reference guide (architectural)

	TIER 1	TIER 2	TIER 3	TIER 4
ARCHITECTURAL				
Site selection				
Proximity to flood hazard area as mapped on a federal Flood Hazard Boundary or Flood Insurance Rate Map	no requirement	not within flood hazard area	Not within 100-year flood hazard area or less than 91 m / 100 yards from 50-year flood hazard area	Not less the 91 m / 100 yards from 100-year flood hazard area
Proximity to coastal or inland waterways	no requirement	no requirement	Not less than 91 m/ 100 yards	Not less than 0.8 km / 1/2 mile
Proximity to major traffic arteries	no requirement	no requirement	Not less than 91 m / 100 yards	Not less than 0.8 km / 1/2 mile
Proximity to airports	no requirement	no requirement	Not less than 1.6 km / 1 mile or greater than 30 miles	Not less than 8 km / 5 miles or greater than 30 miles
Proximity to major metropolitan area	no requirement	no requirement	Not greater than 48 km / 30 miles	Not greater than 16 km / 10 miles
Parking				
Separate visitor and employee parking areas	no requirement	no requirement	yes (physically separated by fence or wall)	yes (physically separated by fence or wall)
Separate from loading docks	no requirement	no requirement	yes	yes (physically separated by fence or wall)
Proximity of visitor parking to data center perimeter building walls	no requirement	no requirement	9.1 m / 30 ft minimum separation	18.3 m / 60 ft minimum separation with physical barriers to prevent vehicles from driving closer
Multi-tenant occupancy within building	no restriction	Allowed only if occupancies are non-hazardous	Allowed if all tenants are data centers or telecommunications companies	Allowed if all tenants are data centers or telecommunications companies

	TIER 1	TIER 2	TIER 3	TIER 4
Building construction				
Type of construction	no restriction	no restriction	Type II-1hr, III-1hr, or V-1hr	Type I or II-FR
Fire resistive requirements				
Exterior bearing walls	Code allowable	Code allowable	1 Hour minimum	4 Hours minimum
Interior bearing walls	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum
Exterior nonbearing walls	Code allowable	Code allowable	1 Hour minimum	4 Hours minimum
Structural frame	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum
Interior non-computer room partition walls	Code allowable	Code allowable	1 Hour minimum	1 Hour minimum
Interior computer room partition walls	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum
Shaft enclosures	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum
Floors and floor-ceilings	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum
Roofs and roof-ceilings	Code allowable	Code allowable	1 Hour minimum	2 Hour minimum
Meet requirements of NFPA 75	No requirements	yes	yes	yes
Building components				
Vapor barriers for walls and ceiling of computer room	no requirement	yes	yes	yes
Multiple building entrances with security checkpoints	no requirement	no requirement	yes	yes
Floor panel construction	na	no restrictions	All steel	All steel or concrete filled
Understructure	na	no restrictions	bolted stringer	bolted stringer
Ceilings within computer room areas				
Ceiling Construction	no requirement	no requirement	If provided, suspended with clean room tile	Suspended with clean room tile
Ceiling Height	2.6 m (8.5 ft) minimum	2.7 m (9.0 ft) minimum	3 m (10 ft) minimum (not less than 460 m (18 in) above tallest piece of equipment	3 m (10 ft) 'minimum (not less than 600 mm/24 in above tallest piece of equipment)

	TIER 1	TIER 2	TIER 3	TIER 4
Roofing				
Class	no restrictions	Class A	Class A	Class A
Type	no restrictions	no restrictions	non-combustible deck (no mechanically attached systems)	double redundant with concrete deck (no mechanically attached systems)
Wind uplift resistance	Minimum Code requirements	FM I-90	FM I-90 minimum	FM I-120 minimum
Roof Slope	Minimum Code requirements	Minimum Code requirements	1:48 (1/4 in per foot) minimum	1:24 (1/2 in per foot) minimum
Doors and windows				
F Fire rating	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 3/4 hour at computer room)	Minimum Code requirements (not less than 1 1/2 hour at computer room)
Door size	Minimum Code requirements and not less than 1 m (3 ft) wide and 2.13 m (7 ft in) high	Minimum Code requirements and not less than 1 m (3 ft) wide and 2.13 m (7 ft) high	Minimum Code requirements (not less than 1 m (3 ft) wide into computer, electrical, & mechanical rooms) and not less than 2.13 m (7 ft) high	Minimum Code requirements (not less than 1.2 m (4 ft) wide into computer, electrical, & mechanical rooms) and not less than 2.13 m (7 ft) high
Single person interlock, portal or other hardware designed to prevent piggybacking or pass back	Minimum Code requirements	Minimum Code requirements – preferably solid wood with metal frame	Minimum Code requirements – preferably solid wood with metal frame	Minimum Code requirements – preferably solid wood with metal frame
No exterior windows on perimeter of computer room	no requirement	no requirement	yes	yes
Construction provides protection against electromagnetic radiation	no requirement	no requirement	yes	yes
Entry Lobby	no requirement	yes	yes	yes
Physically separate from other areas of data center	no requirement	yes	yes	yes
Fire separation from other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)
Security counter	no requirement	no requirement	yes	yes
Single person interlock, portal or other hardware designed to prevent piggybacking or pass back	no requirement	no requirement	yes	yes

	TIER 1	TIER 2	TIER 3	TIER 4
Administrative offices				
Physically separate from other areas of data center	no requirement	yes	yes	yes
Fire separation from other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)
Security office	no requirement	no requirement	yes	yes
Physically separate from other areas of data center	no requirement	no requirement	yes	yes
Fire separation from other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)
180-degree peepholes on security equipment and monitoring rooms	No requirement	Yes	Yes	yes
Harden security equipment and monitoring rooms with 16 mm (5/8 in) plywood (except where bullet resistance is recommended or required)	No requirement	Recommended	Recommended	Recommended
Dedicated security room for security equipment and monitoring	No requirement	No requirement	Recommended	Recommended
Operations Center	no requirement	no requirement	yes	yes
Physically separate from other areas of data center	no requirement	no requirement	yes	yes
Fire separation from other non-computer room areas of data center	no requirement	no requirement	1 hour	2 hour
Proximity to computer room	no requirement	no requirement	indirectly accessible (maximum of 1 adjoining room)	directly accessible
Restrooms and break room areas	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements
Proximity to computer room and support areas	no requirement	no requirement	If immediately adjacent, provided with leak prevention barrier	Not immediately adjacent and provided with leak prevention barrier
Fire separation from computer room and support areas	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)

	TIER 1	TIER 2	TIER 3	TIER 4
UPS and Battery Rooms				
Aisle widths for maintenance, repair, or equipment removal	no requirement	no requirement	Minimum Code requirements (not less than 1 m (3 ft) clear)	Minimum Code requirements (not less than 1.2 m (4 ft) clear)
Proximity to computer room	no requirement	no requirement	Immediately adjacent	Immediately adjacent
Fire separation from computer room and other areas of data center	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)
Required Exit Corridors				
Fire separation from computer room and support areas	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements (not less than 1 hour)	Minimum Code requirements (not less than 2 hour)
Width	Minimum Code requirements	Minimum Code requirements	Minimum Code requirements and not less than 1.2 m (4 ft) clear	Minimum Code requirements and not less than 1.5 m (5 ft) clear)
Shipping and receiving area	no requirement	yes	yes	yes
Physically separate from other areas of data center	no requirement	yes	yes	yes
Fire separation from other areas of data center	no requirement	no requirement	1 hour	2 hour
Physical protection of walls exposed to lifting equipment traffic	no requirement	no requirement	yes (minimum 3/4 in plywood wainscot)	yes (steel bollards or similar protection)
Number of loading docks	no requirement	1 per 2500 sq m / 25,000 sq ft of Computer room	1 per 2500 sq m / 25,000 sq ft of Computer room (2 minimum)	1 per 2500 sq m / 25,000 sq ft of Computer room (2 minimum)
Loading docks separate from parking areas	no requirement	no requirement	yes	yes (physically separated by fence or wall)
Security counter	no requirement	no requirement	yes	yes (physically separated)
Generator and fuel storage areas				
Proximity to computer room and support areas	no requirement	no requirement	If within Data Center building, provided with minimum 2 hour fire separation from all other areas	Separate building or exterior weatherproof enclosures with Code required building separation
Proximity to publicly accessible areas	no requirement	no requirement	9 m / 30 ft minimum separation	19 m / 60 ft minimum separation

	TIER 1	TIER 2	TIER 3	TIER 4
Security				
System CPU UPS capacity	na	Building	Building	Building + Battery (8 hour min)
Data Gathering Panels (Field Panels) UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)
Field Device UPS Capacity	na	Building + Battery (4 hour min)	Building + Battery (8 hour min)	Building + Battery (24 hour min)
Security staffing per shift	na	1 per 3,000 sq m / 30,000 sq ft (2 minimum)	1 per 2,000 sq m / 20,000 sq ft (3 minimum)	1 per 2,000 sq m / 20,000 sq ft (3 minimum)
Security Access Control/Monitoring at:				
Generators	industrial grade lock	intrusion detection	intrusion detection	intrusion detection
UPS, Telephone & MEP Rooms	industrial grade lock	intrusion detection	card access	card access
Fiber Vaults	industrial grade lock	intrusion detection	intrusion detection	card access
Emergency Exit Doors	industrial grade lock	monitor	delay egress per code	delay egress per code
Accessible Exterior Windows/opening	off site monitoring	intrusion detection	intrusion detection	intrusion detection
Security Operations Center	na	na	card access	card access
Network Operations Center	na	na	card access	card access
Security Equipment Rooms	na	intrusion detection	card access	card access
Doors into Computer Rooms	industrial grade lock	intrusion detection	card or biometric access for ingress and egress	card or biometric access for ingress and egress
Perimeter building doors	off site monitoring	intrusion detection	card access if entrance	card access if entrance
Door from Lobby to Floor	industrial grade lock	card access	Single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential, preferably with biometrics.	single person interlock, portal or other hardware designed to prevent piggybacking or pass back of access credential, preferably with biometrics.
Bullet resistant walls, windows & doors				
Security Counter in Lobby	na	na	Level 3 (min)	Level 3 (min)
Security Counter in Shipping and Receiving	na	na	na	Level 3 (min)

	TIER 1	TIER 2	TIER 3	TIER 4
CCTV Monitoring				
Building perimeter and parking	no requirement	no requirement	yes	yes
Generators	na	na	yes	yes
Access Controlled Doors	no requirement	yes	Yes	Yes
Computer Room Floors	no requirement	no requirement	Yes	Yes
UPS, Telephone & MEP Rooms	no requirement	no requirement	Yes	Yes
CCTV				
CCTV Recording of all activity on all cameras	no requirement	no requirement	Yes; digital	Yes; digital
Recording rate (frames per second)	na	na	20 frames/secs (min)	20 frames/secs (min)
Structural				
Seismic zone -any zone acceptable although it may dictate more costly support mechanisms	no restriction	no restriction	no restriction	no restriction
Facility designed to seismic zone requirements	no restriction	no restriction	no restriction	In Seismic Zone 0, 1, 2 to Zone 3 requirements. In Seismic Zone 3 & 4 to Zone 4 requirements
Site Specific Response Spectra - Degree of local Seismic accelerations	no	no	with Operation Status after 10% in 50 year event	with Operation Status after 5% in 100 year event
Importance factor - assists to ensure greater than code design	I=1	I=1.5	I=1.5	I=1.5
Telecommunications equipment racks/cabinets anchored to base or supported at top and base	no	Base only	Fully braced	Fully braced
Deflection limitation on telecommunications equipment within limits acceptable by the electrical attachments	no	no	yes	yes
Bracing of electrical conduits runs and cable trays	per code	per code w/ Importance	per code w/ Importance	per code w/ Importance
Bracing of mechanical system major duct runs	per code	per code w/ Importance	per code w/ Importance	per code w/ Importance
Floor loading capacity superimposed live load	7.2 kPa (150 lbf/sq ft).	8.4 kPa (175 lbf/sq ft)	12 kPa (250 lbf/sq ft)	12 kPa (250 lbf/sq ft)
Floor hanging capacity for ancillary loads suspended from below	1.2 kPa (25 lbf/sq ft)	1.2 kPa (25 lbf/sq ft)	2.4 kPa (50 lbf/sq ft)	2.4 kPa (50 lbf/sq ft)

	TIER 1	TIER 2	TIER 3	TIER 4
Concrete Slab Thickness at ground	127 mm (5 in)	127 mm (5 in)	127 mm (5 in)	127 mm (5 in)
Concrete topping over flutes for elevated floors affects size of anchor which can be installed	102 mm (4 in)	102 mm (4 in)	102 mm (4 in)	102 mm (4 in)
Building LFRS (Shearwall/Braced Frame/Moment Frame) indicates displacement of structure	Steel/Conc MF	Conc. Shearwall / Steel BF	Conc. Shearwall / Steel BF	Conc. Shearwall / Steel BF
Building Energy Dissipation - Passive Dampers/Base Isolation (energy absorption)	none	none	Passive Dampers	Passive Dampers/Base Isolation
Battery/UPS floor vs. building composition. Concrete floors more difficult to upgrade for intense loads. Steel framing with metal deck and fill much more easily upgraded.	PT concrete	CIP Mild Concrete	Steel Deck & Fill	Steel Deck & Fill
Steel Deck & Fill/ PT concrete/ CIP Mild - PT slabs much more difficult to install anchors	PT concrete	CIP Mild Concrete	Steel Deck & Fill	Steel Deck & Fill

Table 10: Tiering reference guide (electrical)

	TIER 1	TIER 2	TIER 3	TIER 4
ELECTRICAL				
General				
Number of Delivery Paths	1	1	1 active and 1 passive	2 active
Utility Entrance	Single Feed	Single Feed	Dual Feed (600 volts or higher)	Dual Feed (600 volts or higher) from different utility substations
System allows concurrent maintenance	No	No	Yes	Yes
Computer & Telecommunications Equipment Power Cords	Single Cord Feed with 100% capacity	Dual Cord Feed with 100% capacity on each cord	Dual Cord Feed with 100% capacity on each cord	Dual Cord Feed with 100% capacity on each cord
All electrical system equipment labeled with certification from 3rd party test laboratory	Yes	Yes	Yes	Yes
Single Points of Failure	One or more single points of failure for distribution systems serving electrical equipment or mechanical systems	One or more single points of failure for distribution systems serving electrical equipment or mechanical systems	No single points of failure for distribution systems serving electrical equipment or mechanical systems	No single points of failure for distribution systems serving electrical equipment or mechanical systems
Critical Load System Transfer	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic Transfer Switch (ATS) with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.
Site Switchgear	None	None	Fixed air circuit breakers or fixed molded case breakers. Mechanical interlocking of breakers. Any switchgear in distribution system can be shutdown for maintenance with by-passes without dropping the critical load	Drawout air circuit breakers or drawout molded case breakers. Mechanical interlocking of breakers. Any switchgear in distribution system can be shutdown for maintenance with by-passes without dropping the critical load
Generators correctly sized according to installed capacity of UPS	Yes	Yes	Yes	Yes
Generator Fuel Capacity (at full load)	8 hrs (no generator required if UPS has 8 minutes of backup time)	24 hrs	72 hrs	96 hrs

	TIER 1	TIER 2	TIER 3	TIER 4
UPS				
UPS Redundancy	N	N+1	N+1	2N
UPS Topology	Single Module or Parallel Non-Redundant Modules	Parallel Redundant Modules or Distributed Redundant Modules	Parallel Redundant Modules or Distributed Redundant Modules or Block Redundant System	Parallel Redundant Modules or Distributed Redundant Modules or Block Redundant System
UPS Maintenance Bypass Arrangement	By-pass power taken from same utility feeds and UPS modules	By-pass power taken from same utility feeds and UPS modules	By-pass power taken from same utility feeds and UPS modules	By-pass power taken from a reserve UPS system that is powered from a different bus as is used for the UPS system
UPS Power Distribution - voltage level	Voltage Level 120/208V up to loads of 1440 kVA and 480V for loads greater than 1440 kVA	Voltage Level 120/208V up to loads of 1440 kVA and 480V for loads greater than 1440 kVA	Voltage Level 120/208V up to loads of 1440 kVA and 480V for loads greater than 1440 kVA	Voltage Level 120/208V up to loads of 1440 kVA and 480V for loads greater than 1440 kVA
UPS Power Distribution - panel boards	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers
PDUs feed all computer and telecommunications equipment	No	No	Yes	Yes
K-Factor transformers installed in PDUs	Yes, but not required if harmonic canceling transformers are used	Yes, but not required if harmonic canceling transformers are used	Yes, but not required if harmonic canceling transformers are used	Yes, but not required if harmonic canceling transformers are used
Load Bus Synchronization (LBS)	No	No	Yes	Yes
Redundant components (UPS)	Static UPS Design.	Static or Rotary UPS Design. Rotating M-G Set Converters.	Static or Rotary UPS design. Static Converters.	Static, Rotary, or Hybrid UPS Design
UPS on separate distribution panel from computer & telecommunications equipment	No	Yes	Yes	Yes
Grounding				
Lighting protection system	Based on risk analysis as per NFPA 780 and insurance requirements.	Based on risk analysis as per NFPA 780 and insurance requirements.	Yes	Yes
Service entrance grounds and generator grounds fully conform to NEC	Yes	Yes	Yes	Yes
Lighting fixtures (277v) neutral isolated from service entrance derived from lighting transformer for ground fault isolation	Yes	Yes	Yes	Yes
Data center grounding infrastructure in	Not required	Not required	Yes	Yes

computer room				
	TIER 1	**TIER 2**	**TIER 3**	**TIER 4**
Computer Room Emergency Power Off (EPO) System				Yes
Activated by Emergency Power Off (EPO) at exits with computer and telecommunications system shutdown only	Yes	Yes	Yes	Yes
Automatic fire suppressant release after computer and telecommunications system shutdown	Yes	Yes	Yes	Yes
Second zone fire alarm system activation with manual Emergency Power Off (EPO) shutdown	No	No	No	Yes
Master control disconnects batteries and releases suppressant from a 24/7 attended station	No	No	No	Yes
Battery Room Emergency Power Off (EPO) System				
Activated by Emergency Power Off (EPO) buttons at exits with manual suppressant release	Yes	Yes	Yes	Yes
Fire suppressant release for single zone system after Emergency Power Off (EPO) shutdown	Yes	Yes	Yes	Yes
Second zone fire alarm system activation. Disconnects batteries on first zone with suppressant release on the second zone	No	No	Yes	Yes
Master control disconnects batteries and releases suppressant from a 24/7 attended station	No	No	Yes	Yes
Emergency Power Off (EPO) Systems				
Shutdown of UPS power receptacles in computer room area.	Yes	Yes	Yes	Yes
Shutdown of AC power for CRACs and chillers	Yes	Yes	Yes	Yes
Compliance with local code (e.g. separate systems for UPS and HVAC)	Yes	Yes	Yes	Yes

	TIER 1	TIER 2	TIER 3	TIER 4
System Monitoring				
Locally Displayed at UPS	Yes	Yes	Yes	Yes
Central power and environmental monitoring and control system (PEMCS) with remote engineering console and manual overrides for all automatic controls and set points	No	No	Yes	Yes
Interface with BMS	No	No	Yes	Yes
Remote Control	No	No	No	Yes
Automatic Text Messaging to Service Engineer's Pager	No	No	No	Yes
Battery Configuration				
Common Battery String for All Modules	Yes	No	No	No
One Battery String per Module	No	Yes	Yes	Yes
Minimum Full Load Standby Time	5 minutes	10 Minutes	15 minutes	15 minutes
Battery type	Valve regulated lead acid (VRLA) or flooded type	Valve regulated lead acid (VRLA) or flooded type	Valve regulated lead acid (VRLA) or flooded type	Valve regulated lead acid (VRLA) or flooded type
Flooded Type Batteries				
Mounting	Racks or cabinets	Racks or cabinets	Open racks	Open racks
Wrapped Plates	No	Yes	Yes	Yes
Acid Spill Containment Installed	Yes	Yes	Yes	Yes
Battery Full Load Testing/Inspection Schedule	Every two years	Every two years	Every two years	Every two years or annually
Battery Room				
Separate from UPS/Switchgear Equipment Rooms	No	Yes	Yes	Yes
Individual Battery Strings Isolated from Each Other	No	Yes	Yes	Yes
Shatterproof Viewing Glass in Battery Room Door	No	No	No	Yes
Battery Disconnects Located Outside Battery Room	Yes	Yes	Yes	Yes
Battery Monitoring System	UPS self monitoring	UPS self monitoring	UPS self monitoring	Centralized automated system to check each cell for temperature, voltage, and impedance

	TIER 1	TIER 2	TIER 3	TIER 4
Rotating UPS System Enclosures (With Diesel Generators)				
Units Separately Enclosed by Fire Rated Walls	No	No	Yes	Yes
Fuel Tanks on Exterior	No	No	Yes	Yes
Fuel Tanks in Same Room as Units	Yes	Yes	No	No
Standby Generating System				
Generator Sizing	Sized for computer & telecommunications system electrical & mechanical only	Sized for computer & telecommunications system electrical & mechanical only	Sized for computer & telecommunications system electrical & mechanical only + 1 spare	Total Building Load + 1 Spare
Generators on Single Bus	Yes	Yes	Yes	No
Single Generator per System with (1) Spare Generator	No	Yes	Yes	Yes
Individual 83 ft. Ground Fault Protection for Each Generator	No	Yes	Yes	Yes
Loadbank for Testing				
Testing UPS modules only	Yes	Yes	Yes	No
Testing of Generators only	Yes	Yes	Yes	No
Testing of Both UPS modules and generators	No	No	No	Yes
UPS Switchgear	No	No	No	Yes
Permanently Installed	No - Rental	No - Rental	No - Rental	Yes
Equipment Maintenance				
Maintenance Staff	Onsite Day Shift only. On-call at other times	Onsite Day Shift only. On-call at other times	Onsite 24 hrs M-F, on-call on weekends	Onsite 24/7
Preventative Maintenance	None	None	Limited preventative maintenance program	Comprehensive preventative maintenance program
Facility Training Programs	None	None	Comprehensive training program	Comprehensive training program including manual operation procedures if it is necessary to bypass control system

Table 11: Tiering reference guide (mechanical)

	TIER 1	TIER 2	TIER 3	TIER 4
MECHANICAL				
General				
Routing of water or drain piping not associated with the data center equipment in data center spaces	Permitted but not recommended	Permitted but not recommended	Not permitted	Not permitted
Positive pressure in computer room and associated spaces relative to outdoors and non-data center spaces	No requirement	Yes	Yes	Yes
Floor drains in computer room for condensate drain water, humidifier flush water, and sprinkler discharge water	Yes	Yes	Yes	Yes
Mechanical systems on standby generator	No requirement	Yes	Yes	Yes
Water-Cooled System				
Indoor Terminal Air Conditioning Units	No redundant air conditioning units	One redundant AC Unit per critical area	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power
Humidity Control for Computer Room	Humidification provided	Humidification provided	Humidification provided	Humidification provided
Electrical Service to Mechanical Equipment	Single path of electrical power to AC equipment	Single path of electrical power to AC equipment	Multiple paths of electrical power to AC equipment. Connected in checkerboard fashion for cooling redundancy	Multiple paths of electrical power to AC equipment. Connected in checkerboard fashion for cooling redundancy
Heat Rejection				
Dry-coolers (where applicable)	No redundant dry coolers	One redundant dry cooler per system	Qty. of dry coolers sufficient to maintain critical area during loss of one source of electrical power	Qty. of dry coolers sufficient to maintain critical area during loss of one source of electrical power
Closed-Circuit Fluid Coolers (where applicable)	No redundant fluid coolers	One redundant fluid cooler per system	Qty. of fluid coolers sufficient to maintain critical area during loss of one source of electrical power	Qty. of fluid coolers sufficient to maintain critical area during loss of one source of electrical power
Circulating Pumps	No redundant condenser water pumps	One redundant condenser water pump per system	Qty. of condenser water pumps sufficient to maintain critical area during loss of one source of electrical power	Qty. of condenser water pumps sufficient to maintain critical area during loss of one source of electrical power
Piping System	Single path condenser water system	Single path condenser water system	Dual path condenser water system	Dual path condenser water system

	TIER 1	TIER 2	TIER 3	TIER 4
Chilled Water System				
Indoor Terminal Air Conditioning Units	No redundant air conditioning units	One redundant AC Unit per critical area	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power
Humidity Control for Computer Room	Humidification provided	Humidification provided	Humidification provided	Humidification provided
Electrical Service to Mechanical Equipment	Single path of electrical power to AC equipment	Single path of electrical power to AC equipment	Multiple paths of electrical power to AC equipment	Multiple paths of electrical power to AC equipment
Heat Rejection				
Chilled Water Piping System	Single path chilled water system	Single path chilled water system	Dual path chilled water system	Dual path chilled water system
Chilled Water Pumps	No redundant chilled water pumps	One redundant chilled water pump per system	Qty. of chilled water pumps sufficient to maintain critical area during loss of one source of electrical power	Qty. of chilled water pumps sufficient to maintain critical area during loss of one source of electrical power
Air-Cooled Chillers	No redundant chiller	One redundant chiller per system	Qty. of chilled water pumps sufficient to maintain critical area during loss of one source of electrical power	Qty. of chillers sufficient to maintain critical area during loss of one source of electrical power
Water-cooled Chillers	No redundant chiller	One redundant chiller per system	Qty. of chillers sufficient to maintain critical area during loss of one source of electrical power	Qty. of chillers sufficient to maintain critical area during loss of one source of electrical power
Cooling Towers	No redundant cooling tower	One redundant cooling tower per system	Qty. of cooling towers sufficient to maintain critical area during loss of one source of electrical power	Qty. of cooling towers sufficient to maintain critical area during loss of one source of electrical power
Condenser Water Pumps	No redundant condenser water pumps	One redundant condenser water pump per system	Qty. of condenser water pumps sufficient to maintain critical area during loss of one source of electrical power	Qty. of condenser water pumps sufficient to maintain critical area during loss of one source of electrical power
Condenser Water Piping System	Single path condenser water system	Single path condenser water system	Dual path condenser water system	Dual path condenser water system

	TIER 1	TIER 2	TIER 3	TIER 4
Air-Cooled System				
Indoor Terminal Air Conditioning Units/Outdoor Condensers	No redundant air conditioning units	One redundant AC Unit per critical area	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power	Qty. of AC Units sufficient to maintain critical area during loss of one source of electrical power
Electrical Service to Mechanical Equipment	Single path of electrical power to AC equipment	Single path of electrical power to AC equipment	Multiple paths of electrical power to AC equipment	Multiple paths of electrical power to AC equipment
Humidity Control for Computer Room	Humidification provided	Humidification provided	Humidification provided	Humidification provided
HVAC Control System				
HVAC Control System	Control system failure will interrupt cooling to critical areas	Control system failure will not interrupt cooling to critical areas	Control system failure will not interrupt cooling to critical areas	Control system failure will not interrupt cooling to critical areas
Power Source to HVAC Control System	Single path of electrical power to HVAC control system	Redundant, UPS electrical power to AC equipment	Redundant, UPS electrical power to AC equipment	Redundant, UPS electrical power to AC equipment
Plumbing (for water-cooled heat rejection)				
Dual Sources of Make-up Water	Single water supply, with no on-site back-up storage	Dual sources of water, or one source + on-site storage	Dual sources of water, or one source + on-site storage	Dual sources of water, or one source + on-site storage
Points of Connection to Condenser Water System	Single point of connection	Single point of connection	Two points of connection	Two points of connection
Fuel Oil System				
Bulk Storage Tanks	Single storage tank	Multiple storage tanks	Multiple storage tanks	Multiple storage tanks
Storage Tank Pumps and Piping	Single pump and/or supply pipe	Multiple pumps, multiple supply pipes	Multiple pumps, multiple supply pipes	Multiple pumps, multiple supply pipes
Fire Suppression				
Fire detection system	no	yes	yes	yes
Fire sprinkler system	When required	Pre-action (when required)	Pre-action (when required)	Pre-action (when required)
Gaseous suppression system	no	no	clean agents listed in NFPA 2001	clean agents listed in NFPA 2001
Early Warning Smoke Detection System	no	yes	yes	yes
Water Leak Detection System	no	yes	yes	yes

[This page is intentionally left blank]

ANNEX H (INFORMATIVE) DATA CENTER DESIGN EXAMPLES

This annex is informative only and is not part of this Standard.

H.1 Small data center design example

One example layout for a small data center is shown below. This is an example of a data center that is small enough to be supported by a main distribution area and no horizontal distribution areas.

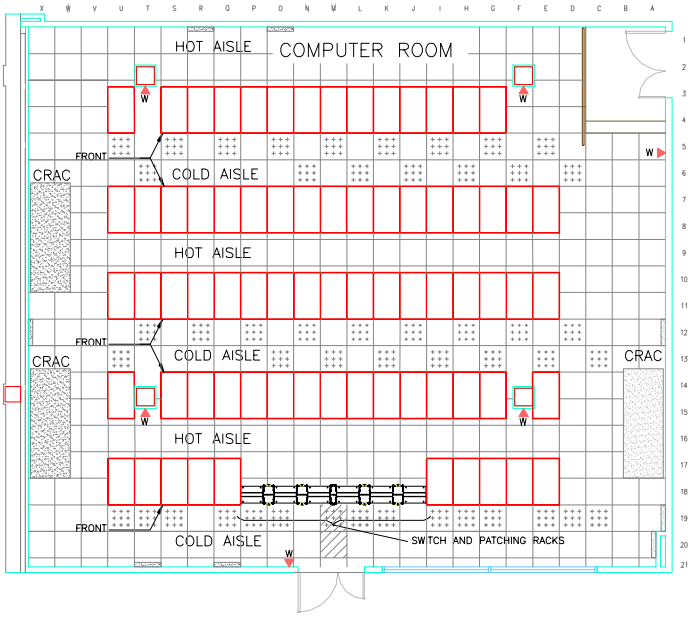


Figure 20: Computer room layout showing “hot” and “cold” aisles

This computer room space is about 1,920 square feet. It has 73 server cabinets in the equipment distribution areas (EDAs) and six 19” racks in the main distribution area (MDA). The six MDA racks are the six ‘SWITCH AND PATCHING RACKS’ at the bottom of the drawing. It was not necessary to put the MDA in the center of the computer room because distance limitations were not an issue. However, cable lengths and cable congestion in the aisles perpendicular to the cabinet aisles could have been reduced by placing the MDA in the center of the room instead.

The MDA supports the HC for horizontal cabling to the EDAs. In a data center with a high density of cabling to the equipment cabinets, it would probably be necessary to have horizontal distribution areas (HDAs) to minimize cable congestion near the MDA.

The rack and cabinet rows are parallel to the direction of under floor airflow created by the Computer Room Air Conditioning (CRAC) units. Each CRAC is located facing the “hot” aisles to allow more efficient return air to each CRAC unit.

Server cabinets are arranged to form alternating “hot” and “cold” aisles

Communications cables are run in wire trays (baskets) in the “hot” aisle area. Power cables are run under the access floor in the “cold” aisles.

The computer room is separate from the Network Operations Center (NOC is not shown) for access and contaminant control.

H.2 Corporate data center design example

The following example is for an internet or web hosting data center used to house computer and telecommunications equipment for multiple corporate web sites.

The corporate data center in this example has two floors of about 4,140 sq m (44,500 sq ft) each. This data center is an example of a data center with several horizontal distribution areas, each differentiated primarily by the type of systems that they support. Due to the density of cabling to the personal computer based servers, these systems are served by two horizontal distribution areas (HDAs), each supporting only 24 server cabinets. Seven additional horizontal distribution areas are planned to support additional server cabinets. Thus, horizontal distribution areas may be required not only for different functional areas, but also to minimize cable congestion in the HDA. Each HDA was designed to support a maximum of 2,000 4-pair category 6 cables.

The 1st floor includes the electrical rooms, mechanical rooms, storage rooms, loading dock, security room, reception area, operations center, and entrance room.

The computer room is on the 2nd floor and is entirely on access floor. All telecommunications cabling is run under the access floor space in wire-basket cable trays. In some locations where the volume of cables is the greatest and where they do not impede airflow, the cable trays are installed in two layers. The drawing below shows the 2nd floor computer room with cable trays.

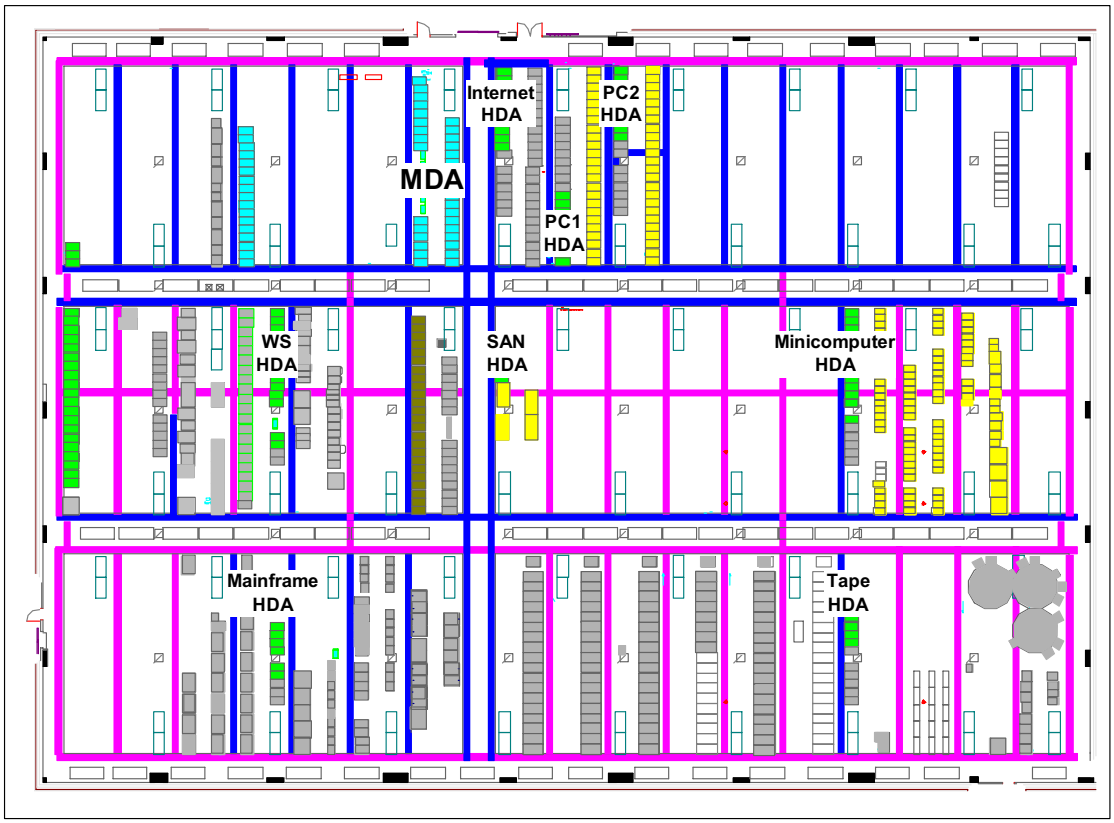


Figure 21: Example for corporate data center

Telecommunications cabling is installed in the “hot” aisles behind the server cabinets. Electrical cabling is installed in the “cold” aisles in front of the server cabinets. Both telecommunications cabling and electrical cabling follow the main aisles in the east/west direction, but follow separate pathways to maintain separation of power and telecommunications cabling.

The locations of the Entrance Room on the 1st floor and MDA on the 2nd floor are carefully positioned so that T-1 and T-3 circuits can be terminated on equipment anywhere in the computer room.

Cabinets for rack-mounted servers have standardized cabling that includes multimode fiber and category 6 UTP. Administration is somewhat simplified if cabinets have a standard cabling configuration.

In this data center, due to the very wide variety of cabling requirements for floor standing systems, it was not possible to develop a standardized configuration for zone outlets.

H.3 Internet data center design example

The internet data center in this example has one floor of approximately 9,500 sq m (102,000 sq ft) with a computer room of about 6400 sq m (69,000 sq ft). It is an example of a data center where horizontal distribution areas are differentiated primarily by the area served rather than the type of systems that they support. The drawing below shows the data center floor plan with cable trays. MDA and HDA racks are shown but customer racks and cabinets are not.

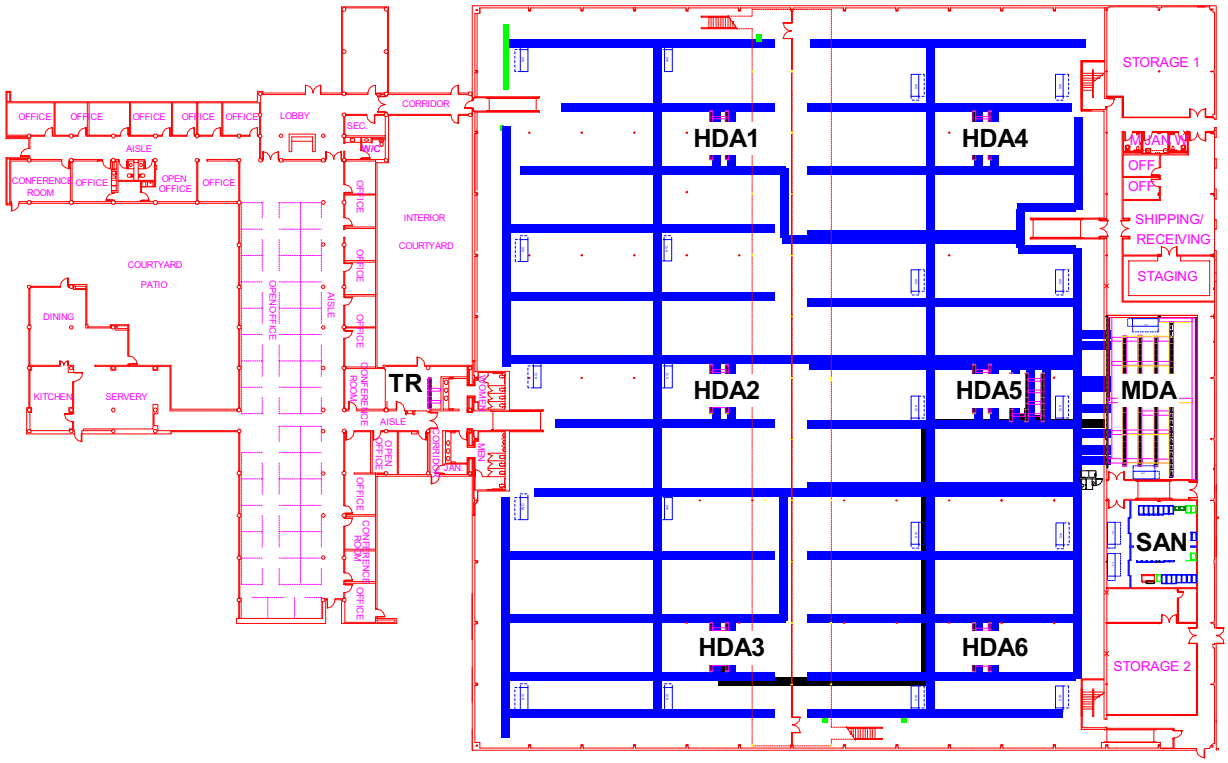


Figure 22: Example for internet data center

The main distribution area (MDA) incorporates the function of the entrance room and the main cross-connect. It accommodates 50 access provider racks and 20 racks for the main cross-connect space. This room is supported by two dedicated PDUs, two dedicated computer room air conditioning units, and is on access floor. The MDA is in a dedicated room with a separate entrance that allows access and service providers to work in this room without entering the customer spaces in the main computer room. The locations of the MDA and HDAs were planned to ensure that circuit lengths for T-1 and T-3 circuits will not be exceeded for circuits to any rack in the computer room.

Automated tape libraries, storage servers, and control equipment for storage services are in a dedicated SAN room adjacent to the MDA. This equipment is provided and managed by third parties, not by the owner of the internet data center. A separate room for this equipment allows storage service providers to manage their equipment without entering the main computer room.

The computer room space has 4,300 customer racks. The customer space is supported by six horizontal distribution areas (HDAs) to limit the volume of cable in the underfloor cable trays. Each HDA supports approximately 2,000 copper-pair connections. These HDAs are in the center of the spaces they serve to minimize cable lengths. Cabling from the HDAs to the customer racks is standardized to simplify administration. However, additional cabling may be run to customer racks as required.

Telecommunications cabling to storage and staging areas east of the computer room are supported from the MDA. Telecommunications cabling for the offices west of the computer room are supported by a telecommunications room (TR).

ANNEX I (INFORMATIVE) BIBLIOGRAPHY AND REFERENCES

This annex is informative only and is not part of this Standard.

This annex contains information on the documents that are related to or have been referenced in this document. Many of the documents are in print and are distributed and maintained by national or international standards organizations. These documents can be obtained through contact with the associated standards body or designated representatives. The applicable electrical code in the United States is the National Electrical Code.

- ANSI/IEEE C2-1997, *National Electrical Safety Code*
- ANSI/NFPA 70-2002, *National Electrical Code*
- ANSI/NFPA 75-2003*, Standard for the protection of information technology equipment*
- ANSI T1.336*, Engineering requirements for a universal telecommunications frame.*
- ANSI/TIA/EIA-568-B.1-2001, *Commercial Building Telecommunications Cabling Standard*
- ANSI/TIA/EIA-568-B.2-2001, *Commercial Building Telecommunications Cabling Standard: Part 2: Balanced Twisted-Pair Cabling Components*.
- ANSI/TIA/EIA-568-B.3-2000, *Optical Fiber Cabling Components*
- ANSI/TIA-569-A-1998, *Commercial Building Standard for Telecommunications Pathways and Spaces*
- ANSI/TIA/EIA-606-A-2002, *Administration Standard for the Telecommunications Infrastructure of Commercial Buildings*
- ANSI/TIA/EIA-J-STD-607-2001, *Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications*
- ANSI/TIA-758-1999, *Customer-owned Outside Plant Telecommunications Cabling Standard*
- ASHRAE, *Thermal Guidelines for Data Processing Environments*
- ASTM B539-90, *Measuring Contact Resistance of Electrical Connections (Static Contacts)*
- BICSI *Telecommunications Distribution Methods Manual*
- BICSI *Cabling Installation Manual*
- BICSI *Customer-owned Outside Plant Methods Manual*
- BOMA – *Building Owners Management Association, International – Codes & Issues, July 2000*
- CABA - *Continental Automated Buildings Association*,
- Federal Communications Commission (FCC) Washington D.C., "*The Code of Federal Regulations, FCC 47 CFR 68"*
- Federal Telecommunications Recommendation 1090-1997*, Commercial Building Telecommunications Cabling Standard,* by National Communications System (NCS)

- IBC, *International Building Code*
- ICC, *International Code Council*
- IEEE Std. 142, *Recommended Practice for Grounding of Industrial and Commercial Power Systems*
- IEEE Std. 446, *Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*
- IEEE Std. 1100, *Recommended Practice for Powering and Grounding Electronic Equipment*
- IEEE 802.3-2002 (also known as ANSI/IEEE Std 802.3-2002 or ISO 8802-3: 2002 (E), *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*
- IEEE 802.4-1990, *Standard for Local Area Network Token Passing Bus Access Method, Physical Layer Specification*
- IEEE 802.5-1998, *Token Ring Access Method and Physical Layer Specifications*
- IEEE 802.7-1989 (R1997) *IEEE Recommended Practices for Broadband Local Area Networks (ANSI)*
- IEEE Standard 518-1982, *Guide for the installation of electrical equipment to minimize electrical noise to controllers of external sources*
- IFMA – *International Facility Management Association - Ergonomics for Facility Managers*, June 2000
- NFPA 72,*National Fire Alarm Code, 1999*
- NFPA 2001, *Standard on clean agent fire extinguishing systems, 2000 Edition*
- NEC, *National Electrical Code, article 725, Class 1, Class 2 and Class 3 Remote-Control, Signaling and Power-Limited Circuits*.
- NEC, *National Electrical Code, article 760, Fire Alarm System*.
- NEMA VE 2-2001, *cable tray installation guidelines*
- *Society of Cable Television Engineers, Inc., Document #IPS-SP-001, Flexible RF Coaxial Drop cable Specification*
- TIA/EIA TSB-31-B, FCC 47 CFR 68, *Rationale and Measurement Guidelines*
- ANSI/TIA/EIA-485-A-1998, *Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems*
- TIA/EIA-TSB89-1998, *Application Guidelines for TIA/EIA-485-A*
- UL 444/CSA-C22.2 No. 214-94, *Communications Cables*
- The Uptime Institute White Paper, *Alternating Cold and Hot Aisles Provides More Reliable Cooling for Server Farms*
- The Uptime Institute White Paper, *Industry Standard Tier Classifications Define Site Infrastructure Performance*

- The Uptime Institute White Paper, *Fault-Tolerant Power Compliance Specification*

The organizations listed below can be contacted to obtain reference information.

ANSI
American National Standards Institute (ANSI)
11 W 42 St.
New York, NY 10032
USA
(212) 642-4900
www.ansi.org

American Society of Heating, Refrigeration and Air conditioning Engineers (ASHRAE)
1791 Tullie Circle, NE
Atlanta, GA 30329
1-800-527-4723
(404) 636-8400
www.ashrae.org

ASTM
American Society for Testing and Materials (ASTM)
100 Barr Harbor Drive
West Conshohocken, PA 19428-2959
USA
(610) 832-9500
www.astm.org

BICSI
Building Industry Consulting Service International (BICSI)
8610 Hidden River Parkway
Tampa, FL 33637-1000
USA
(800) 242-7405
www.bicsi.org

CSA
Canadian Standards Association International (CSA)
178 Rexdale Blvd.
Etobicoke, (Toronto), Ontario
Canada M9W 1R3
(416) 747-4000
www.csa-international.org

EIA
Electronic Industries Alliance (EIA)
2500 Wilson Blvd., Suite 400
Arlington, VA 22201-3836
USA
(703) 907-7500
www.eia.org

FCC
Federal Communications Commission (FCC)
Washington, DC 20554
USA
(301) 725-1585
www.fcc.org

Federal and Military Specifications
National Communications System (NCS)
Technology and Standards Division
701 South Court House Road Arlington, VA 22204-2198
USA
(703) 607-6200
www.ncs.gov

International Code Council (ICC)
International Building Code (IBC)
5203 Leesburg Pike, Suite 600
Falls Church, VA 22041
703-931-4533
www.iccsafe.org

IEC
International Electrotechnical Commission (IEC)
Sales Department
PO Box 131
3 rue de Varembe
1211 Geneva 20
Switzerland
+41 22 919 02 11
www.iec.ch

IEEE
The Institute of Electrical and Electronic Engineers, Inc (IEEE)
IEEE Service Center
445 Hoes Ln., PO Box 1331
Piscataway, NJ 08855-1331
USA
(732) 981-0060
www.ieee.org

IPC
The Institute for Interconnecting and Packaging Electronic Circuits
2215 Sanders Rd.
Northbrook, IL 60062-6135
USA
(847) 509-9700
www.ipc.org

ISO
International Organization for Standardization (ISO)
1, Rue de Varembe
Case Postale 56
CH-1211 Geneva 20
Switzerland
+41 22 74 901 11
www.iso.ch

NEMA
National Electrical Manufacturers Association (NEMA)
1300 N. 17th Street, Suite 1847
Rosslyn, VA 22209
USA
(703) 841-3200
www.nema.org

NFPA
National Fire Protection Association (NFPA)
Batterymarch Park
Quincy, MA 02269-9101
USA
(617) 770-3000
www.nfpa.org

SCTE
Society of Cable Telecommunications Engineers (SCTE)
140 Philips Rd.
Exton, PA 19341-1318
USA
(800) 542-5040
www.scte.org

TIA-942

Telcordia Technologies (formerly; Bellcore)
Telcordia Technologies Customer Service
8 Corporate Place Room 3C-183
Piscataway, NJ 08854-4157
USA
(800) 521-2673
www.telcordia.com

The Uptime Institute, Inc.
1347 Tano Ridge Road
Santa Fe, NM 87506
USA
(505) 986-3900
www.upsite.com

TIA
Telecommunications Industry Association (TIA)
2500 Wilson Blvd., Suite 300
Arlington, VA 22201-3836
USA
(703) 907-7700
www.tiaonline.org

UL
Underwriters Laboratories, Inc. (UL)
333 Pfingsten Road
Northbrook, IL 60062-2096
USA
(847) 272-8800
www.ul.com

ANEXO B.

Estudio de factibilidad de sistema de detección y extinción de incendios.

Durante el desarrollo del proyecto se presento la propuesta de implementación de un sistema de extinción de incendios con agentes limpios que no producen daño a los equipos ni al personal, en vista de una falta de aprobación de presupuesto no se ha realizado la implementación pero queda constancia del estudio para una posterior instalación, a continuación el resumen del estudio realizado por una empresa proveedora para dicha implementación.

ECARO-25 Flow Calculation Software Version 4.00.0000

Fike Corporation UL Ex4623, FM 3014476

Licensed to Richard Puig, Fike Corporation Results Printed on 7/14/2011

Project Name: Data Center - 3 x 5.5 x 2.2m

Project Designer: Richard Puig -Fike

Project Location: Quito, Ecuador

Project Account:

Project Description:

Project Filename: C:\Documents and Settings\richard.puig\My Documents\~Fike\Project Files\Fike

PROJECT INFORMATION

ECARO-25 Flow Calculation\Farmaenlace DataCenter Ecuador.125

CUSTOMER INFORMATION

Nozzle Number	*Type*	*Enclosure Name*	*Requested Agent*
0101	180°	Ambiente Principal y Unico	11.5 kg

Company Name: Farmaenlace

Company Address: FARMAENLACE Cia. Ltda. Av. Cap Rafael Ramos E2-120 y Castelli

Quito,

Ecuador

Company Phone: (593-2) 2993100 Company Fax: Contact Information: Marco Ramirez F

Redes y Telecomunicaciones Telf: (593-2)-2993100 Ext 1630

Agent Requirements - Enclosure 0001 (Ambiente Principal y Unico)

Nozzle Information - Pipe Network 0001 (Pipe Network 0001)

Total Agent Distributed Through Pipe Network: 11.5 kg

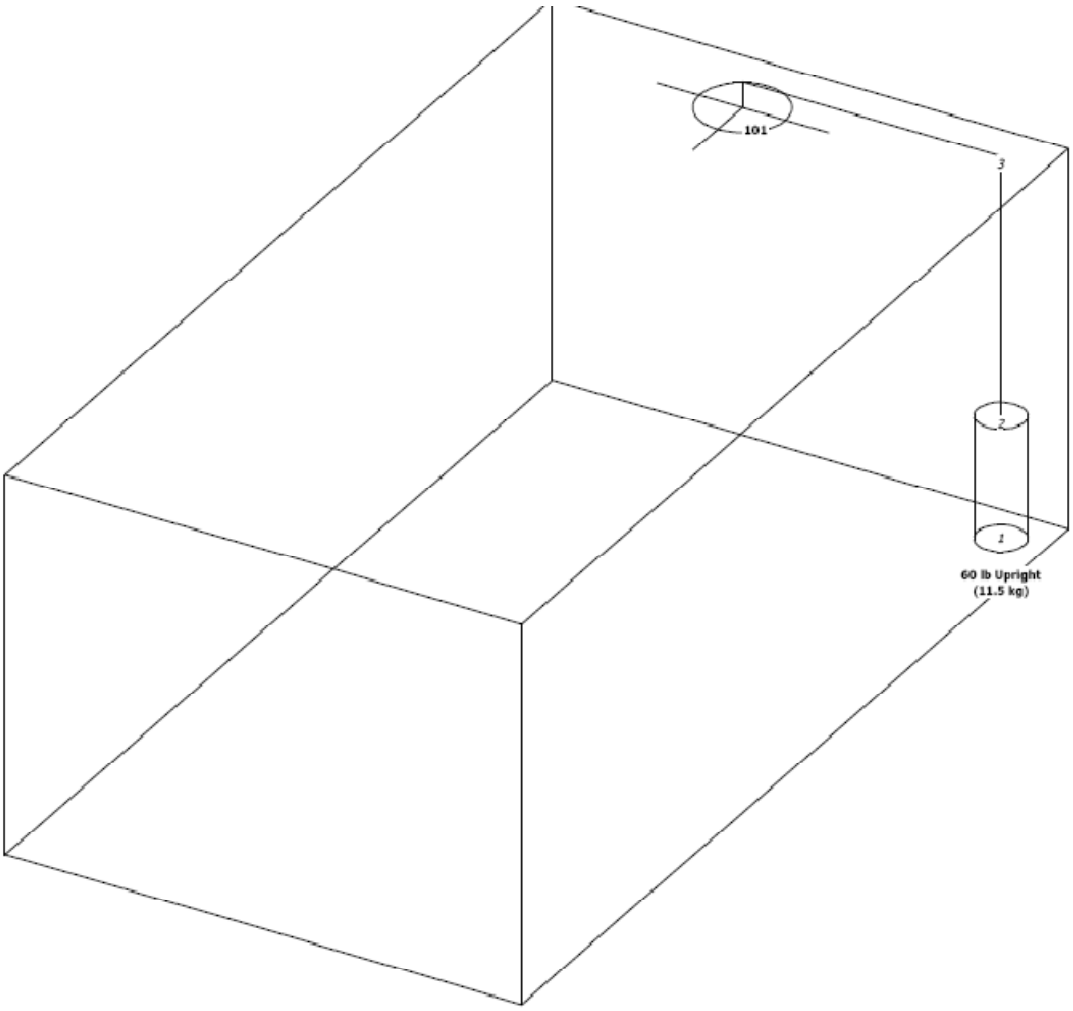
Enclosure Area		*Enclosure Height*	*Volume Added*	*Volume Subtracted*	*Protected Volume*
16.50 m²		2.20 m	None	None	36.30 m³
Design Concentration	*Maximum Concentration*	*Minimum Temperature*	*Maximum Temperature*	*Elevation*	*Agent Required*
8.00 %	8.01 % at 21 °C	21 °C	21 °C	2700 m	11.5 kg

Cylinder Information - Pipe Network 0001 (Pipe Network 0001)

Cylinder Type	*Agent Per Cylinder*	*Manifold Type*	*Cylinder Spacing*	*Valve to Manifold*	*Cylinder to Exit*
70-265 60 lb Upright	1 X 11.5 kg	No Manifold	-	-	-

Fill Density	*Empty Weight*	*Floor Area*	*Floor Loading*
417.0 kg / m³	24 kg	0.06 m²	683 kg / m²

Pipe Network Isometric



Flow Calculation Input Data - Pipe Network 0001 (Pipe Network 0001)

Start	End	Length	Elevation	Select Pipe Dia	Select Pipe Sch	90°	Thru	Side	Union	Equ Length	Cyl	Nozz Type	Select Agent	Select Orifice
1	2	0.71 m	0.71 m	25 mm	SCH 40 T					1.13 m	1			
2	3	1.50 m	1.50 m	15 mm	SCH 40 T									
3	101	1.65 m	-0.15 m	15 mm	SCH 40 T	2						180	11.5 kg	0.1200 in

Flow Calculation Output Data - Pipe Network 0001 (Pipe Network 0001)

Start	End	Pipe Type	Equ Length	Start Pressure	End Pressure	Flow Rate	Agent Discharged	Orifice Diameter
1	2	25 mm -SCH 40	1.84 m	2158 kPa	2151 kPa	1.1 kg/s		
2	3	15 mm -SCH 40	1.50 m	2151 kPa	2089 kPa	1.1 kg/s		
3	101	15 mm -SCH 40	2.60 m	2089 kPa	2027 kPa	1.1 kg/s	11.5 kg	0.1200 in

Flow Calculation Messages
ECARO-25 Flow Calculation Software Version 4.00.0000
Calculation based on fixed nozzle codes and pipe sizes.
Calculation performed on 7/14/2011 1:51:48 PM
System calculated within limits of Fikes UL listing and FM approval

Qty	Part Number	Cylinder Description	Agent Fill Amount
1	70-265	60 lb Upright	11.5 kg

Bill of Materials - Pipe Network 0001 (Pipe Network 0001)

Num	Part Number	Nozzle Size	Nozzle Type	Drill Diameter
101	80-045-1200	15 mm -SCH 40	180°	0.1200 in

Cylinder List

Nozzle List

Section	*Pipe Length*	*Pipe Type*
1 - 2	0.71 m	25 mm -SCH 40
2 - 3	1.50 m	15 mm -SCH 40
3 - 101	1.65 m	15 mm -SCH 40

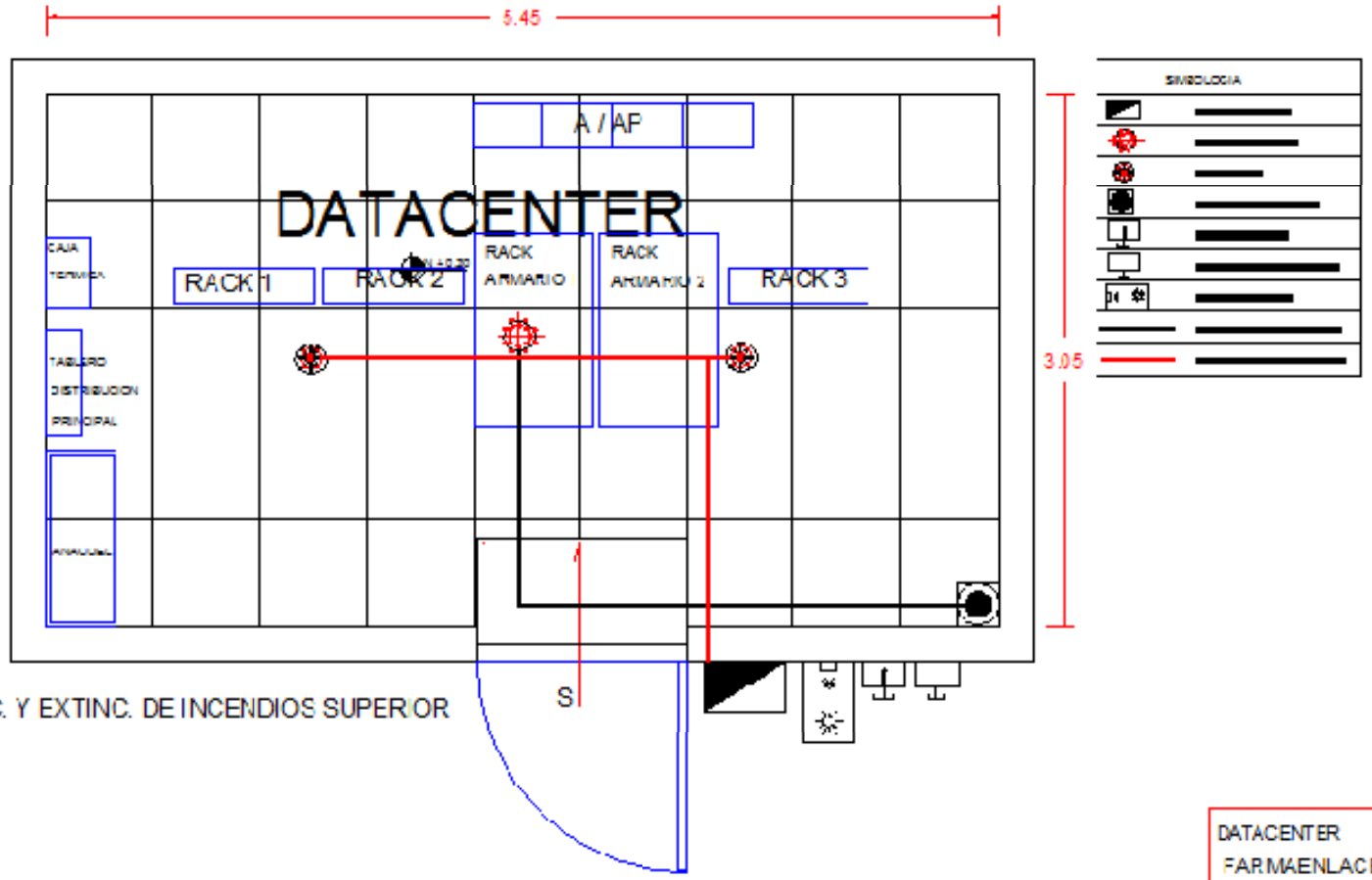
Pipe Network	*Discharge Time*	*%Agent in Pipe Network*	*Pipe Temperature*
0001 - Pipe Network 0001	9.03 s	8.95%	21 °C

Pipe List

System Acceptance Report

Pipe Network Discharge Time

Enclosure 0001 (Ambiente Principal y Unico) - Nozzle Performance

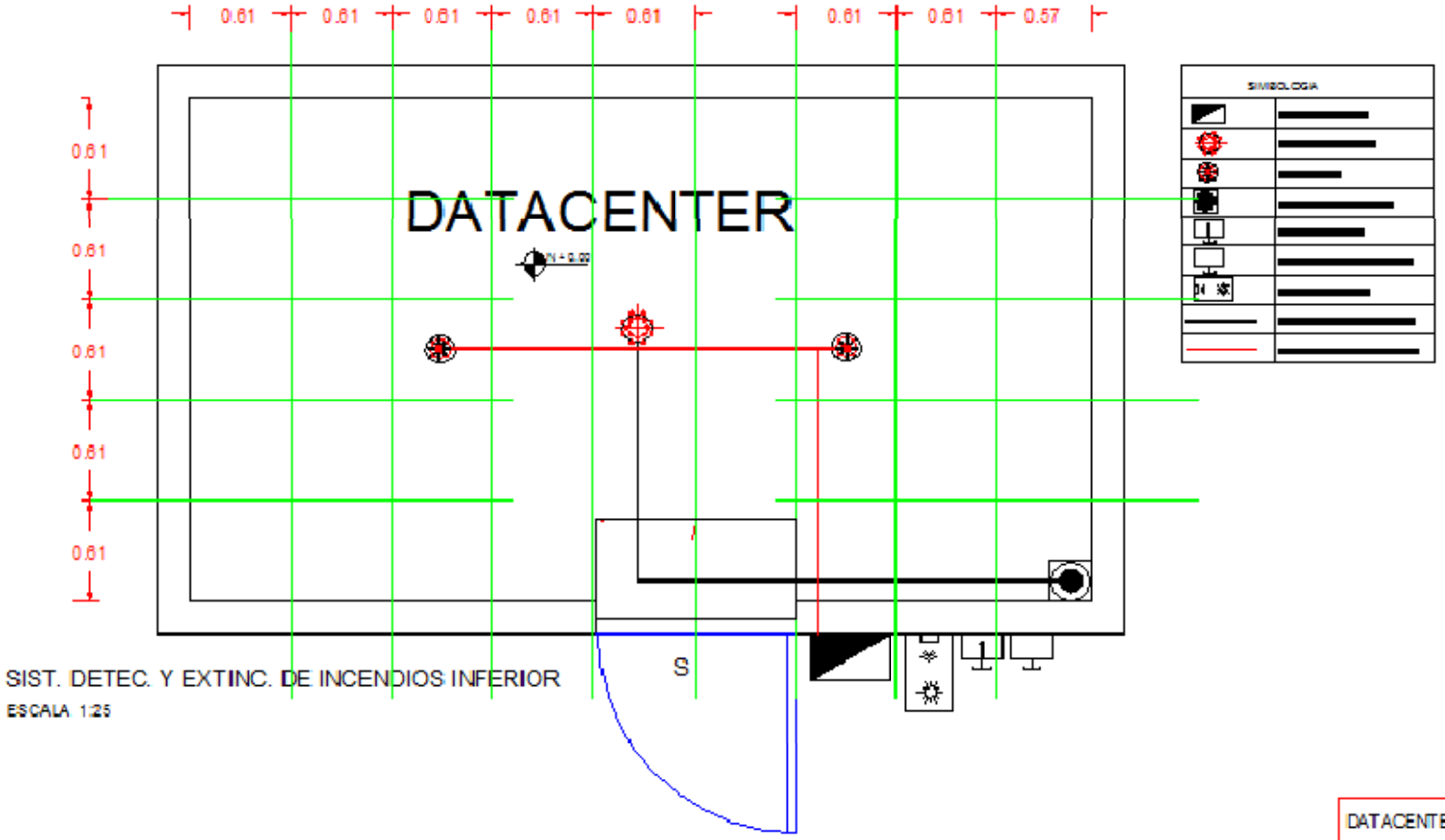


SIST. DETEC. Y EXTINC. DE INCENDIOS SUPERIOR

ESCALA 1:25

DATACENTER
FARMAENLACE CIA. LTDA.

DC-7



SIST. DETEC. Y EXTINC. DE INCENDIOS INFERIOR

ESCALA 1:25

DATACENTER
FARMAENLACE CIA. LTDA.

DC-8

ANEXO C

Archivos de Configuración de Switches 3COM

A continuación se presentara el contenido de los archivos de configuración de un switch 3COM 5500 y un switch 3COM 4500, equipos utilizados en la red LAN de Farmaenlace.

CONFIGURACION DE SWITCH 3COM 5500

DATOS GENERALES

sysname 5500G-EI

undo password-control aging enable

undo password-control length enable

undo password-control history enable

password-control login-attempt 3 exceed lock-time 120

local-server nas-ip 127.0.0.1 key 3com

igmp-snooping enable

radius scheme system

domain system

local-user admin

password simple admin

service-type lan-access

service-type telnet terminal

level 3

service-type ftp

local-user manager

password simple manager

service-type telnet terminal

level 2

local-user monitor

password simple monitor

service-type telnet terminal

level 1

acl number 3997

rule 0 permit ip dscp ef

rule 1 permit tcp destination-port eq www

rule 2 permit udp destination-port eq snmp

rule 3 permit udp destination-port eq snmptrap

rule 4 permit ip dscp cs6

rule 5 permit ip dscp cs7

acl number 4999

rule 0 permit type 8868 ffff

rule 1 permit source 00e0-bb00-0000 ffff-ff00-0000

rule 2 permit source 0003-6b00-0000 ffff-ff00-0000

rule 3 permit source 00e0-7500-0000 ffff-ff00-0000

rule 4 permit source 00d0-1e00-0000 ffff-ff00-0000

rule 5 permit source 0001-e300-0000 ffff-ff00-0000

rule 6 permit source 000f-e200-0000 ffff-ff00-0000

rule 7 permit source 0060-b900-0000 ffff-ff00-0000

rule 8 deny dest 0000-0000-0000 ffff-ffff-ffff

qos-profile default

packet-filter inbound link-group 4999 rule 8

traffic-priority inbound ip-group 3997 rule 0 cos voice

traffic-priority inbound ip-group 3997 rule 4 cos network-management

traffic-priority inbound ip-group 3997 rule 5 cos network-management

traffic-priority inbound link-group 4999 rule 0 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 1 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 2 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 3 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 4 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 5 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 6 dscp ef cos voice
traffic-priority inbound link-group 4999 rule 7 dscp ef cos voice

CONFIGURACION DE VLANs

vlan 1
igmp-snooping enable
vlan 2
vlan 3
vlan 300

interface Vlan-interface1
description RED FARMA DATOS
ip address 192.168.238.245 255.255.255.0
rip version 2 multicast

interface Vlan-interface2
description RED TELEFONIA
ip address 192.168.110.1 255.255.255.0
rip version 2 multicast

interface Vlan-interface3
description RED DATOS MediMagda
ip address 192.168.101.253 255.255.255.0

rip version 2 multicast

CONFIGURACION DE PUERTOS

interface Aux1/0/0

interface GigabitEthernet1/0/1
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/2
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/3
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

```
interface GigabitEthernet1/0/4
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/5
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/6
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/7
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
```

```
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/8
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/9
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/10
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/11
 stp edged-port enable
```

```
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/12
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/13
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/14
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default
```

```
interface GigabitEthernet1/0/15
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/16
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/17
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/18
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
```

```
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/19
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/20
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 1 to 2 untagged
 port hybrid pvid vlan 2
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/21
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 1 to 2 untagged
 port hybrid pvid vlan 2
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default
```

```
interface GigabitEthernet1/0/22
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 1 to 2 untagged
 port hybrid pvid vlan 2
 broadcast-suppression pps 3000
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/23
 stp edged-port enable
 duplex full
 speed 10
 port link-type hybrid
 port hybrid vlan 1 to 2 tagged
 port hybrid vlan 3 untagged
 broadcast-suppression pps 3000
 port isolate
 description chassis remoto
 apply qos-profile default

interface GigabitEthernet1/0/24
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 300
 undo jumboframe enable
 description enlace a magda
 apply qos-profile default
```

```
interface GigabitEthernet1/0/25
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/26
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 broadcast-suppression pps 3000
 shutdown
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/0/27
 stp edged-port enable
 duplex full
 speed 10
 port link-type hybrid
 port hybrid vlan 1 to 2 tagged
 port hybrid vlan 3 untagged
 broadcast-suppression pps 3000
 shutdown
 port isolate
```

```
 apply qos-profile default

interface GigabitEthernet1/0/28
 stp edged-port enable
 broadcast-suppression pps 3000
 shutdown
 port access vlan 300
 undo jumboframe enable
 apply qos-profile default

interface GigabitEthernet1/1/1
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/2
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/3
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/4
```

```
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/5
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/6
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/7
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default

interface GigabitEthernet1/1/8
 stp edged-port enable
 port link-type trunk
 port trunk permit vlan all
 apply qos-profile default
```

interface Cascade1/2/1

interface Cascade1/2/2

interface NULL

CONFIGURACION DE RUTEO

rip

network 192.168.101.0

network 192.168.102.0

network 192.168.103.0

network 192.168.104.0

network 192.168.105.0

network 192.168.238.0

network 192.168.100.0

import-route static

import-route direct

ip route-static 0.0.0.0 0.0.0.0 192.168.238.254 preference 60

ip route-static 10.100.1.0 255.255.255.0 192.168.238.239 preference 60

ip route-static 172.30.0.0 255.255.0.0 192.168.238.1 preference 60

ip route-static 192.168.103.30 255.255.255.255 192.168.238.238 preference 60

ip route-static 192.168.104.100 255.255.255.255 192.168.238.238 preference 60

ip route-static 192.168.105.20 255.255.255.255 192.168.238.238 preference 60

CONFIGURACIÓN SWITCH 3COM 4500

DATOS GENERALES

```
sysname RecMercaderia
 undo password-control aging enable
 undo password-control length enable
 undo password-control history enable
 password-control login-attempt 3 exceed lock-time 120
local-server nas-ip 127.0.0.1 key 3com
igmp-snooping enable
radius scheme system
domain system
local-user admin
 service-type lan-access
 service-type ssh telnet terminal
 level 3
local-user manager
 password simple manager
 service-type ssh telnet terminal
 level 2
local-user monitor
 password simple monitor
 service-type ssh telnet terminal
 level 1
acl number 4999
```

rule 0 deny dest 0000-0000-0000 ffff-ffff-ffff

CONFIGURACION DE VLAN’s

vlan 1

igmp-snooping enable

vlan 2 to 3

vlan 300

interface Vlan-interface1

ip address 192.168.238.242 255.255.255.0

rip version 2 multicast

interface Vlan-interface2

rip version 2 multicast

interface Vlan-interface3

rip version 2 multicast

interface Vlan-interface3

rip version 2 multicast

CONFIGURACION INTERFACES

interface Aux1/0/0

interface Ethernet1/0/1

stp edged-port enable

port link-type hybrid

port hybrid vlan 2 tagged

port hybrid vlan 1 3 untagged

broadcast-suppression pps 3000

packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/2

stp edged-port enable

port link-type hybrid

port hybrid vlan 2 tagged

port hybrid vlan 1 3 untagged

broadcast-suppression pps 3000

packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/3

stp edged-port enable

port link-type hybrid

```
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/4
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/5
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/6
```

```
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged

interface Ethernet1/0/5
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/6
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/7
```

```
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/8
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/9
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0
```

```
interface Ethernet1/0/10
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/11
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/12
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
```

```
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/13
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/14
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/15
 stp edged-port enable
 port link-type hybrid
```

```
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/16
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/17
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/18
```

```
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/19
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/20
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0
```

```
interface Ethernet1/0/21
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged

interface Ethernet1/0/22
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/23
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0
```

```
interface Ethernet1/0/24
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/25
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/26
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
```

```
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/27
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/28
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/29
 stp edged-port enable
 port link-type hybrid
```

```
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/30
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/31
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/32
```

```
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/33
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/34
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0
```

```
interface Ethernet1/0/35
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/36
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged

interface Ethernet1/0/36
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0
```

```
interface Ethernet1/0/37
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/38
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/39
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
```

```
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/40
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/41
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/42
 stp edged-port enable
 port link-type hybrid
```

```
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/43
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/44
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/45
```

```
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/46
 stp edged-port enable
 port link-type hybrid
 port hybrid vlan 2 tagged
 port hybrid vlan 1 3 untagged
 broadcast-suppression pps 3000
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/47
 stp edged-port enable
 broadcast-suppression pps 3000
 port access vlan 300
 packet-filter inbound link-group 4999 rule 0

interface Ethernet1/0/48
```

stp edged-port enable

port link-type trunk

port trunk permit vlan all

broadcast-suppression pps 3000

packet-filter inbound link-group 4999 rule 0

interface GigabitEthernet1/0/49

interface GigabitEthernet1/0/50

interface GigabitEthernet1/0/51

shutdown

interface GigabitEthernet1/0/52

shutdown

undo xrn-fabric authentication-mode

interface NULL0

RUTEO

rip

network 192.168.238.0

network 192.168.101.0

network 192.168.110.0

ip route-static 0.0.0.0 0.0.0.0 192.168.238.245 preference 60

DATOS ADICIONALES

snmp-agent

snmp-agent local-engineid 8000002B20FDF184F5406877

snmp-agent community read public

snmp-agent community write private

snmp-agent sys-info version all

user-interface aux 0 7

authentication-mode scheme

screen-length 22

user-interface vty 0 4

authentication-mode scheme

return

Listado de Enlaces FARMAENLACE CIA LTDA

Nº	Direccion Red		ENLACE	OFICINA
1	192.168.0.0/24 (IP10)	0	Matriz Quito Easy Soft	
2	192.168.2.0/24		Eco Calle Sucre	002
3	192.168.3.0/24		DATAFAST	
4	192.168.4.0/24		Eco Machachi	004
5	192.168.5.0/24		Medi Av. América	005
6	192.168.6.0/24		Medi El Ejido	006
7	192.168.7.0/24		Medi Estadio Olímpico	007
8	192.168.8.0/24		Medi Pomasqui	008
9	192.168.9.0/24		Eco Maldonado Ambato	009
10	192.168.10.0/24		Medi La Prensa	010
11	192.168.11.0/24		Eco Carcelén	011
12	192.168.12.0/24		Difarmes Ambato	003
13	192.168.13.0/24		Medi Eloy Alfaro	013
14	192.168.14.0/24		Medi PUCE	514
15	192.168.15.0/24		Medi San Rafael	515
16	192.168.16.0/24		Eco Rodrigo de Chavez	161
17	192.168.17.0/24		Eco Conocoto	017
18	192.168.18.0/24		Eco 5 Esquinas	018
19	192.168.19.0/24		Enmascaramiento EASYSOFT - Rodrigo de Chavez	018
20	192.168.20.0/24		Eco Atacames	020
21	192.168.21.0/24		Eco Villaflora	021
22	192.168.22.0/24		Medi La Y	522
23	192.168.23.0/24		Medi Republica	523
24	192.168.24.0/24		Medi Shyris	510
25	192.168.25.0/24		Eco La Mena	25
26	192.168.26.0/24		Eco 29 de Mayo	926
27	192.168.27.0/24		Eco Av. Quito	927
28	192.168.28.0/24		Eco Andinatel Otavalo	028
29	192.168.29.0/24		Eco Cruz Roja Otavalo	029
30	192.168.30.0/24		Medi Indoamerica	030
31	192.168.31.0/24		Eco Central Cayambe	031
32	192.168.32.0/24		Eco La Union	032
33	192.168.33.0/24		Eco La Estación	033
34	192.168.34.0/24		Eco La Merced	034
35	192.168.35.0/24		Zermat	035
36	192.168.36.0/24		Eco Olmedo Siglo XXI	036
37	192.168.37.0/24		Eco Restauración	037
38	192.168.38.0/24		Eco La Concordia	038
39	192.168.39.0/24		Eco Pío XII	039
40	192.168.40.0/24		Eco Sacha	040
41	192.168.41.0/24		Eco Llano Grande	
42	192.168.42.0/24		Eco Parque Sucre	042
43	192.168.43.0/24		Eco Calle Guayaquil	043
44	192.168.44.0/24		Eco la J	044
45	192.168.45.0/24		Eco Parque Maldonado	045
46	192.168.46.0/24		PAF Más Distribuidora	046
47	192.168.47.0/24		Eco Quininde Uno	047

48	**192.168.48.0/24**		**Eco Sto. Dom. Calle Guayaquil**	048
49	**192.168.49.0/24**		**Eco Las Lomas**	049
50	**192.168.50.0/24**		**Eco Sánchez y Cifuentes**	050
51	**192.168.51.0/24**		**Eco El Recreo**	051
52	**192.168.52.0/24**		**Eco Hosp. Quinindé**	052
53	**192.168.53.0/24**		**Eco Quinindé Dos**	053
54	**192.168.54.0/24**		**Medi Mariana de Jesus**	054
55	**192.168.55.0/24**		**Eco Cotocollao**	955
56	**192.168.56.0/24**		**Eco Coca**	056
57	**192.168.57.0/24**		**Medi Calle Rocafuerte**	057
58	**192.168.58.0/24**		**Medi Parq. Cent. Cayambe**	058
59	**192.168.59.0/24**		**Eco Central San Gabriel**	059
60	**192.168.60.0/24**		**Eco Merc. Princ. Ambato**	060
61	**192.168.61.0/24**		**Servicio de DataFast**	060
62	**192.168.62.0/24**		**Eco San Gabriel**	062
63	**192.168.63.0/24**		**Eco San Francisco**	063
64	**192.168.64.0/24**		**Eco Copacabana**	064
65	**192.168.65.0/24**		**Medi Interoceánica**	065
66	**192.168.66.0/24**		**Medi Real Audiencia**	066
67	**192.168.67.0/24**		**PAF Difarime**	067
68	**192.168.68.0/24**		**Medi Central Tumbaco**	068
69	**192.168.69.0/24**		**Eco Clínica Pichincha**	069
70	**192.168.70.0/24**		**Eco Carapungo**	070
71	**192.168.71.0/24**		**Eco Bolivar**	071
72	**192.168.72.0/24**		**Eco Libertad**	072
73	**192.168.73.0/24**		**Medi Clínica Especialidades**	073
74	**192.168.74.0/24**		**Eco Quinindé Tres**	074
75	**192.168.75.0/24**		**Eco Cevallos**	075
76	**192.168.76.0/24**		**Eco El Cisne**	076
77	**192.168.77.0/24**		**Eco Hosp. San Vicente**	077
78	**192.168.78.0/24**		**Eco Sudamericana**	078
79	**192.168.79.0/24**		**Eco Santa Monica**	079
80	**192.168.80.0/24**		**Eco París**	080
81	**192.168.81.0/24**		**Eco Hosp. Andrade Marín**	081
82	**192.168.82.0/24**		**Medi Hosp. Andrade Marín**	082
83	**192.168.83.0/24**		**Eco San Luis**	083
84	**192.168.84.0/24**		**PAF Santa Clara**	084
85	**192.168.85.0/24**		**Difarmes Mañosca**	085
86	**192.168.86.0/24**		**Eco El Inca**	086
87	**192.168.87.0/24**		**Eco Republica Dominicana**	087
88	**192.168.88.0/24**		**Eco Carabobo**	088
89	**192.168.89.0/24**		**Eco Colón Esmeraldas**	089
90	**192.168.90.0/24**		**Eco México**	090
91	**192.168.91.0/24**		**Medi Brasil**	091
92	**192.168.93.0/24**		**HMO**	093
93	**192.168.94.0/24**		**HMO**	094
94	**192.168.95.0/24**		**Eco Venezuela**	095
95	**192.168.96.0/24**		**Medi San Carlos - Esmeraldas**	096
96	**192.168.97.0/24**		**Eco Merc. Mod. Ambato**	097
97	**192.168.98.0/24**		**Medi San Marino**	098
98	**192.168.99.0/24**		**Eco Central Cumbaya**	099

99	**192.168.100.0/24**		**Eco El Conde**	100
100	**192.168.101.0/24**		**Medi Magda La Luz**	101
101	**192.168.102.0/24**		**Medi Magda Venezuela**	353
102	**192.168.103.0/24**		**Medi Magada El Ejido**	363
103	**192.168.104.0/24**		**Medi Magda River Mall**	368
104	**192.168.105.0/24**		**Medi Magda Carapungo**	373
105	**192.168.106.0/24**		**Eco 12 de Noviembre**	106
106	**192.168.107.0/24**		**Eco Casa Rosada**	107
107	**192.168.108.0/24**		**Eco Veintimilla Tulcan**	108
108	**192.168.109.0/24**		**Eco Lago Agrio**	109
109	**192.168.110.0/24**		**Telefonía IP - Matriz**	110
110	**192.168.111.0/24**		**Eco Patronato Sur**	111
111	**192.168.112.0/24**		**Eco Sabanilla (Ofelia)**	112
112	**192.168.113.0/24**		**Eco El Retorno**	113
113	**192.168.114.0/24**		**Eco Clinica Ibarra**	114
114	**192.168.115.0/24**		**Eco Florida**	115
115	**192.168.116.0/24**		**Medi Amazonas**	116
116	**192.168.117.0/24**		**Eco Biloxi**	117
117	**192.168.118.0/24**		**Eco Comité del Pueblo**	118
118	**192.168.119.0/24**		**Eco Pedernales**	119
119	**192.168.120.0/24**		**Difarmes Sur**	120
120	**192.168.121.0/24**		**Eco La Concordia Dos**	121
121	**192.168.122.0/24**		**Eco Olmedo Ibarra**	122
122	**192.168.123.0/24**		**Eco La Castellana**	123
123	**192.168.124.0/24**		**Eco Atahualpa**	124
124	**192.168.125.0/24**		**Eco Huachichico**	125
125	**192.168.126.0/24**		**Eco Mariano Acosta**	126
126	**192.168.127.0/24**		**Medi El Bosque**	127
127	**192.168.128.0/24**		**Medi Plaza Tumbaco**	128
128	**192.168.129.0/24**		**Eco Sacha Dos**	129
129	**192.168.130.0/24**		**Eco La Mirage**	130
130	**192.168.131.0/24**		**Medi Playa Chica**	131
131	**192.168.132.0/24**		**Eco Industrial**	132
132	**192.168.133.0/24**		**Medi Santa Barbara**	133
133	**192.168.134.0/24**		**Medi Granados**	134
134	**192.168.135.0/24**		**Eco Chimborazo**	135
135	**192.168.136.0/24**		**Eco America**	136
136	**192.168.137.0/24**		**Eco Hospital del IESS Norte**	137
137	**192.168.138.0/24**		**Medi Ficoa**	138
138	**192.168.139.0/24**		**Eco Gonzales Suarez**	139
139	**192.168.140.0/24**		**Eco Universal**	140
140	**192.168.141.0/24**		**Medi Italia**	141
141	**192.168.142.0/24**		**PAF Fátima**	142
142	**192.168.143.0/24**		**Quicentro Sur**	143
143	**192.168.144.0/24**		**PAF San Andrés**	144
144	**192.168.145.0/24**		**Eco 9 de Octubre**	145
145	**192.168.146.0/24**		**Eco Santa Clara**	146
146	**192.168.147.0/24**		**Eco Las Américas 2**	147
147	**192.168.148.0/24**		**Eco La Salud**	148
148	**192.168.149.0/24**		**Eco Eloy Alfaro**	149
149	**192.168.150.0/24**		**Medi La Granja**	150

150	**192.168.151.0/24**		**Eco Kenia**	151
151	**192.168.152.0/24**		**Eco San Cayetano**	152
152	**192.168.153.0/24**		**Eco su Farmacia**	153
153	**192.168.154.0/24**		**Eco San Miguel**	154
154	**192.168.155.0/24**		**Eco Pelileo**	155
155	**192.168.156.0/24**		**Eco Vaca de Castro**	156
156	**192.168.157.0/24**		**Eco Alejandro**	157
157	**192.168.158.0/24**		**Eco Mi Farmacia El Carmen**	158
158	**192.168.159.0/24**		**Medi Granda Centeno**	159
159	**192.168.160.0/24**		**MEDI PLAZA**	160
160	**192.168.161.0/24**		**Eco Tierra Nueva**	061
161	**192.168.162.0/24**		**Eco La Magdalena**	162
162	**192.168.163.0/24**		**Medi Miravalle**	163
163	**192.168.164.0/24**		**Eco Turubamba**	164
164	**192.168.165.0/24**		**Sylvana 1**	165
165	**192.168.166.0/24**		**Eco Mariscal Sucre**	166
166	**192.168.167.0/24**		**Sylvana 2**	167
167	**192.168.168.0/24**		**Sylvana 4**	168
168	**192.168.169.0/24**		**Eco Rex**	169
169	**192.168.170.0/24**		**Sylvana 3**	170
170	**192.168.171.0/24**		**Paf La Merced Ibarra**	171
171	**192.168.172.0/24**		**PAF La Dolorosa Cayambe**	172
172	**192.168.173.0/24**		**Medi Gonzalez Suarez**	173
173	**192.168.174.0/24**		**ECO - Las Casas**	174
174	**192.168.175.0/24**		**ECO El Batan**	175
175	**192.168.176.0/24**		**ECO Tena**	176
176	**192.168.177.0/24**		**ECO San Lorenzo**	177
177	**192.168.178.0/24**		**ECO Shushufindi**	178
178	**192.168.179.0/24**			179
179	**192.168.182.0/24**		**ECO DE LAS AMERICAS**	784
180	**192.168.181.0/24**		**ECO Jaime Roldos**	181
181	**192.168.184.0/24**		**MEDI Cumbaya**	
182	**192.168.185.0/24**		**Eco La Castellana**	101
183	**192.168.186.0/24**		**PAF Nacional - El Carmen**	
184	**192.168.187.0/24**		**ECO Inglesa III**	
185	**192.168.189.0/24**		**ECO Catedral**	
186	**192.168.190.0/24**		**ECO Santa Marianita**	
187	**192.168.191.0/24**		**ECO Atacames II**	
188	**192.168.192.0/24**		**ECO Parque Infantil**	
189	**192.168.193.0/24**		**ECO El Salvador**	
190	**192.168.194.0/24**		**PAF Yaruqui**	
191	**192.168.195.0/24**		**ECO Siglo XXI Ambato**	
192	**192.168.196.0/24**		**PAF El Carmen -Ibarra**	
193	**192.168.197.0/24**		**ECO - Vida Sana**	
194	**192.168.198.0/24**		**PAF Calderón**	
195	**192.168.199.0/24**		**ECO - Real Audiencia**	
196	**192.168.200.0/24**		**PAF Corazón de Jesús**	
197	**192.168.201.0/24**		**Eco Michelena**	102
198	**192.168.202.0/24**		**Eco Merc. Prin. Tulcán**	103
199	**192.168.203.0/24**		**Eco Obelisco**	509
200	**192.168.204.0/24**		**PAF Nandy**	

201	**192.168.206.0/24**		**ECO Principal Sto. Dom.**	110
202	**192.168.207.0/24**		**ECO - Duque**	
203	**192.168.208.0/24**		**MEDI La Pampa**	208
204	**192.168.209.0/24**		**MEDI El Condado**	209
205	**192.168.210.0/24**		**Eco 3 de Julio**	
206	**192.168.211.0/24**		**Eco Obispo Mosquera**	211
207	**192.168.212.0/24**		**Medi Plaza de Toros**	212
208	**192.168.213.0/24**		**Eco Ramon Borja**	
209	**192.168.214.0/24**		**MEDI Coruña**	214
210	**192.168.215.0/24**		**PAF Sagrado Corazón III**	
211	**192.168.216.0/24**		**PAF Sagrado Corazón II**	
212	**192.168.217.0/24**		**ECO Vargas Torres**	
213	**192.168.218.0/24**			218
214	**192.168.219.0/24**		**ECO Puruhá**	219
215	**192.168.220.0/24**		**MEDI Los Chillos**	220
216	**192.168.221.0/24**		**Eco Socorrito Sacha**	221
217	**192.168.222.0/24**		**PAF Sagrado Corazón I - Quininde**	222
218	**192.168.223.0/24**		**ECO Coca II**	223
219	**192.168.224.0/24**		**ECO Los Libertadores**	224
220	**192.168.225.0/24**		**ECO La Marín**	225
221	**192.168.226.0/24**		**ECO Dylan**	226
222	**192.168.227.0/24**		**PAF Medi Salud**	227
223	**192.168.228.0/24**		**ECO San Carlos**	228
224	**192.168.229.0/24**		**ECO Junín (Metropolitana)**	229
225	**192.168.230.0/24**		**PAF Descuento Calderón II**	230
226	**192.168.231.0/24**		**ECO Mucho Lote B**	231
227	**192.168.232.0/24**		**ECO Pascuales**	232
228	**192.168.233.0/24**		**PAF EL Quinche**	233
229	**192.168.234.0/24**		**ECO Cómite del Pueblo II**	234
230	**192.168.235.0/24**		**ECO Casuarina**	235
231	**192.168.236.0/24**		**ECO Sangolquí**	236
232	**192.168.237.0/24**		**Oficinas Ibarra**	237
233	**192.168.238.0/24**		**Servidores Matriz UIO**	238
234	**192.168.239.0/24**		**Telefonía IP - Ibarra**	239
235	**192.168.240.0/24**		**ECO Playas**	240
236	**192.168.241.0/24**		**ECO Urdesa Centro**	241
237	**192.168.242.0/24**		**ECO Atarazana**	242
238	**192.168.243.0/24**		**MEDI Blue Coast**	243
239	**192.168.244.0/24**		**MEDI Lumbisi**	244
240	**192.168.246.0/24**		**ECO Martha Roldos**	246
241	**192.168.247.0/24**		**ECO Pillaro**	247
242	**192.168.248.0/24**		**ECO Mayorista Sucre**	248
243	**192.168.249.0/24**		**ECO Las Acacias**	249
244	**192.168.250.0/24**		**ECO Martha Bucaram**	250
245	**192.168.251.0/24**		**MEDI Puerto Azul**	251
246	**192.168.252.0/24**		**ECO Carapungo II**	252
247	**192.168.253.0/24**		**ECO San Eduardo**	253
248	**192.168.254.0/24**		**MEDI Plaza Tumbaco**	254

ANEXO E

Listado de Politicas GPO de Active Directory

Default Domain Policy

Datos recopilados en: 05/09/2011
14:32:42

General

Detalles

Dominio	farmaenlace.com
Propietario	FARMAENLACE0\Admins. del dominio
Creado	21/01/2008 22:59:36
Modificado	06/07/2011 8:22:26
Revisiones de usuario	84 (AD), 83 (sysvol)
Revisiones de equipo	101 (AD), 101 (sysvol)
Id. Único	{31B2F340-016D-11D2-945F-00C04FB984F9}
Estado de GPO	Habilitado

Vínculos

Ubicación	Forzada	Estado de vínculo	Ruta
Farmaenlace	Sí	Habilitado	farmaenlace.com

Esta lista sólo incluye vínculos en el dominio del GPO

Filtrado de seguridad

La configuración en este GPO sólo se puede aplicar a los grupos, usuarios y equipos siguientes:

Nombre
NT AUTHORITY\Usuarios autentificados

Filtrado WMI

Nombre de filtro WMI	Ninguno
Descripción	No aplicable

Delegación

Estos grupos y usuarios tienen los permisos especificados para este GPO

Nombre	Permisos	Heredado
FARMAENLACE0\Administradores de organización	Editar configuración, eliminar, modificar seguridad	No
FARMAENLACE0\Admins. del dominio	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Lectura	No
NT AUTHORITY\SYSTEM	Editar configuración, eliminar, modificar seguridad	No
NT AUTHORITY\Usuarios autentificados	Lectura (de Filtrado de seguridad)	No

Configuración del equipo (habilitada)

Configuración de Windows

Configuración de seguridad

Directivas de cuenta/Directiva de contraseñas

Directiva	Configuración
Almacenar contraseñas usando cifrado reversible	Deshabilitado
Forzar el historial de contraseñas	3 contraseñas recordadas
Las contraseñas deben cumplir los requerimientos de complejidad	Deshabilitado
Longitud mínima de la contraseña	7 caracteres
Vigencia máxima de la contraseña	90 días
Vigencia mínima de la contraseña	1 días

Directivas de cuenta/Directiva de bloqueo de cuentas

Directiva	Configuración

Duración del bloqueo de cuenta	1 minutos
Restablecer la cuenta de bloqueos luego de	1 minutos
Umbral de bloqueos de la cuenta	999 intentos de inicio de sesión no válidos

Directivas de cuenta /Directiva Kerberos

Directiva	**Configuración**
Edad máxima de renovación de tíquets de usuario	7 días
Forzar restricciones de inicio de sesión de usuario	Habilitado
Tolerancia máxima para la sincronización de los relojes de los equipos	5 minutos
Vigencia máxima del vale de servicio	600 minutos
Vigencia máxima del vale de usuario	10 horas

Directivas locales/Directiva de auditoría

Directiva	**Configuración**
Auditar sucesos de inicio de sesión	Correcto, erróneo
Auditar sucesos de inicio de sesión de cuenta	Correcto, erróneo

Directivas locales/Asignación de derechos de usuario

Directiva	**Configuración**
Change the system time	FARMAENLACE0\Sistemas

Directivas locales/Opciones de seguridad

Seguridad de redmostrar

Directiva	**Configuración**
Seguridad de red: forzar el cierre de sesión cuando expire la hora de inicio de sesión	Deshabilitado

Directivas de claves públicas/Configuración de inscripción automática

Directiva	**Configuración**
Registrar certificados automáticamente	Habilitado
Renovar certificados caducados, actualizar certificados pendientes y quitar certificados revocados	Deshabilitado

Actualizar certificados que usan plantillas de certificados	Deshabilitado

Directivas de claves públicas/Sistema de archivos de cifrado

Propiedades

Directiva	Configuración
Permitir a usuarios cifrar archivos utilizando el Sistema de archivos cifrados (EFS)	Habilitado

Certificados

Emitido para	Emitido por	Fecha de caducidad	Propósitos planteados
Administrador	Administrador	20/01/2011 23:14:44	Recuperación de archivos

Para obtener información adicional sobre configuraciones individuales, inicie el Editor de Objeto de directiva de grupo.

Directivas de claves públicas/Entidades emisoras raíz de confianza

Propiedades

Directiva	Configuración
Permitir a los usuarios seleccionar nuevas entidades emisoras de certificados raíz de confianza	Habilitado
Los equipos cliente pueden confiar en los siguientes almacenes de certificados	Entidades emisoras de certificados raíz de terceros y entidades emisoras de certificados raíz de empresa
Para realizar la autenticación de usuarios y equipos basada en certificados, las entidades emisoras de certificados deben cumplir los siguientes criterios	Sólo los registrados en Active Directory

Plantillas administrativas

Componentes de Windows/Terminal Services

Directiva	Configuración
Permitir que los usuarios se conecten de forma remota utilizando Servicios de Terminal Server	Habilitado

Sistema

Directiva	Configuración

Desactivar reproducción automática	Habilitado

Desactivar reproducción automática en:	Todas las unidades

Configuración de usuario (habilitada)

Configuración de

Servicios de instalación

Opciones de Asistente para instalación de

Directiva	**Configuración**
Herramientas	Deshabilitado
Personalizar la instalación	Deshabilitado
Reiniciar la instalación	Deshabilitado

Mantenimiento de Internet Explorermostrar

Interfaz de usuario del explorador/Barra de títulos personalizadamostrar

Texto de la barra de título

Farmaenlace

Conexión/Configuración automática del

Directiva	**Configuración**
Detectar automáticamente la configuración	Deshabilitado
Configuración automática del explorador	No configurado

Conexión/Configuración de la

Este GPO contiene configuración de conexión.

Direcciones URL/Direcciones URL importantesmostrar

Nombre	Dirección URL
Dirección URL de la página principal	http://www.farmaenlace.com/farmaenlace
Dirección URL de la barra de búsqueda	No configurado
Dirección URL de la página de soporte técnico	No configurado

Direcciones URL/Favoritos y vínculos

Directiva	Configuración
Colocar los Favoritos y vínculos en la parte superior de la lista en el siguiente orden	Habilitado
Eliminar los Favoritos y los Vínculos existentes, si los hay	No configurado
Eliminar canales existentes si los hubiera	Habilitado

Favoritos\Aplicaciones Farma

Nombre	Dirección URL
Central Telefónica NBX	http://192.168.238.10:8081/sistar/login.sis
Medicación Frecuente	http://192.168.238.10/SitioMedicacionFrecuenteCanje/Canje/Facturas.aspx
Novedades de Bodega	http://192.168.238.10:8082/farma1/frmIncBodega.jsp
Novedades de Desarrollo Humano	http://192.168.238.10:8082/dh/
Novedades de Infraestructura	http://192.168.238.10:8082/infraestructura/
Novedades de Sistemas	http://192.168.238.10:8082/sistemas/
Pago Comisiones	http://192.168.238.158/EasyLogin/wfLogin.aspx?UrlRedirect=http://192.168.238.10/SitioPagoComision/wfIndex.aspx&Aplicacion=SITIO_PAGOCOMISIONES&AppCod=PC
Registro de Valijas	http://192.168.238.10:8082/valijas/

Reporte Top Ventas	http://192.168.238.10/SitioReportesPV/Reportes/Ventas.aspx
Reserva de Citas Médicas	http://192.168.238.19:8585/SHAM/busca_paciente1.jsp

Plantillas administrativas

Sistema

Directiva	**Configuración**
Desactivar reproducción automática	Habilitado
Desactivar reproducción automática en:	Todas las unidades

ANEXO F

RECOMENDACIONES PARA EL DATACENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Luego de la visita realizada a las instalaciones del DataCenter de la UNIVERSIDAD TECNICA DEL NORTE donde se tuvo la oportunidad de ingresar y evaluar las características y condiciones bajo las que está funcionando el DataCenter, se procede a realizar varias recomendaciones en base al estándar de la norma TIA-942 y a la experiencia recabada en el proyecto de tesis que se ha realizado para la empresa Farmaenlace Cía. Ltda.

Características DataCenter UTN

a) Área aproximada: 20 metros cuadrados
b) Altura aproximada: 2 metros mas 30 cm de piso técnico
c) Piso técnico de 30 cm de altura aproximadamente
d) Techo falso
e) Aire acondicionado: Liebert de Presicion 30000BTU con control de humedad
f) Cuatro racks tipo gabinete
    a. Rack de servidores
    b. Rack de equipos de comunicaciones
    c. Rack de Cableado estructurado
    d. Rack de terminación de fibra Optica
g) Sistema de extinción de Incendios con componentes de gas FM200 de activación automática.
h) Cámara de video - monitoreo
i) UPS de 25 KVA
j) Posee dos mesas de madera con equipos de computo
k) Puerta de seguridad con barra de pánico y acceso controlado con panel numérico (sin utilización)

Recomendaciones

Las recomendaciones para implementar en la infraestructura física del DataCenter de la Universidad Técnica del Norte son las siguientes:

1. El DataCenter es una zona de alta importancia en el edificio por lo que se recomienda que el espacio destinado para este sea únicamente para albergar equipamiento de comunicaciones, servidores y cableado estructurado, se recomienda no colocar dentro de esta área materia potencialmente inflamable como:
    a. Cajas de cartón
    b. Mesas de madera
    c. Papel o plástico que no deba estar dentro de esta área.
2. Para la implementación de nuevo equipamiento, el retirar de cajas y embalajes debe ser realizado en una zona fuera del DataCenter y los equipos deben ingresar ya armados para ser colocados en los racks pertinentes.
3. Se observa que existen cuatro racks tipo gabinete albergando cableado estructurado, equipos de comunicaciones y servidores, la colocación de los racks en "L" no es la adecuada, la norma TIA-942 recomienda la colocación de hileras de racks de tal manera que se creen pasillos calientes y pasillos fríos, al tener una disposición en hilera se podrá obtener un mejor flujo de aire y ahorro de energía en enfriamiento.
4. En los racks existen espacios abiertos que deben ser cubiertos con placas plásticas esto con la finalidad de que el flujo de aire sea correcto y no haya desperdicio de energía por el funcionamiento del aire acondicionado.
5. Se detecta una organización de cableado en ciertas partes de los racks, pero también existen cables sueltos o desorganizados, se recomienda realizar una alineación o peinado de cables, retirar cables no utilizados sean de red o cable eléctricos
6. Se observa que se tiene implementado piso técnico asi como tabien en la parte superior existe techo falso y se posee espacio en el interior para paso de cableado, que no está siendo utilizado por completo ya que existen cables que pasan entre racks por la parte alta sin un orden o canal de guía. Se recomienda el uso de estos espacios o de ser necesario la implementación de canaletas o escalerillas para la colocación de cableado estructurado entre racks.
7. Se tiene equipamiento de comunicaciones sin utilizar y colocado en la parte alta de los rack, se recomienda retirarlo y almacenarlo en una zona fuera del DataCenter.

8. Existen paneles de cableado estructurado que no está siendo utilizado se observan cables cortados, se recomienda retirar lo que no está siendo utilizado y liberar espacio en los racks o reorganizar los racks colocando espacios justos entre equipamiento lo que mejora el flujo de aire que es aprovechado por loe equipos.
9. Existen servidores tipo torre que están colocados en el piso del DataCenter y en una de las mesas de madera, se recomienda aprovechar el espacio libre del rack de servidores y colocar sobre una bandeja metálica estos servidores para aprovechar el espacio y liberar la zona.
10. La administración de los equipos como servidores o equipos de comunicaciones debe ser en lo posible siempre desde fuera del DataCenter por consola Telnet o conexión por Escritorio Remoto, solo en casos en que se necesite una interacción de tipo física con el equipo el personal autorizado debe ingresar a esta zona
11. Se observa que la puerta de ingreso es de tipo metálica y con seguridad implementada para el acceso que es una correcta implementación, sin embargo según comentario del Ingeniero Cosme Ortega este tipo de ingreso no está siendo utilizada ya que personal de desarrollo tiene acceso al DataCenter para la implementación de software en producción, se recomienda que se les brinde acceso remoto a los servidores y que el acceso al DataCenter sea estrictamente limitado por políticas de seguridad.
12. En cuanto a instalaciones eléctricas se observa que el DataCenter posee un respaldo de energía UPS de 25 KVA se considera suficiente para esta zona, sin embargo se podría consultar con proveedores para que se incremente el tiempo de duración del respaldo que generan las baterías de este UPS por un tiempo superior a 20 minutos
13. Se recomienda se implemente un generador eléctrico que alimente a esta zona para que en caso de falla eléctrica se proceda a activar este generador y el DataCenter no tenga que ser apagado luego que se termina la alimentación emergente que genera el UPS y la energía aun no haya sido restablecida.
14. La Norma TIA-942 recomienda la instalación de una o varias tomas eléctricas que no pertenezcan a la misma instalación eléctrica que alimenta a los equipos del DataCenter, esto para conectar equipamiento de limpieza o equipos no pertenecientes al DataCenter y que serán utilizados temporalmente.
15. Se observa se tiene una cámara de monitoreo que permite visualizar las actividades que se están realizando en el DataCenter, pero no se tiene grabación de los eventos, se recomienda implementar una solución que permita la grabación de eventos en DataCenter para poder

obtener respaldos o visualizar actividades en momentos que no se tenía a personal video-vigilando el DataCenter.

Lamentablemente no se ha podido acceder a documentación referente a políticas o planes de recuperación de servicios pero se recomienda tener la siguiente documentación, que de existir no debe tomarse en cuenta o pensar en actualizarla a las actuales características del DataCenter.

1. Política de seguridad y acceso a áreas restringidas
2. Política de uso de servicios correo electrónico, navegación
3. Procedimiento para configuración de servidores
4. Plan de mantenimiento anual de equipos
5. Plan de continuidad del negocio
6. Plan de recuperación de desastres.

Extiendo el más profundo agradecimiento al Ingeniero Fernando Garrido Jefe de tecnología de la Universidad Técnica del Norte y a su personal por la oportunidad y facilidades de acceso brindadas para esta evaluación, se espera estas recomendaciones sean de beneficio para el correcto desempeño y funcionamiento de esta importante zona y puedan ser aprovechadas de la mejor manera.