



ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

TESINA DE SEMINARIO

“Diseño y Simulación de un Data Center Cloud Computing que Cumpla con la Norma PCI-DSS”

Previo a la obtención del Título de:

**INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN
SISTEMAS DE INFORMACIÓN**

**INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN
SISTEMAS TECNOLÓGICOS**

**INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN
SISTEMAS TECNOLÓGICOS**

Presentada por:

**María Elizabeth Aguirre Patiño
Iván Isaac Solís Granda
Rut Ester España Peláez**

GUAYAQUIL – ECUADOR

Año: 2011

A G R A D E C I M I E N T O

Agradeciendo en primer lugar a Dios, a mis padres y hermanas, por su amor y apoyo incondicional, siendo parte fundamental para la culminación de esta etapa de la vida. Al Ing. Alfonso Aranda por su ayuda durante todo el seminario para la elaboración de este trabajo con éxito, y mis amigos de tesis por ser parte de este grupo de tesis.

María

A G R A D E C I M I E N T O

Agradezco a Dios, a mi amado esposo y a todas las personas que me apoyaron durante la realización de mi carrera profesional.

En especial a mis padres que me enseñaron a seguir siempre adelante hasta alcanzar mis metas. A mis hermanos que siempre me dieron buenos y sabios consejos que me guiaron durante mi vida.

Les agradezco a todos por su apoyo incondicional.

Rut

A G R A D E C I M I E N T O

Agradezco de manera muy especial a mis padres y mis hermanos por haberme apoyado en toda mi vida estudiantil, ya que sin su apoyo, colaboración e inspiración habría sido imposible terminar ni culminar mi proyecto de graduación y por ende mi carrera de Ingeniería en Ciencias Computacionales.

A mis padres, Catalina e Isaac, por su ejemplo de lucha y honestidad; a mis hermanos Luis y Mario por su ejemplo de capacidad y superación.

También a mis compañeras de grupo María Aguirre y Rut España un agradecimiento, especialmente por aquellos momentos en que el proyecto se ha tornado un camino largo y duro pero sin embargo se ha podido salir adelante.

Y por ultimo extender un sincero agradecimiento al Ingeniero José Alfonso Aranda Segovia, por su paciencia, disponibilidad y generosidad para compartir su experiencia y amplio conocimiento durante el seminario de graduación.

Iván

DEDICATORIA

Dedico este trabajo a Dios por ser nuestro guía.

A mis padres Guillermo y Martha a mis hermanas Martha, Verónica y Diana, a mi amado esposo José Paúl quienes han sido un apoyo incondicional durante mi vida. Y de manera muy especial a mi amorcito pequeño Mathias.

A los profesores que nos brindaron su conocimiento a lo largo de nuestra vida universitaria.

María

D E D I C A T O R I A

Dedico esta tesis a mis hijos Isaac y Ana, porque son la inspiración para que cada día yo pueda continuar creciendo en la vida, y a las personas que siempre confiaron en mí.

Rut

DEDICATORIA

Dedico este proyecto de Tesis a toda mi familia.

A mis padres y mis hermanos, por su comprensión y ayuda. Porque me han enseñado a encarar las diferentes adversidades sin perder nunca el optimismo.

Iván

TRIBUNAL DE SUSTENTACIÓN



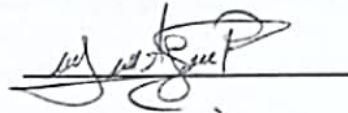
Ing. José Aranda Segovia
Profesor de Seminario de Graduación



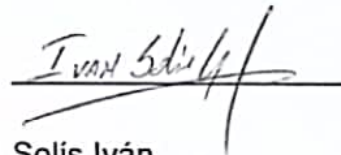
Ing. Vanessa Cedeño
Profesor Delegado de la FIEC

DECLARACIÓN EXPRESA

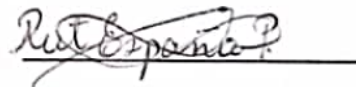
"La responsabilidad del contenido expuestos en este trabajo de Graduación nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

A handwritten signature in black ink, appearing to read 'María Aguirre', written over a horizontal line.

Aguirre María

A handwritten signature in black ink, appearing to read 'Iván Solís', written over a horizontal line.

Solís Iván

A handwritten signature in black ink, appearing to read 'Rut España', written over a horizontal line.

España Rut

RESUMEN

En el presente trabajo consiste en el diseño y análisis de un Centro de Datos Cloud Computing que cumpla con la Norma PCI-DSS analizando sus objetivos y el alcance del mismo. Se presentan la descripción del servicio como es su funcionalidad de un Centro de Datos con su respectivo Estándar TIA-942, y así mismo explicaremos acerca del Cloud Computing con la Norma PCI-DSS.

Posteriormente en el Capítulo 2, se describe el marco teórico acerca del Centro de Datos Cloud Computing, explicando los requerimientos que conllevan para la creación de un Centro de Datos en su parte eléctrica, mecánica, el cableado, etc. También describe acerca de la tecnología y la virtualización que se usa en el Cloud Computing.

Luego, en el capítulo 3 se mencionará todo lo concerniente al diseño del Centro de Datos como las recomendaciones, ubicación, el cableado, el detalle de cada cuarto que contiene dicho Centro de Datos. Así mismo en este capítulo describiremos los requisitos de hardware y software para el servicio del Cloud Computing.

Después en el capítulo 4 presentaremos los detalles del diseño topológico tanto lógico y físico que se debe tener en cuenta durante el diseño. Aparte se describe los diferentes servicios que contará el Centro de Datos.

En el capítulo 5, se realizará un breve análisis del costo que implica poner en funcionamiento un Centro de Datos Cloud Computing, como también aquí el análisis eléctrico que deberá tener a la hora de poner en marcha dicho proyecto.

Finalmente se presenta las conclusiones referentes al diseño y análisis del proyecto, así como también las recomendaciones correspondientes que es puedan dar a partir del estudio obtenido en este proyecto de graduación.

ABREVIATURA

NOC	Network Operation Center
ANSI	American National Standards Institute - Instituto Nacional Americano de Estándares
TIA	Telecommunications Industry Association
EIA	Electronic Components Association
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
UPS	Uninterruptible Power Supply - Sistema de alimentación ininterrumpida
SLA	Service Level Agreement – Acuerdo de Nivel de Servicio
PCI-DSS	Payment Card Industry Data Security Standard
PCI-SSC	Payment Card Industry Security Standards Council
QSA:	Qualified Security Assessor
LAN	Network Area Local
MDA:	Area de Distribution Principal
PBX	Private Branch Exchange
HDA	Área de Distribución Horizontal

EDA	Área de Distribución Equipos
ZDA	Área de Distribución Zonal
PDU	Unidad de Distribución de Energía
ATS	Switch de Transferencia Automática
PLC	Sistema del Controlador Lógico Programable
EMI	Interferencia Electromagnética
RFI	Interferencia de Radiofrecuencia
TGB	Telecommunications Grounding Busbar
TMGB	Telecommunications Main Ground Busbar
LCP	Paquete de Enfriamiento Líquido
LPARs	Particiones Lógicas
VPARS	Particiones Virtuales
JSP	JavaServer Pages
EJB	Enterprise JavaBeans
LOMMF	Laser Optimized Multimode Fiber
CRAC	Unidad de Aire Acondicionado
UR	Unidad de Rack
UTP	Par Trenzado sin Apantallar
FTP	Par Trenzado Apantallado
ADSL	Línea de Abonado Digital Asimétrica

MPPS	Millón de paquetes por segundo
GSM	Sistema Global para las comunicaciones Móviles
OSI	Interconexión para sistemas Abiertos
VLAN	Red de área local Virtual
VPN	Red privada Virtual
PVC	Policloruro de Vinilo
LUX	Nivel de Iluminación
MAC	Control de acceso al medio
WAN	Wide Area Network
RAID	Redundant Array of Inexpensive Disks

ÍNDICE GENERAL

AGRADECIMIENTO

DEDICATORIA

TRIBUNAL DE SUSTENTACIÓN

DECLARACIÓN EXPRESA

RESUMEN

INDICE GENERAL

ABREVIATURAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

1. Descripción del Servicio.....	1
1.1. Antecedentes.....	1
1.1.1. Data Center.....	1
1.1.1.1. Funcionalidad.....	2
1.1.1.2. Aplicaciones en Sur-América.....	3
1.1.1.3. Estándar TIA-942.....	4
1.1.2. Cloud Computing.....	9
1.1.2.1. Concepto de Cloud Computing.....	10
1.1.2.2. Característica del Cloud Computing.....	12

1.1.2.3. Adopción del Cloud Computing en Latinoamérica.....	12
1.1.2.4. Obstáculos del Cloud Computing en el Ecuador.....	14
1.1.2.5. Oportunidades y amenazas para el mercado ecuatoriano.....	16
1.1.3. Norma PCI-DSS.....	17
1.1.3.1. Antecedentes.....	17
1.1.3.2. Cuadro Evolutivo de la Norma PCI-DSS.....	18
1.1.3.3. Objetivos de control y requisitos Norma PCI-DSS.....	18
1.1.3.4. Relación con otras Normas.....	22
1.2. Objetivos.....	23
1.3. Alcance.....	24
1.3.1. Mercado Objetivo.....	25
1.4. Compromiso del Servicio.....	26
1.4.1 Acuerdo del Nivel de Servicio (SLA).....	26

2. Marco Teórico del Centro de Datos y Cloud Computing.....	27
2.1. Requerimientos de un Centro de Datos TIER III.....	27
2.1.1. Disposición Espacial de un Centro de Datos III.....	28
2.1.1.1. Cuarto de Entrada o de Servicios	29

2.1.1.2. Cuarto de Telecomunicaciones.....	29
2.1.1.3. Cuarto de Equipos.....	29
2.1.2. Ubicación del Centro de Datos para TIER III.....	31
2.1.3. Suelo técnico, Paredes y Techos.....	31
2.1.4. Diseño Eléctrico.....	34
2.1.5. Sistema Eléctrico.....	35
2.1.5.1. Switch Transferencia Automática (ATS).....	36
2.1.5.2. Grupo Electrónico o Generador de Energía.....	38
2.1.5.3. Unidad de Almacenamiento de Energía (UPS).....	39
2.1.5.4. Unidad de Distribución de Energía (PDU).....	40
2.1.6. Alumbrado.....	42
2.1.7. Sistema de puesta a tierra.....	43
2.1.8. Sistema de cableado.....	43
2.1.8.1. Cableado Horizontal.....	44
2.1.8.2. Cableado Vertical.....	44
2.1.9. Sistema Climatización.....	45
2.1.9.1. Aire Acondicionado del Cuarto de Computadoras (CRAC).....	47
2.1.9.2. Contención de pasillo caliente para configuraciones de alta densidad	49

2.1.9.3. Sistema de Climatización de las Salas Internas.....	50
2.1.10. Detección de Agua en Piso Falso.....	51
2.1.11. Protección Contra Incendios.....	51
2.1.12. Rack.....	52
2.1.12.1. Ubicación de Equipos.....	52
2.1.12.1.1. Paneles de Conexión.....	53
2.1.12.1.2. Enrutadores (Router).....	54
2.1.12.1.3. Conmutadores (Switch).....	57
2.1.12.1.4. Servidores.....	59
2.1.12.1.5. Matriz de Discos.....	63
2.1.13. Dispositivos o Módulos de Servicios de Seguridad.....	64
2.2. Tecnología que Soporta el Cloud Computing.....	66
2.2.1. Arquitectura del Cloud Computing.....	66
2.2.2. Niveles de Servicios.....	67
2.2.2.1. Saas: Software como Servicio.....	67
2.2.2.2. PaaS: Plataforma como Servicio.....	68
2.2.2.3. IaaS: Infraestructura como Servicio.....	68
2.2.3. Tipos de Nubes.....	68
2.3. Virtualización del Cloud Computing.....	69
2.3.1. Virtualización de Plataforma.....	71

2.3.2. Virtualización de Red.....	72
2.3.3. Virtualización de Aplicaciones.....	72
3. Diseño del Diseño.....	73
3.1. Recomendaciones del Cableado Estructurado.....	73
3.2. Ubicación del Centro de Datos.....	74
3.3. Cableado Horizontal.....	74
3.4. Cableado Vertical.....	76
3.5. Sala de Centro de Operaciones y Sala de Cómputo.....	78
3.5.1. Sala de Centro de Operaciones.....	78
3.5.2. Sala de Computo.....	80
3.5.2.1. Área Principal de Distribución.....	82
3.5.2.2. Área de Distribución Horizontal.....	83
3.5.2.3. Área de Distribución Equipos.....	85
3.5.2.4. Climatización.....	86

3.5.2.5.	Unidad de Distribución de Energía.....	88
3.6.	Cuarto de Telecomunicaciones y de Entrada de Servicio.....	89
3.7.	Sistema Puesta a Tierra.....	91
3.8.	Protección Contra Incendios.....	95
3.9.	Medidas de Seguridad.....	96
3.10.	Requisitos de Hardware y Software para el servicio del Cloud Computing.....	99
3.10.1.	Software para virtualización (Pagados).....	100
3.10.2.	Software para virtualización (Libre).....	101
3.10.3.	Ventajas Plataformas de Virtualización.....	103
4.	Diseño Topológico y Servicios del Centro de Datos.....	106
4.1.	Topología de la Red.....	106
4.1.1.	Topología Física.....	107
4.1.2.	Topología Lógica	108

4.1.2.1.	Red Fuera de Banda.....	109
4.1.2.2.	Protocolos del Centro de Datos.....	112
4.2.	Servicios del Centro de Datos.....	115
4.3.	Servicio Ofrecido por el Centro de Datos.....	117
4.3.1.1.	Servicios Compartidos.....	117
4.3.1.2.	Servicios Dedicados (Hosting).....	118
4.3.1.3.	Servicios Virtuales.....	122
4.3.1.4.	Servicios de Colocación.....	128
5.	Análisis de Costo y Eléctrico.....	130
5.1.	Presupuesto.....	130
5.2.	Análisis Eléctrico del Centro de Datos.....	136
5.3.	Análisis del Mercado Objetivo versus al servicio ofrecido.....	139

CONCLUSIONES

RECOMENDACIONES

BIBLIOGRAFIA

ANEXOS

INDICE DE TABLA

Tabla 1.1 Subsistemas.....	6
Tabla 1.2 Oportunidades y Amenazas del Cloud Computing en el Ecuador.....	17
Tabla 1.3 Cuadro Evolutivo de la Norma PCI-DSS.....	18
Tabla 1.4 Objetivo de Control y Requisitos PCI-DSS.....	19
Tabla 1.5 Comparación Norma PCI-DSS con otras Normas.....	22
Tabla 2.1 Arquitectura Cloud Computing.....	67
Tabla 2.2 Niveles de Servicio Cloud Computing.....	67
Tabla 3.1 Requisitos Hardware y Software en Cloud Computing.....	99
Tabla 3.2 Software de Virtualización Pagadas.....	100
Tabla 3.3 Aceptación en el Mercado Software Virtualización Pagadas.....	100
Tabla 3.4 Software Virtualización Libre.....	101
Tabla 3.5 Aceptación en el Mercado Software Virtualización Libres.....	102
Tabla 3.6 Cuadro Comparativo de las Características del Cloud Computing.....	103
Tabla 3.7 Ventajas Plataformas de Virtualización.....	103

Tabla 3.8. Desventajas Plataformas de Virtualización.....	104
Tabla 4.1 Servidores Dedicados sin Administración.....	118
Tabla 4.2 Servidores Dedicados con Administración.....	119
Tabla 4.3 Características de los Servicios Alquilados.....	120
Tabla 4.4 Característica del Servicio de Bronce.....	124
Tabla 4.5 Característica del Servicio de Plata.....	126
Tabla 4.6 Característica del Servicio de Oro.....	127
Tabla 5.1 Presupuesto de Enrutamiento.....	131
Tabla 5.2 Presupuesto de Sistema Cableado.....	131
Tabla 5.3 Presupuesto de Sistema Eléctrico.....	132
Tabla 5.4 Presupuesto de Sistema Mecánico.....	132
Tabla 5.5 Presupuesto de Sistema Puesta a Tierra.....	132
Tabla 5.6 Presupuesto de Cuarto de Cómputo.....	134
Tabla 5.7 Presupuesto de Centro de Operaciones.....	135
Tabla 5.8 Costo del Proyecto.....	136
Tabla 5.9 Consumo de Potencia de Energía.....	138
Tabla 5.10 Mercado Objetivo Vs. Servicios.....	138

INDICE DE FIGURA

Figura 1.1 Cloud Computing.....	11
Figura 2.1 Diseño de la Topología del Centro de Datos TIER III.....	28
Figura 2.1.3 Piso falso del Centro de Datos.....	33
Figura 2.2 El Flujo Eléctrico De Poder.....	35
Figura 2.3 Esquema de configuración Principal – Generador.....	37
Figura 2.4 Switch de Transferencia Automática (ATS-NW Clase 2700).....	38
Figura 2.5 Grupo Electrónico - TIER III.....	39
Figura 2.6 Unidad de Almacenamiento de Energía (UPS NX).....	40
Figura 2.7 Unidad de Distribución de Energía (PDU).....	41
Figura 2.8 Balastro Eléctrico.....	42
Figura 2.9 Lámpara de 3 tubos fluorescente.....	42
Figura 2.10 Aire Acondicionado del Cuarto de Computadoras - CRAC.....	48
Figura 2.11 Criterio de Pasillos Fríos y Pasillos Calientes.....	49
Figura 2.12 Contención de pasillos calientes.....	50
Figura 2.13 Gas Protección contra Incendios.....	51
Figura 2.14 Rack.....	52

Figura 2.15 Panel de Conexión.....	54
Figura 2.16 Servidor y Servidor Blade.....	62
Figura 3.1 Cableado Horizontal del Centro de Datos.....	76
Figura 3.2 Bandeja metálica para el cableado vertical.....	78
Figura 3.3 Cuarto de Centro de Operaciones.....	79
Figura 3.4 Distribución de los gabinetes en la sala de cómputo.....	82
Figura 3.5 Rack del Área de Distribución Principal.....	83
Figura 3.6 Rack del Área de Distribución Horizontal.....	84
Figura 3.7 Rack del Área de Distribución de Equipos.....	85
Figura 3.8 Rack del Área de Almacenamiento de Red.....	86
Figura 3.9 Sistema de Climatización por Chiller.....	87
Figura 3.10 Sistema de Climatización por Rack.....	88
Figura 3.11 Administración de Energía en Rack.....	89
Figura 3.12 Rack del Cuarto de Entrada.....	90
Figura 3.13 Sistema Puesta a Tierra.....	93
Figura 3.14 Pasos de Puesta a Tierra en una Red.....	94
Figura 3.15 FM-200 – Protección Incendios.....	95
Figura 3.16 Funcionamiento FM-200	96
Figura 3.17 Aceptación en el Mercado Software Virtualización Pagadas.....	101

Figura 3.18 Aceptación en el Mercado Software Virtualización	
Libre.....	102
Figura 3.19 Ventajas Plataformas de Virtualización.....	104
Figura 3.20 Desventajas Plataformas de Virtualización.....	104
Figura 4.1 Diseño Físico del Centro de Datos.....	108
Figura 4.2 Diseño Lógico del Centro de Datos.....	109
Figura 4.3 Diseño Lógico de la Red Fuera de Banda.....	110
Figura 4.4 Diseño Puerto de Consola.....	112
Figura 4.5 Diseño del Protocolo HSRP.....	113
Figura 4.6 Diseño Topológico del Plan de Servicio Bronce.....	123
Figura 4.7 Diseño Topológico del Plan de Servicio Plata.....	125
Figura 4.8 Diseño Topológico del Plan de Servicio Oro.....	128
Figura 5.1 Análisis Eléctrico del Centro de Datos.....	137

INTRODUCCIÓN

Justificación

Un data center está relacionado con todos los recursos necesarios para el procesamiento de la información de una organización, por otro lado un Cloud Computing es una nueva tecnología o mezclas de tecnologías.

Por tal motivo es la respuesta a la tecnología de información a varios problemas, tales como costos de infraestructura, problemas ambientales, costo de energía y la mayor prioridad de contar con una infraestructura que sea fácil de usar pero a la vez confiable y redundantes a fallos, manteniendo los parámetros de disponibilidad, confiabilidad, integridad de la seguridad de la información como también es la respuesta de los altos costos de infraestructura que demanda las modernas empresa en la actualidad.

Diseñar un Data Center que provea servicios de Cloud Computing involucra el desarrollo de una serie de conocimientos que va desde la capa física hasta la capa lógica.

Este diseño sirve de referencia para cualquier organización que desee implementar un Centro de dato o Data Center con Tier III de última generación cumpliendo estándares internacionales.

Estado de Arte

En la actualidad existe una gama de Data Center. Una de las tantas empresas dedicadas a diseñar Data Center es **MYSI** ubicada en Colombia posee una amplia experiencia en el diseño y construcción de centros de cómputo, integrando productos de reconocidos fabricantes y garantizando la correcta operatividad de los subsistemas. Dentro de las consideraciones de diseño se incluye la optimización del uso de la energía, los requerimientos de continuidad operativa, el crecimiento y los parámetros de seguridad requeridos por dicha instalación.

Debido a que hoy en día existe una gran necesidad por asegurar a las empresas de estar al tanto de los últimos adelantos tecnológicos en el área de data centers.

El Cloud Computing, o “computación en la nube”, es la tendencia en el mundo tecnológico, que consiste en eliminar la dependencia de equipos computacionales, discos duros, pen-drives; para trabajar y almacenar información directamente en Internet.

Empresas tales como Google con Google Apps, Movistar con Movistar Cloud Computing, Amazon, Blue Cloud de IBM, Salesforce y Azure de Microsoft entregan actualmente este servicio en Latinoamérica tanto para empresas como para usuarios particulares dispuestos a adentrarse en el mundo del Cloud Computing. Así mismo estos servicios se pagan según alguna métrica de consumo.

Entre algunas características podemos mencionar del Cloud Computing: Auto Reparable, Escalable, Regidos por un Acuerdo de Nivel de Servicio, Virtualizado, Multipropósito.

1.- DESCRIPCIÓN DEL SERVICIO

1.1. Antecedentes.

1.1.1. Data Center

Denominado *centro de datos*, es un repositorio centralizado, ya sea físico o virtual, para el almacenamiento, gestión y difusión de datos e información organizada entorno a un conjunto de conocimientos o en relación con un negocio particular.

Data Center físico es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico. Suelen ser creados y mantenidos por grandes organizaciones con objeto de tener acceso a la información necesaria para sus operaciones.

Los recursos consisten esencialmente en dependencias debidamente acondicionadas, computadoras y redes de comunicaciones.

Entre los factores más importantes que motivan la creación de un Centro de Datos es poder destacar la continuidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, debido a la importancia de la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica. De acuerdo a expertos en redes, cada organización tiene un centro de datos, este puede referirse como una sala de servidores o incluso un equipo de armario. Por lo tanto, los Centros de Datos puede ser sinónimo de Centro de Operaciones de Red (NOC), un área de acceso restringido que contiene los sistemas automatizados que controlan constantemente la actividad del servidor, el tráfico Web y rendimiento de la red.

1.1.1.1. Funcionalidad

La función de un data center es proveer almacenamiento, seguridad, procesamiento y administración de datos, siendo su principal objetivo de diseño brindar confiabilidad y disponibilidad. En este sentido, las compañías han comprendido la importancia de contar con Centro de Datos robustos y confiables que garanticen la disponibilidad de la información almacenada, lo que ha dado paso a un creciente interés

por conocer y aplicar estándares internacionales como ANSI/TIA/EIA-942.

1.1.1.2. Aplicaciones en Sur-América

Telmex: Centro de Datos en TELMEX le ofrece una infraestructura robusta y segura, especialmente diseñada para soportar las necesidades de escalabilidad, redundancia, balanceo de carga, respaldo de energía y seguridad que requieren los recursos de información y las aplicaciones críticas de su empresa para hacer frente a las exigencias de incorporarse a la e-economía.

Dentro de las aplicaciones y/o funcionalidades de los servicios de Data Center de TELMEX, se encuentran:

- Operación remota de equipos con aplicaciones Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Portales de Comercio Electrónico, Bases de Datos, etc.
- Consolidación de Sistemas (reducción de equipos de cómputo).
- Soluciones de Continuidad de Negocio (Planes de Recuperación de Desastres).
- Correo electrónico.
- Registro y Mantenimiento de Dominio.

NXnet: posee sus servidores en Centro de Datos con la última tecnología y mejor conectividad del mercado, implementados con canales de alta velocidad especialmente diseñados para garantizar un excelente acceso desde cualquier parte del mundo. Poseemos equipos de última tecnología que respaldan nuestro servicio brindándole facilidad y estabilidad.

Los mismos cuentan con las siguientes características:

- Suministro de Energía Eléctrica permanente
- Sistema de detección y extinción de incendios
- Aire acondicionado
- Seguridad y vigilancia
- Vínculos de Comunicaciones
- Conectividad Interna del Data Center

1.1.1.3. Estándar TIA-942

En abril de 2005, la Telecommunication Industry Association publica su estándar TIA-942 con el propósito de unificar criterios en el diseño de áreas de tecnología y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, mejora la infraestructura de los subsistemas generando los lineamientos que se deben seguir para

clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar.

La infraestructura de soporte de un Centro de Datos se divide en cuatro subsistemas:

- Telecomunicaciones
- Arquitectura
- Sistema eléctrico
- Sistema Mecánico

Dentro de cada subsistema el estándar desarrolla una serie de ítems como se ilustra en la tabla I.

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de racks	Selección del sitio	Cantidad de accesos	Sistemas de Climatización
Accesos redundantes	Tipo de construcción	Puntos únicos de falla	Presión positiva
Cuarto de entrada	Protección ignífuga	Cargas críticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chillers
Backbone	Barrera de vapor	Topología de UPS	CRAC's y Condensadores
Cableado horizontal	Techos y pisos	PDU's	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendio
Alimentación redundante	NOC	EPO (Emergency)	Sprinklers

		Power Off)	
Patch panels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV	Transfer switch	

Tabla 1.1 Subsistemas

En el anexo del estándar establece cuatro niveles de TIERS de disponibilidad, teniendo que a mayor número de TIER mayor disponibilidad, lo que implica también mayores costos constructivos.

La norma describe, resumidamente, los distintos TIERS de la manera que sigue:

✓ **TIER I: Data Center Básico - 1960s**

Puede admitir interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía, pero puede no tener piso técnico, UPS o generador eléctrico. Si los posee pueden tener varios puntos únicos de falla. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del Data Center deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Errores de operación

o fallas en los componentes de su infraestructura causarán la interrupción del Data Center.

La tasa de disponibilidad máxima del Data Center es 28.8 horas y 99.671% del tiempo. Este nivel TIER I generalmente es para negocios pequeños.

- **TIER II: Componentes Redundantes – 1970s**

Con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto planeadas como las no planeadas. Estos Data Centers cuentan con piso falso, UPS y generadores eléctricos, pero está conectado a una sola línea de distribución eléctrica. Su diseño es (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas es del 100%. El mantenimiento en la línea de distribución eléctrica o en otros componentes de la infraestructura, pueden causar una interrupción del servicio. La tasa de disponibilidad máxima del Data Center es 22.0 horas y 99.741% del tiempo. Un Data Center TIER II puede encontrarse en compañías basados sus negocios en internet sin serias penalidades financieras por la calidad de servicio prestado.

- **TIER III: Mantenimiento Concurrente – 1980s**

Permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación.

Actividades planeadas incluyen mantenimiento preventivo, reparaciones o reemplazo de componentes, agregar o eliminar componentes, realizar pruebas de sistemas o subsistemas, entre otros. Debe existir suficiente capacidad y doble línea de distribución de los componentes, de forma tal que sea posible realizar mantenimiento o pruebas en una línea y mientras que la otra atiende la totalidad de la carga. En este nivel, actividades no planeadas como errores de operación o fallas espontáneas en la infraestructura pueden todavía causar una interrupción del Data Center. La carga máxima en los sistemas en situaciones críticas es de 90%.

La tasa de disponibilidad máxima del Data Center es 1.6 horas y 99.982% del tiempo. Este nivel es incluido en compañías que brindan servicios las 24 horas de forma continuas y soportan procesos de negocios automatizados.

- **TIER IV: Tolerante a Fallas – 1990s**

Provee capacidad para realizar cualquier actividad planeada sin interrupciones en el servicio, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aún ante un evento crítico no planeado. Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración Sistema + Sistema. Eléctricamente esto significa dos sistemas de UPS independientes, cada sistema con un nivel de redundancia N+1. La

carga máxima de los sistemas en situaciones críticas es de 90%. Persiste un nivel de exposición a fallas, por el inicio una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia, los cuales deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos. La tasa de disponibilidad máxima del Data Center es 0.4 horas y 99.995% del tiempo. En este nivel se encuentran compañías de servicios de correos electrónicos, transacciones de bolsa de valores, procesos financieros.

El concepto de Clasificación TIER se trata de una mejora prácticas y contiene ciertas norma de Uptime Institute, el cual representa el nivel de desempeño y disponibilidad con el que se establecen los criterios de diseño de un data center o se selecciona un proveedor para dichos servicios.

1.1.2. Cloud Computing

Antecedentes

La idea de Cloud Computing no es nueva, se ha venido trabajando en este concepto desde hace algunos años, como Computación en Demanda, Computación Elástica.

El mayor inconveniente que presenta este esquema de trabajo para la mayoría de las empresas es la falta de un nivel de madurez adecuado para su implementación en el mercado, sin embargo cada día esto evoluciona a mayor velocidad.

Esta madurez se ve favorecida por la aparición de dos componentes, por un lado las tecnologías de virtualización de cómputo y de almacenamiento de datos y por el otro el aumento en la confiabilidad de las soluciones empresariales de Internet.

El Internet usualmente se visualiza y conceptualiza como una gran nube donde todo está conectado, en las cuales al conectarse a Internet se suministran todos los servicios de cómputo requeridos, se denomina Cloud Computing o Computación en Nube, la cual es similar a todos los esquemas antes nombrados, pero potenciada con las tecnologías de virtualización.

1.1.2.1 Concepto de un Cloud Computing

El Cloud Computing es un nuevo paradigma de computación donde los datos y los servicios residen en centros de datos masivamente escalables y se puede acceder desde cualquier dispositivo conectado a través de internet.

Esta tecnología es utilizada para guardar y mantener todo nuestros datos en servidores lejanos o remotos donde tenemos libre acceso las

24 horas y los 7 días de la semana en cualquier lugar del mundo a través de aplicaciones.

De esta manera se facilita aún para los usuarios el uso de respaldo, puesto que se eliminan los servidores necesarios para archivar información que requieren mantención de mano de obra especializada, la cual tenía un costo elevado.

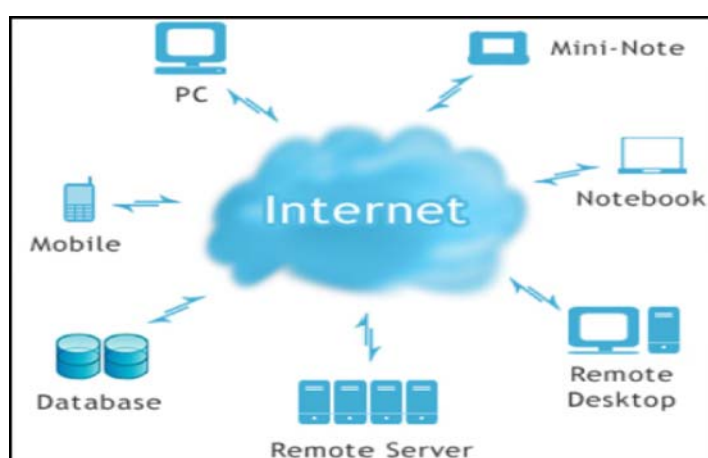


Figura 1.1 Cloud Computing

Empresas tales como Google, con Google Apps, y Movistar, entregan actualmente este servicio en varios países de Latinoamérica.

La idea de esta "nube" es un intermediario virtual entre el proveedor del servicio y el usuario o cliente, y se puede acceder a esta nube desde cualquier dispositivo con acceso a internet. El proveedor maneja desde sus propias oficinas los recursos que presta a sus clientes, y estos recursos se "virtualizan" y pasan a ser parte de una "nube virtual"

1.1.2.2 Características del Cloud Computing

- **Auto Reparable:** En caso de fallo, el último backup de la aplicación pasa a ser automáticamente la copia primaria y se genera uno nuevo.
- **Escalable:** Todo el sistema/arquitectura es predecible y eficiente. Si un servidor maneja 1000 transacciones, 2 servidores manejarán 2000 transacciones.
- **Regidos por un Acuerdo de Nivel de Servicio (SLA)** que define varias políticas como cuáles son los tiempos esperados de rendimiento y en caso de pico, debe crear más instancias.
- **Virtualizado:** las aplicaciones son independientes del hardware en el que corran, incluso varias aplicaciones pueden correr en una misma máquina o una aplicación puede usar varias máquinas a la vez.
- **Multipropósito:** El sistema está creado de tal forma que permite a diferentes clientes compartir la infraestructura sin preocuparse de ello y sin comprometer su seguridad y privacidad

1.1.2.3 Adopción del Cloud Computing en Latinoamérica

En Latinoamérica se proyecta un auge de la tecnología del Cloud Computing y se necesitaría aproximadamente 5 años para que la tecnología llegue a su madurez.

Cerca de un tercio de las organizaciones en Latinoamérica implementará la computación en nube en 2010, según la encuesta conducida por ISACA "IT Risk/Reward Barometer" (Barómetro Riesgo/Recompensa de TI).

Mientras el 41% de los 433 profesionales de tecnología de información latinoamericanos encuestados considera que los riesgos de la computación en nube sobrepasan los beneficios, el 18% cree lo contrario y el 42% opina que los beneficios y riesgos tienen un balance apropiado: *"La nube representa un gran cambio de paradigma en cuanto a la manera en que los recursos de computación se implementan, de modo que no es sorprendente que los profesionales de TI se preocupen sobre la compensación del riesgo frente a la recompensa"*, señaló Robert Stroud, CGEIT, vicepresidente internacional de ISACA y vicepresidente de Gestión de Servicios de TI y Gobernabilidad de CA.

En nuestro País el interés de adquirir sistemas para mantener la seguridad de la información en empresas ha ido creciendo desde hace 5 años. Por ello diferentes empresas están dando a conocer las bondades de la tecnología del Cloud Computing y los servicios que prestan al mercado para tener una mayor seguridad de la información.

1.1.2.4. Obstáculos del Cloud Computing en el Ecuador

A continuación, se describen algunos de los obstáculos identificados que dificultan la adopción del Cloud Computing:

- **Percepción de la seguridad** Una de las mayores preocupaciones en moverse hacia el Cloud Computing es el tema de seguridad. Aún existe mucho desconocimiento acerca de las grandes ventajas de seguridad de las nubes de cómputo de talla mundial, que en su mayoría superan a la de los centros de datos “in-house”. Sin embargo, la percepción de que los datos están más seguros dentro de las instalaciones propias es aún muy extendida. Con el objetivo de superar este obstáculo, se recomienda seguir los lineamientos de las mejores prácticas de seguridad como proteger los datos (24/7), asegurar y certificar todo el software, encriptar siempre los datos del suscriptor y validar prácticas de seguridad, entre otros; actividades que cumplen las nubes de cómputo en su gran mayoría.
- **Percepción acerca de la conformidad con la regulación** Bajo el modelo de Cloud Computing, los datos de los usuarios pueden estar en cualquier parte del mundo. Esto compromete al usuario a conocer y cumplir con las normas y leyes existentes sobre temas como el almacenamiento y la difusión de los datos, impuestos en

transacciones comerciales, entre otros; reguladas en cada nación. Del mismo modo, compromete al proveedor de Cloud Computing a responsabilizarse por el cumplimiento con la normatividad, lo cual conlleva a procesos de auditoría y seguimientos periódicos. Estas normas pueden ser fácilmente cumplidas por los proveedores de Cloud Computing y con mayor dificultad por parte de las empresas; sin embargo, existe la percepción de que para cumplir con la normatividad una empresa no debe tercerizar sus sistemas de información.

- **Restricciones de Internet** El tráfico de Internet está sujeto a retardos introducidos por cada uno de los nodos por donde pasa. El tráfico de Internet puede experimentar cuellos de botella.
- **Pérdida del control** En el Cloud Computing, el usuario debe prever una pérdida de control sobre la información, pues no tiene acceso a los servidores o no pueden estar seguros que el proveedor de la nube tenga un plan de continuidad adecuado para el negocio ante cualquier perturbación o interrupción física o fracaso y cierre del proveedor de Cloud Computing. De hecho, el Cloud Computing no permite a los usuarios poseer físicamente los dispositivos de almacenamiento de su información o datos, dejando la responsabilidad de su almacenamiento y su control en manos de un determinado proveedor del servicio. Por este motivo, existen

detractores sobre el tema que argumentan que sólo es posible usar las aplicaciones y servicios que el proveedor esté dispuesto a ofrecer, y que este esquema limita la libertad de los usuarios haciéndolos dependientes del proveedor de servicios. Aunque se pueden exigir Acuerdos de Nivel de Servicio detallado, la pérdida de control del usuario sigue presente.

Otro de los problemas que se plantean sobre el concepto de almacenamiento externo de la información se centra en aspectos relativos a la seguridad, ya que cuando se tratan aspectos del Cloud Computing relativos al hospedaje de los datos (hosting), su regulación y legislación aplicada depende del país dónde se encuentren los servidores que sustentan el servicio, así como aspectos relacionados con la integridad, disponibilidad o recuperación en caso de desastre.

1.1.2.5 Oportunidades y amenazas para el mercado ecuatoriano

En el siguiente cuadro se ilustra las oportunidades y amenazas identificadas en el proceso de adopción de la nube para una gran empresa en territorio Ecuatoriano.

<ul style="list-style-type: none"> • Posibilidad de reducir costos operativos • Mayor agilidad para responder a las condiciones del mercado. • Cloud Computing permite a las empresas Centrarse en su negocio principal • Incrementar la capacidad para ser flexible • Primeros en adoptar las nuevas tecnologías 	<ul style="list-style-type: none"> • Percepción de pérdida del control de datos y sistemas • Temor al mal manejo de un tercero sobre información de su compañía.

Tabla 1.2 Oportunidades y Amenazas del Cloud Computing en el Ecuador

1.1.3. Norma PCI – DSS

1.1.3.1 Antecedentes

PCI DSS (Payment Card Industry Data Security Standard): significa Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago. Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayude a las organizaciones que procesan,

almacenan y/o transmiten datos de tarjeta habientes (o titulares de tarjeta), para asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.

1.1.3.2 Cuadro Evolutivo de la Norma PCI-DSS.

Visa CISP (Cardholder Information Security Program)	2000
Visa AIS (Account Information Security)	2000,2001-06
Mastercard SDP (Site Data Protection)	
American Express DSOP (Data Security Operating Policy)	
Discover DISC (Discover Information Security and Compliance)	
PCI DSS (Payment Card Industry Data Security Standard).	2004,2005-01,2005-06

Tabla 1.3 Cuadro Evolutivo de la Norma PCI-DSS

Tenemos tres principales agentes implicados en el tratamiento de tarjetas que definen los requisitos para instituciones financieras, comerciantes y proveedores de servicios que tratan con datos de titulares de tarjeta. Este estándar consta de una lista de requisitos para administración de seguridad, directivas, procedimientos, arquitectura de red, diseño de software y otras medidas para proteger los datos. Los análisis de auditoría los realizan dos tipos de organizaciones de terceros, conocidas como evaluadores de seguridad calificados (QSA, Qualified Security Assessors) y proveedores de servicios de escaneo aprobados (ASV, Approved Scanning Vendors). Los evaluadores QSA

realizan la parte de auditoría, mientras que los proveedores ASV realizan los exámenes de vulnerabilidad en los entornos de Internet de la organización.

1.1.3.3 Objetivos de control y sus requisitos son los siguientes:

Requisito 1:	Instalar y mantener una configuración de cortafuegos para proteger los datos de los propietarios de tarjetas.
Requisito 2:	No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores.
Objetivo de control	Proteger los datos de los propietarios de tarjetas.
Requisito 3:	Proteger los datos almacenados de los propietarios de tarjetas.
Requisito 4:	Cifrar los datos de los propietarios de tarjetas e información confidencial transmitida a través de redes públicas abiertas.
Objetivo de control	Mantener un Programa de Manejo de Vulnerabilidad.
Requisito 5:	Usar y actualizar regularmente un software antivirus.
Requisito 6:	Desarrollar y mantener sistemas y aplicaciones seguras.
Objetivo de control	Implementar Medidas sólidas de control de acceso.
Requisito 7:	Restringir el acceso a los datos tomando como base la necesidad del funcionario de conocer la información.
Requisito 8:	Asignar una Identificación única a cada persona que tenga acceso a un computador.
Requisito 9:	Restringir el acceso físico a los datos de los propietarios de tarjetas.
Objetivo de control	Monitorear y Probar regularmente las redes.
Requisito 10:	Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los propietarios de tarjetas.
Requisito 11:	Probar regularmente los sistemas y procesos de seguridad.
Objetivo de	Mantener una Política de Seguridad de la

control	Información.
Requisito 12:	Mantener una política que contemple la seguridad de la información

Tabla 1.4 Objetivo de Control y Requisitos PCI-DSS

Estos requisitos de la norma se aplica a todos los miembros de la red de tarjetas de pago, los comerciantes y proveedores de servicios que almacenan, procesan o transmiten datos de los tarjeta habientes, y afectan a todos los canales de pago, incluida la venta al por menor.

De una manera resumida se puede mostrar los controles de la Norma PCI-DSS con sus requisitos:

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Este documento, Requisitos de normas de seguridad de datos de la PCI y procedimientos de evaluación de seguridad, utiliza como base los 12 requisitos de las DSS de la PCI y los combina con los procedimientos de evaluación pertinentes en una herramienta de evaluación de seguridad. Se diseñó para que lo utilizaran los asesores que realizan visitas en el sitio del comerciante y de los proveedores de servicios que deben validar la conformidad con las DSS de la PCI.

Las compañías que procesan, guardan o transmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito (Pérdida de franquicias), enfrentar auditorías rigurosas o pagos de multas. Los Comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica.

Esta validación es realizada por auditores autorizados Qualified Security Assessor (QSAs). Sólo a las compañías que procesan menos de 80,000 transacciones por año se les permite realizar un auto evaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC).

El incumplimiento de los requisitos del PCI-DSS puede dar lugar a sanciones o puede ser privada de procesar tarjetas de pago. Entre ellas, las siguientes:

- Multas de 500.000 dólares por incidente de seguridad de datos
- Multas de 50.000 dólares por día de incumplimiento de los estándares publicados
- Responsabilidad por todas las pérdidas incurridas como resultado de números de cuenta robados
- Responsabilidad por todos los gastos asociados a la reemisión de las tarjetas de dichas cuentas
- Suspensión de cuentas comerciales

Desventaja de no cumplir con la Norma PCI-DSS:

- 3 de cada 4 clientes no quieren comprar en un negocio que ha sido previamente comprometido.
- 84% de los clientes quieren comprar en negocios que son líderes en seguridad.

¿Quién certifica la norma PCI-DSS?

Para el cumplimiento con la norma PCI-DSS, el proceso deberá estar respaldado con los procedimientos adecuados y se deberá generar la documentación necesaria para que el sistema sea aprobado por un QSA (Estándares de configuración, plantilla de revisión, entregables, etc.), en el anexo 1 podemos visualizar el Cuestionario de Certificación para la Norma PCI-DSS.

1.1.3.4 Relación con otras normas

PCI-DSS	ITIL	ISO:27001
El cumplimiento de esta norma es obligatorio.	ITIL no es una norma sino un estándar en que se puede basar para ofrecer seguridad en la TI.	El cumplimiento de esta norma es por seguridad.
Se relaciona con la prevención y detección de la manipulación de los registros electrónicos.	Las pymes pueden obtener ventajas implementando mejoras de buenas prácticas basadas en ITIL en la prestación de servicios y la asistencia.	Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la

		Información (SGSI).
Detalla los requisitos de seguridad para los miembros, los comerciantes y los proveedores de servicios que almacenan, procesan o transmiten datos de los titulares de tarjetas.		

Tabla 1.5 Comparación Norma PCI-DSS con otras Normas

1.2. Objetivos.

- Diseñar y simular un Data Center que provea servicios de Cloud Computing al mercado local cumpliendo con el estándar de la norma PCI-DSS.
- Ofrecer un servicio eficiente a través del Data Center usando la tecnología del Cloud Computing aplicando las normas que se exigen.
- Brindar ayuda a las empresas que manejan grandes cantidades de información la cual necesitan tener disponibilidad, integridad y seguridad al manejar sus datos.
- Proveer un ahorro económico en las empresas al momento de contratar el servicio del Data Center y mejorar la experiencia de conexión de los usuarios.

- Realizar un análisis financiero para la adquisición de los servicios del Cloud Computing, comparando los costos actuales con los obtenidos en el análisis.

1.3. Alcance

1.3.1. Mercado Objetivo.

Es fundamental estudiar el mercado objetivo de este proyecto; para referirse a quien va dirigido nuestro servicio así como también satisfacer sus necesidades

PYMES: son Pequeñas y Medianas Empresas, con un número no muy grande de trabajadores, es decir, tienen que tener como número menos de 250 empleados contratados refiriéndose a los de planta, como también a los empleados externos que se puedan llegar a subcontratar.

Corporaciones: es una entidad constituida en forma legal y separada de sus accionistas. Una corporación puede ser una universidad, una empresa, un gremio, un sindicato u otro tipo de persona colectiva.

Entidades Financieras: Son aquellas encargadas de facilitar la financiación a los que necesitan recursos, sean sociedades o particulares. Van desde los bancos y cajas de ahorros hasta las

sociedades que nos prestan dinero para la compra de un bien concreto como pueda ser un vehículo.

Services Provider: es una entidad que proporciona servicios a otras entidades. Por lo general, esto se refiere a un negocio que ofrece la suscripción o servicio web a otras empresas o individuos. Ejemplos de estos servicios incluyen acceso a Internet , operador de telefonía móvil, y aplicaciones web hosting . El término se aplica con mayor frecuencia a los servicios de comunicación que a otros tipos de industria de servicios .

1.4. Compromiso del Servicio.

1.4.1. Acuerdo de Nivel de Servicio (SLA)

SLA (Service Level Agreement - Acuerdo de Nivel de Servicio), es un documento de carácter legal, generalmente anexo en el Contrato de Prestación de Servicios. En el SLA se estipulan las condiciones y parámetros que comprometen al prestador del servicio (el *proveedor*) a cumplir con unos niveles de calidad de servicio frente al contratante de los mismos (el *cliente*); este puede ser medido y demostrado.

En un SLA se pueden establecer tantos indicadores como se estime necesario y de su evaluación se obtienen por ejemplo penalizaciones a la empresa suministradora, identificación de puntos débiles del

proceso e indicaciones para procesos de mejora continua en determinadas actividades.

2. MARCO TEÓRICO DEL CENTRO DE DATOS Y CLOUD COMPUTING

2.1 Requerimientos de un Centro Datos TIER 3

El Centro de Datos es un ambiente especialmente diseñado para albergar todos los equipos y elementos necesarios para el procesamiento de información de una organización. Es por esto que deben ser extremadamente confiables y seguros al tiempo que deben ser capaces de adaptarse al crecimiento y la re-configuración permitiendo que cualquiera alteración al diseño y mantenimiento

ocurra sin paralizar los servicios y proveer por lo menos una redundancia N+1.

2.1.1 Disposición Espacial de una Centro de Datos TIER 3

El principal objetivo de un Centro de Datos es el espacio a seleccionarse debe ser lo suficientemente grande para poder brindar facilidades de expansión de los servicios. Por esto se recomienda que el Centro de Datos debe contar con espacios libres para que en un futuro puedan ser ocupados ya sea por racks, gabinetes o servidores. La construcción de un Centro de Datos requiere la integración de la infraestructura y de equipos, para el diseño de un Centro de Datos TIER 3 se escogerá la siguiente topología de acuerdo a la norma TIA 942.

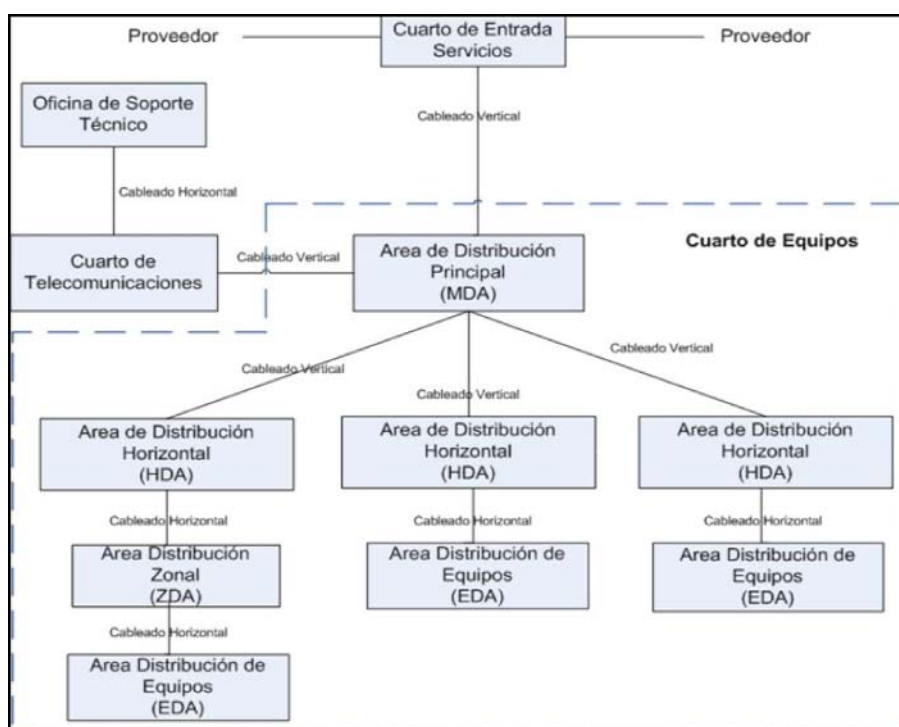


Figura 2.1 Diseño de la Topología del Centro de Datos TIER III

2.1.1.1 Cuarto de Entrada o de Servicios

Es un espacio de interconexión entre el cableado estructurado del Centro de Datos y el cableado proveniente de las operadoras de telecomunicación; es decir es el punto de conexión donde el cableado externo se une con el cableado vertical o también conocido como Backbone interno del Centro de Datos. No necesariamente tiene que estar en el cuarto de equipos.

2.1.1.2 Cuarto de Telecomunicaciones

Es el lugar donde termina el cableado horizontal y se origina el cableado vertical, contienen componentes como patch panels. Pueden tener también equipos activos de LAN como por ejemplo switches. Dicho cuarto debe ser de uso exclusivo de equipos de telecomunicaciones y por lo menos debe haber uno por piso siempre y cuando no se excedan los 90 m. especificados para el cableado horizontal.

2.1.1.3 Cuarto de Equipos

Es el lugar donde se ubican los principales equipos de telecomunicaciones tales como centrales telefónicas, switches, routers y equipos de cómputo como servidores de datos o video. Además éstos incluyen uno o varias áreas de trabajo para personal especial encargado de estos equipos. Se puede decir entonces que los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y complejidad del equipo que contienen.

- El Área de Distribución Principal (MDA): Es el espacio central donde se encuentra el punto de distribución para el sistema de cableado estructurado en el centro de datos, además de alojar los equipos de core, como son los routers, switches de LAN o PBX. En un Centro de Datos pequeño puede incluir las terminaciones del cableado horizontal (HDA).
- El Área de Distribución Horizontal (HDA): Es el espacio que apoya a las áreas de cableado de equipos de distribución, donde se encuentra los equipos activos.
- El Área de Distribución de Equipos (EDA): Son los espacios asignados para el equipo final, incluidos los sistemas y equipos de comunicaciones. Contienen los gabinetes o bastidores que contienen los patch panels correspondientes a las terminaciones del cableado horizontal.

- El Área de Distribución Zonal (ZDA): Es un área opcional, en donde se colocan los equipos que no deben permitir terminaciones en el patch panel, sino más bien conectarse directamente a los equipos de distribución.

2.1.2 Ubicación del Centro de Datos para TIER 3

La ubicación de un Centro de Datos, es un factor determinante en su correcto funcionamiento, puesto que de esto depende la mayor protección y seguridad de una de las áreas más importantes de cualquier organización.

El Centro de Dato en TIER 3 debe estar en una zona empresarial de fácil acceso, cercano a vías de comunicación permitiendo el rápido acceso y libre de interferencias electromagnéticas.

2.1.3 Suelo Técnico, Paredes y Techos

En un Centro de Datos se debe crear un espacio para permitir el paso del cableado eléctrico, el sistema de detección, extinción de incendios y el acceso para el mantenimiento de equipos.

De esta forma permitirá la libre circulación del aire de los equipos de climatización por impulsión bajo el falso suelo, para la refrigeración de los servidores alojados en el Centro de Datos.

Todas las zonas contarán con este elemento, que deberá tener las siguientes características:

- Incluir fijación de pedestales al suelo existente mediante tornillería, instalando estructuras entre pedestales, colocando y nivelando las placas, así como colocación final de rejillas de refrigeración según distribución de la sala.
- El diámetro de la varilla pedestal no será inferior a 16 mm. e irá dotado de tuerca y contratuerca para el bloqueo de la altura requerida.
- Baldosa de 600 x 600 mm. formada por un núcleo de madera prensada de alta densidad (no inferior a 720 kg/m³) y un espesor mínimo de 35-40 mm.
- Bordes de placa de PVC de grosor 0,60 mm.
- El acabado superior de la placa debe ser de material antiestático.
- El revestimiento inferior estará constituido por una cubierta de acero galvanizado de al menos 0,5 mm. de espesor que además de crear una barrera al fuego y la humedad, constituye una armadura equipotencial que favorece la continuidad eléctrica del pavimento, ayudando a la eliminación de electricidad estática.
- Peso soportado 12 kN.

- Se suministrará rampa portátil de 900 mm. de ancho, 2000 mm. de largo para salvar la altura de entrada al Centro de Dato con capacidad para 1000 Kg.
- Las bases y cabezal (gatos) del piso falso deben ser en hierro acerado, totalmente rígido y altura graduable para permitir la nivelación del piso. Se debe implementar un sistema con arrastramiento transversal y longitudinal (stringers) sobre las cabezas de los gatos esto con el fin de amarrar, afianzar las bases y ofrecer una mayor estabilidad al piso.
- El sistema debe quedar perfectamente nivelado y no serán aceptadas baldosas o áreas que tengan libertad de desplazamiento horizontal.
- La altura libre entre el piso falso y el techo falso debe estar entre 2.70 y 3.30 metros para permitir la movilidad del aire.

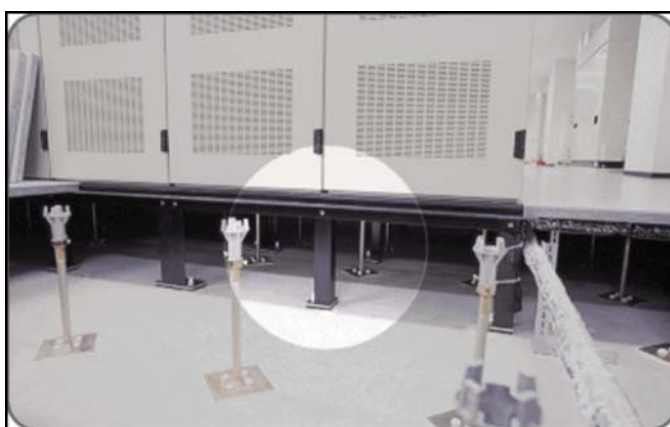


Figura 2.1.3 Piso falso del Centro de Datos

Paredes y Techo

- El techo real deberá pintarse, así como las placas del techo falso y los amarres.
- Las paredes irán con pintura plástica, inflamable y lavable para poder limpiarlas fácilmente y evitar la erosión.

Puertas de acceso

- La puerta de acceso debe tener como mínimo 95cm de ancho y abrir hacia afuera.
- Tener en cuenta las dimensiones máximas de los equipos si hay que atravesar puertas y ventanas de otras dependencias.
- Crear rutas de salida en caso de emergencia.

2.1.4 Diseño Eléctrico

Todos los sistemas de tier 3 en un Centro de Datos, deberán ofrecer un mínimo de redundancia N+1 y para esto se debe incluir generadores de energía o grupo electrógeno, unidades de UPS con sus respectivas baterías, sistema de distribución de energía (PDU), tablero de distribución y un switch de transferencia de energía (ATS). Este nivel de redundancia tier 3 cuenta con un suministro de energía redundante y de disponibilidad continua, esto puede ser obtenido por

cualquiera de las dos fuentes de suministro de energía. Los alimentadores y tableros de distribución son de doble vía, es decir, si existe una falla o mantenimiento de un cable o un panel no cause la interrupción de las operaciones.

La redundancia deber proporcionar suficiente energía para permitir el aislamiento de cualquier elemento del equipo mecánico o eléctrico que sean necesarias para el mantenimiento esencial, sin afectar los servicios que se proporcionan con el enfriamiento. (Ver anexo TIA 942)

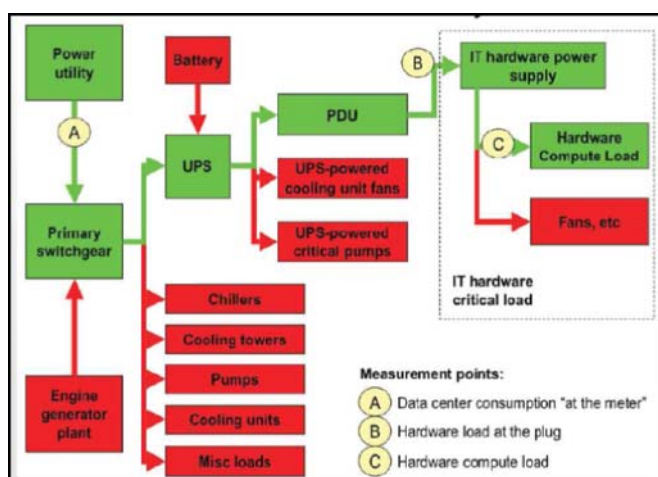


Figura 2.2 El Flujo Eléctrico De Poder

2.1.5 Sistema Eléctrico

El sistema eléctrico estará compuesto por equipos y dispositivos necesarios para suministrar la alimentación eléctrica del Centro de Datos y así garantizar mediante la redundancia oportuna y las

conmutaciones pertinentes, el suministro continuo al equipamiento del Centro de Datos.

Los equipos a utilizar son:

1. Switch de Transferencia Automática(ATS)
2. Grupo Electrónico o Generador de Energía
3. Unidad de Almacenamiento de Energía(UPS)
4. Unidad de Distribución de Energía (PDU)
5. Cuadros, cableado de potencia, canalización y conmutación.

2.1.5.1 Switch de Transferencia Automática (ATS)

El ATS o switch de transferencia automática proporciona una transición sin fisuras entre una fuente de energía primaria y una fuente de energía secundaria. También mantiene el suministro de energía de manera continua monitoreado por el PLC (sistema del controlador lógico programable).

El ATS cuenta con panel de control de baja tensión del cual detecta cualquier anomalía en el flujo primario de energía para lo cual se conecta automáticamente con el generador de reserva que al instante arranca en funcionamiento.

Una vez que la frecuencia y la tensión se estabilizan, el sistema se transfiere a la acometida eléctrica en cuanto se encuentra disponible y la señal de arranque del generador es descontinuada.

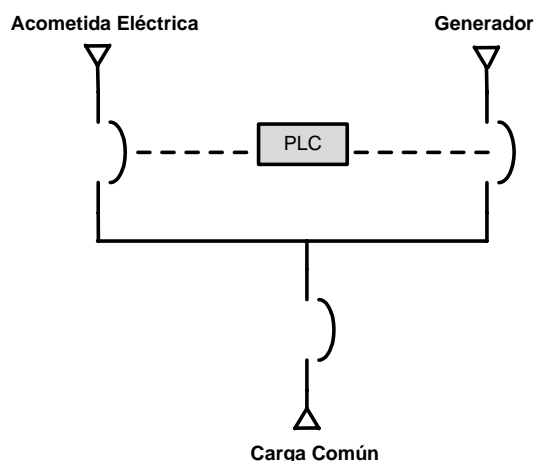


Figura 2.3 Esquema de configuración Principal - Generador

El ATS-NW Clase 2700, minimizan la interrupción de corriente eléctrica al transferir la carga de la fuente normal a una fuente alternativa cuando la fuente normal está temporalmente fuera de servicio.

Este sistema de transferencia puede incluir interruptores automáticos fijos o removibles, y son controlados por un PLC (controlador lógico programable) que contienen fuentes redundantes de alimentación de control (UPS) dentro del mismo equipo.

Para la instalación del ATS este va a estar ubicado en la sala de centro de operaciones y se conectara de forma directa con la acometida eléctrica y con el generador de voltaje por medio de los bloques conectores que el ATS tiene en la parte posterior.

Todo este cableado con las fuentes de energía y con el UPS debe llevarse por tuberías de aluminio conocidas como tubo conduit que van a estar empotradas en la pared del cuarto.



Figura 2.4 Switch de Transferencia Automática (ATS-NW Clase 2700)

2.1.5.2 Grupo Electrónico o Generador de Energía

El Grupo Electrónico o Generador de Energía es el encargado de suministrar la alimentación eléctrica de manera mecánica en caso de existir interrupción en la misma red.

La ubicación física será en un punto próximo al Centro de Datos y se deberá tener en cuenta la conducción y canalización eléctrica y de comunicaciones necesaria, así como cualquier elemento constructivo necesario.

El grupo electrónico que se utilizara en nuestra data center tendrá como mínimo las siguientes características:

- Grupo electrógeno automático de 800 KW/1000Kva a 50 - 60 Hz.
- Motor diesel de 4 tiempos, con inyección directa, turboalimentado, y enfriado por agua.
- Tiempo de arranque aproximado 30 seg.
- Tensión de 230/400 V ajustable y de 3 fases
- Protección tipo IP-21/23.

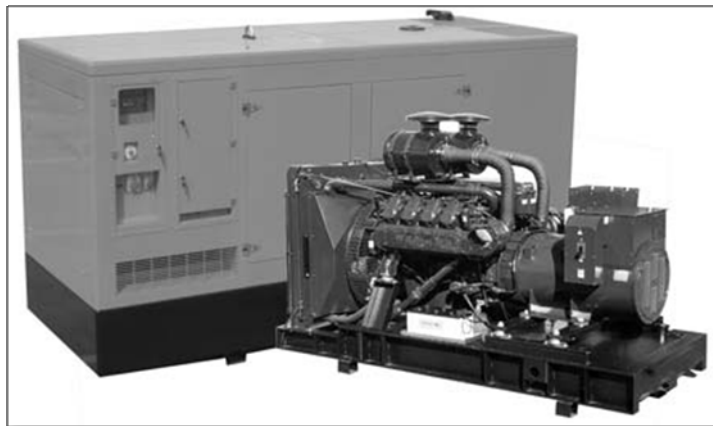


Figura 2.5 Grupo Electrónico - TIER III

2.1.5.3 Unidad de Almacenamiento de Energía (UPS)

El UPS o SAI, es un equipo de alimentación ininterrumpida con protección redundante N+1, de alto rendimiento de potencia y autonomía escalable.

Los UPS permiten la ampliación de potencia insertando módulos o baterías externas que se conectaran paralelamente, en caliente, sin tener que parar el UPS ni pasarlo a Bypass.

Algunos UPS del mercado distribuye la energía en el momento que detecta un disturbio o variación de voltaje por algún defecto en el flujo eléctrico, este equipo viene con un tablero de mando para el operador, lo cual provee información de estado básico operacional y de alarma.

EL voltaje de entrada y de salida es de 480 V - 3 W trifásico.

Y para una optimización y el buen desempeño del UPS y el gabinete de Batería hay que mantenerlos a una temperatura dentro del rango de 74-80 ° F, (23-27 ° C).



Figura 2.6 Unidad de Almacenamiento de Energía (UPS NX)

2.1.5.4 Unidad de Distribución de Energía (PDU)

Permiten la distribución de energía de manera eficiente, confiable y ordenada al interior de los racks donde se alojan los equipos del centro de datos. Sus presentaciones son en formato vertical como armarios y de forma horizontal permitiendo su montaje en racks que

cumplan los estándares de la EIA/TIA. Cuenta también con unidades básicas, que pueden ser monitoreadas y administradas en forma remota desde la red para conocer el estado y poder controlar individualmente cada una de las salidas.

Algunas equipos PDU utiliza un doble transformador de protección y el grado de tierra del equipo garantiza que los interrupciones eléctricas como ruido, tales como EMI y RFI hacer no afecta los equipos informáticos la operación. Esto permite que la PDU pueda suministrar energía de alta calidad rendimiento.

El PDU del Centro de Datos debe contar con las siguientes características:

- Transformador hecho de cobre de doble blindaje con armónicos de mitigación disponible.
- Sistema de monitoreo lo cual nos permitirá ver el consumo y calidad de la energía distribuida.
- Voltaje de entrada y salida de 208V, 480V o 600V trifásico de 60 Hz.



Figura 2.7 Unidad de Distribución de Energía (PDU)

2.1.6 Alumbrado

En la Sala de Computo como las zonas comunes están equipadas con luminarias fluorescentes. Las luminarias disponen balasto electrónico que tiene como función de limitar la corriente eléctrica que circula por una lámpara de modo de suministrarle la corriente y la tensión necesarias para su operación.

Cada balastro eléctrico tiene una potencia que consumirá y el número de tubos de fluorescencia.

El sistema de iluminación debe ser mediante pantallas con luminarias fluorescentes uniforme para evitar reflejos en los equipos deben estar puestas de forma paralela en los respectivos cuartos del centro de dato.

Las salas deben tener la misma intensidad de luz y conseguir un nivel de luz 200 (lux.) de forma uniforme que es lo exigido en la norma TIA – 942 y con lo cual se evitará la incidencia directa del sol sobre los equipos.



Figura 2.8 Balastro Eléctrico



Figura

2.9

Lámpara de 3 tubos fluorescente

2.1.7 Sistema de puesta a tierra

Establecido en el estándar ANSI/TIA/EIA-607, es un componente importante de cualquier sistema de cableado estructurado moderno. El gabinete deberá disponer de una toma de tierra, conectada a la tierra general de la instalación eléctrica, para efectuar las conexiones de todo equipamiento. El conducto de tierra no siempre se halla indicado en planos y puede ser único para ramales o circuitos que pasen por las mismas cajas de pase, conductos ó bandejas.

Los cables de tierra de seguridad serán puestos a tierra en el subsuelo. Se instalará una puesta de tierra para uso exclusivo de la red eléctrica.

TGB (Telecommunications Grounding Busbar) es la barra de tierra ubicada en el armario de telecomunicaciones o en la sala de equipos. Sirve de punto central de conexión de tierra de los equipos de la sala.

TMBG (Telecommunications Main Ground Busbar) es la barra principal de tierra. Es la que se conecta a la tierra del edificio y actúa como punto central de conexión de los TGB.

2.1.8 Sistema de cableado

La administración del sistema de cableado incluye la documentación de los cables, terminaciones de los mismos, paneles de parcheo,

armarios de telecomunicaciones y otros espacios ocupados por los sistemas. La norma TIA/EIA 606 proporciona una guía que puede ser utilizada para la ejecución de la administración de los sistemas de cableado.

El alcance de la norma TIA/EIA 606 son:

- Topología.
- La distancia máxima de los cables.
- El rendimiento de los componentes.
- La toma y los conectores de telecomunicaciones.

2.1.8.1 Cableado Horizontal

Se emplea el término horizontal por la ubicación del cableado de manera horizontal entre los pisos y techos de un edificio. El sistema de cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende del área de trabajo al cuarto de telecomunicaciones. El cableado horizontal incluye los cables horizontales, las tomas/conectores de telecomunicaciones en el área de trabajo, la terminación mecánica y las interconexiones horizontales localizadas en el cuarto de telecomunicaciones.

2.1.8.2 Cableado Vertical

El propósito del cableado del backbone o vertical es proporcionar interconexiones entre cuartos de entrada de servicios de edificio,

cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas. El cableado vertical realiza la interconexión entre los diferentes gabinetes de telecomunicaciones y entre estos y la sala de equipamiento.

2.1.9 Sistema de Climatización

Con el fin de cumplir los requerimientos ambientales especificados por los fabricantes de Hardware, así como la norma TIA-942, es necesario mantener en la sala una temperatura de $21^{\circ} \pm 1^{\circ} \text{C}$ y una humedad relativa del 50% con una tolerancia de $\pm 5\%$.

El sistema de climatización será redundante, suministrando dos equipos de características idénticas. La potencia de cada uno será suficiente para mantener la temperatura y humedad dentro de la sala de acuerdo con una ocupación de la sala del 100%.

Los dos equipos podrán trabajar en alternancia de acuerdo a los ciclos de tiempo establecidos.

Para establecer la climatización en la sala de computo se debe tener en cuenta la densidad de potencia en el centro de datos esto se lo

representa muy a menudo como vatios por metro cuadrado o vatios por rack.

Pero en un centro de datos donde habrá racks con diferentes potencias distribuidos entre las hileras de rack la densidad de potencia tendrá un aumento significativo.

Teniendo en cuenta que cada rack consume un promedio de 10KW y que la superficie de la sala de cómputo es de 15 x 10 m² se debe seguir las siguientes recomendaciones para un buen rendimiento en la refrigeración:

- Debe haber un suministro de 2.500 pies cúbicos por minuto (1.180 L / s) de aire fresco para cada rack.
- Desfogue de 2.500 pies cúbicos por minuto (1.180 L / s) de aire caliente saliente de la sala de computo.
- Mantener el aire caliente de saliente lejos de la entrada de aire equipo.
- Proporcionar una redundancia y sin interrupciones a los equipos de refrigeración.

Para lograr estas recomendaciones se debe haber implementado la instalación del piso falso en la sala de cómputo para la entrada y salida del aire caliente.

Para la climatización del centro de datos se utilizara el CRAC.

2.1.9.1 Aire Acondicionado del Cuarto de Computadoras(CRAC)

El Equipo de Aire Acondicionado o controladores de aire son un elemento básico de diseño de centros de datos, proporcionando la temperatura precisa y la humedad para entornos de misión crítica, el CRAC proporciona el intercambio de calor recurrente al aceptar la energía térmica generada por los equipos informáticos, después refrigerándolo y regresando de nuevo a los equipos informáticos. El diseño del CRAC está dispuesto para operar 24x7x365.

Para satisfacer las demandas de refrigeración de los equipos informáticos. El CRAC tienen las especificaciones de diseño para el suministro de aire, aire de retorno, y la temperatura del refrigerante, todo lo cual afecta su funcionamiento y rendimiento.

El funcionamiento del CRAC incluye cuatro Evapco 500 toneladas, circuito cerrado de torres de refrigeración por agua y bombas de agua del condensador. Las torres de refrigeración proporcionan el agua fría a los aires acondicionados del cuarto de computadoras (CRAC) y a otras habitaciones utilizando las bombas de calor que se encuentran instaladas en todo el edificio. Cada torre de refrigeración tiene dos ventiladores de dos velocidades y una bomba de agua de circulación. El circuito de agua condensada se compone de cuatro bombas, con

tres bombas que funcionan a la vez. La planta de la torre de refrigeración está diseñada para un despidido del 15 por ciento.

El centro de datos está en un piso elevado, a través del cual se hace circular aire de refrigeración a través de las unidades CRAC.

Cuando la densidad de potencia es superior a 10 kW por rack, el carácter imprevisible del flujo de aire se convierte en el problema dominante. Por lo cual la solución de este problema es acortar la ruta del flujo de aire entre el sistema de refrigeración y las rejillas usando el criterio de pasillos fríos y pasillos calientes.

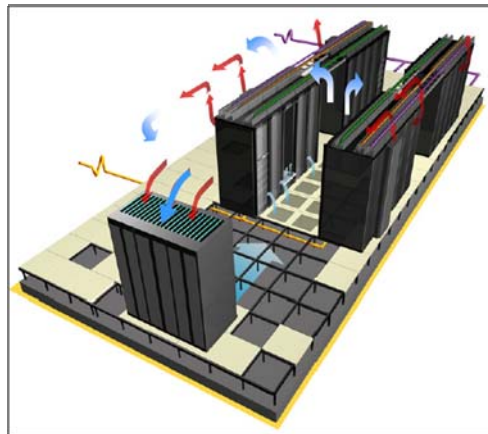


Figura 2.10 Aire Acondicionado del Cuarto de Computadoras - CRAC

Criterio de Pasillo Fríos y Pasillos Calientes

- Disponemos de líneas de servidores y equipos de red con la orientación de dichos equipos en forma alternada.
- De esta manera si nos ubicamos en un pasillo tendremos a ambos lados el frente de los equipos o la parte trasera de los mismos.

- Las líneas de piso falso perforado quedaran en los pasillos con vista al frente de los equipos
- El techo con ventilación forzada quedara en los pasillos con vista a las partes traseras de los equipos.

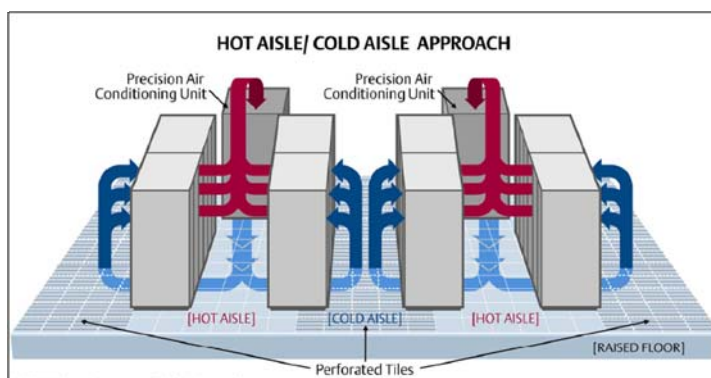


Figura 2.11 Criterio de Pasillos Fríos y Pasillos Calientes

2.1.9.2 Contención de pasillo caliente para configuraciones de alta densidad.

Es un sistema de contención basado en la fila de alta densidad diseñada para maximizar la previsibilidad en la fila de refrigeración, capacidad y eficiencia. La mezcla de aire caliente y de corrientes frías en el centro de datos reduce la disponibilidad de los equipos informáticos. El sistema de contención de pasillo caliente garantiza una distribución adecuada del aire por la oferta completa separación y caminos de retorno de aire. El pasillo caliente está cerrado con puertas y techo de tejas transparentes que extienden la anchura del pasillo

caliente. Los azulejos del techo están disponibles tanto para 19 "y 23" bastidores. Dos equipos de rack completo con azulejo del techo y el hardware están disponibles para una futura expansión.



Figura 2.12 Contención de pasillos calientes

2.1.9.3 Sistema de Climatización de las Salas Internas

El sistema de aire acondicionado debe ser capaz de lograr que las suites, la sala general, cuarto de proveedores, cuarto de telecomunicaciones, cuarto de cuarentena, sala de UPS y baterías, se mantengan dentro de los siguientes parámetros medioambientales, la temperatura es $21 \pm 2^{\circ}\text{C}$

2.1.10 Detección de Agua en Piso Falso

Cada equipo climatizador de sala dispone de un sistema de detección de agua en la parte inferior de la máquina que envía una señal de alarma al sistema de monitorización en caso de agua.

2.1.11 Protección Contra Incendios

Sistemas base agua son eficaces para la protección de estructuras en general. Pero dentro de un centro de datos, el agua va a destruir el equipo. Dependiendo del gas utilizado, un sistema sin agua puede proteger el equipo, sino que sería perjudicial para los seres humanos o el medio ambiente.

Un gas puede proteger el equipo durante un incendio, pero deja un residuo que daña el equipo.



Figura 2.13 Gas Protección contra Incendios

2.1.12 Rack

Los racks están equipados con barandillas laterales de montaje para que el equipo y el hardware estén montados.

Los racks deben tener la altura suficiente para acomodar el equipo revisto, incluyendo el cableado en la parte delantera y / o trasera, los cables de alimentación, el hardware de administración de cables, y los enchufes múltiples. A fin de garantizar flujo de aire adecuado y proporcionar un espacio adecuado para las tiras de energía y cableado, considere el uso gabinetes que por lo menos 150 mm (6 pulgadas) más profundo o más ancho que profundo.



Figura 2.14 Rack

2.1.12.1 Ubicación de Equipos

El equipo debe ser colocado en los armarios y racks, con la entrada de aire frío en la parte delantera del armario o rack, y el aire caliente de escape por la parte trasera. Inversión del equipo en el armario de distorsionar el correcto funcionamiento de los pasillos fríos y calientes.

Paneles en blanco deben ser instalados en un rack sin utilizar el espacio del armario para mejorar el funcionamiento de los pasillos fríos y calientes. Las baldosas del suelo perforada al acceso debe estar ubicado en los pasillos fríos en lugar de en los pasillos calientes para mejorar el funcionamiento de los pasillos fríos y calientes. Además, las bandejas de cables deben ser colocados en los pasillos fríos por debajo de las baldosas perforadas.

Cada armario o rack está compuesto de equipos de conectividad como paneles de conexión, router, switch, servidores y dispositivos de almacenamiento.

A continuación se detallara cada equipo que va instalado en el rack.

2.1.12.1.1 Paneles de Conexión

Los paneles de conexión también conocidos como patch panel son una pieza vital para los equipos montados en los gabinetes o rack, ya que permite gestionar las conexiones cruzadas con facilidad.

Existen diferentes tipos de paneles de conexión como son de 12, 24 o 48 puertos los cuales suelen usar un tipo de cableado estándar Cat5 o Cat6.

También existen paneles de fibra óptica de parches conocidos como tableros de distribución de fibra cuya función es dar por terminado el cableado de fibra óptica y facilitar el acceso a fibras individuales del

cable de conexión cruzada. El panel de conexión de fibra puede utilizar cables de conexión de fibra de conexión cruzada, conectarse a equipos de comunicaciones de fibra óptica o prueba de las fibras individuales en el cable de fibra.

Un panel de conexión de fibra consiste de una serie de adaptadores SC duplex, adaptadores de híbridos, o jacks.



Figura 2.15 Panel de Conexión

2.1.12.1.2 Enrutadores (Router)

Es un dispositivo de hardware para interconexión de redes informáticas que opera en la capa tres y permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Otra función de los enrutadores es manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra. Como no todas las redes pueden manejar el mismo tamaño de

paquetes de datos, los enrutadores deben fragmentar los paquetes de datos para que puedan viajar libremente.

Se puede distinguir cuatro tipos de enrutadores:

- **Enrutador de Acceso:** Los enrutadores de acceso, incluyendo SOHO, se encuentran en sitios de clientes como son de sucursales que no necesitan de enrutamiento jerárquico de los propios. Normalmente, son optimizados para un bajo costo.
- **Enrutador de Distribución:** Los enrutadores de distribución agregan tráfico desde enrutadores de acceso múltiple, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa. Los enrutadores de distribución son a menudo responsables de la aplicación de la calidad del servicio a través de una WAN, por lo que deben tener una memoria considerable, múltiples interfaces WAN, y transformación sustancial de inteligencia.

También pueden proporcionar conectividad a los grupos de servidores o redes externas. En la última solicitud, el sistema de funcionamiento del enrutador debe ser cuidadoso como parte de la seguridad de la arquitectura global. Separado del enrutador puede estar un Cortafuegos o VPN concentrador, o el enrutador puede incluir estas y otras funciones de seguridad. Cuando una empresa se basa

principalmente en un campus, podría no haber una clara distribución de nivel, que no sea tal vez el acceso fuera del campus.

En tales casos, los enrutadores de acceso, conectados a una red de área local (LAN), se interconectan a través del Core routers.

- Enrutadores de Núcleo: En las empresas, el core router puede proporcionar una "columna vertebral" interconectando la distribución de los niveles de los enrutadores de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto.

Cuando una empresa está ampliamente distribuida sin ubicación central, la función del Core router puede ser asumido por el servicio de WAN al que se suscribe la empresa, y la distribución de enrutadores se convierte en el nivel más alto.

- Enrutadores de Borde: Los routers de borde enlazan sistemas autónomos con las redes troncales de Internet u otros sistemas autónomos, tienen que estar preparados para manejar el protocolo BGP y si quieren recibir las rutas BGP deben poseer mucha memoria.

2.1.12.1.3 Conmutadores (Switch)

Es un dispositivo digital lógico de interconexión de redes de computadores que opera en la capa del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LAN.

Se tiene una gran variedad de conmutadores con distintas características y por ello distintos criterios de clasificación, los cuales son:

Por el Tipo de Administración:

a. Conmutadores Administrables

Aquellos que permiten cierta funcionalidad de administración del switch.

b. Conmutadores no Administrables

Son aquellos que no permiten ninguna o escasa funcionalidad de configuración y administración.

Por la Capacidad:**a. Conmutadores apilables**

Permiten agrupar varias unidades sobre un bus de expansión, el bus debe proporcionar suficiente ancho de banda para manejar comunicaciones full-duplex. Se recomienda comprarlos del mismo fabricante para evitar problemas de administración global e intercomunicación entre los Conmutadores. Por lo general son Conmutadores administrables.

b. Conmutadores no apilables

Son aquellos que no soportan un bus de expansión.

Por la Modularidad:**a. Conmutadores modulares**

Tienen la capacidad de soportar la agregación de puertos, como nuevos módulos, por lo general son Conmutadores multicapa por trabajar en capa 2, 3, u otros superiores (Modelo OSI). Generalmente utilizados como Conmutadores de troncal (backbone, columna vertebral de la red). Por lo general son Conmutadores administrables.

b. Conmutadores no modulares

No poseen ninguna capacidad de agregación de módulos.

Por la Capacidad de Tráfico:

Se clasifican por las velocidades con las que trabajan, siendo estas 10, 100 y 1000 Mbps., los de mayor velocidad por lo general son utilizados como switch de troncal (backbone), pueden ser modulares y administrables.

2.1.12.1.4 Servidores

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

En la siguiente lista hay algunos tipos comunes de servidores:

- Servidor de archivo: Es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red.
- Servidor de correo: Almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.
- Servidor de la telefonía: Realiza funciones relacionadas con la telefonía, como es la de contestador automático, realizando las funciones de un sistema interactivo para la respuesta de la voz, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet, p. ej., la entrada excesiva de la voz sobre IP (VoIP), etc.
- Servidor proxy: Realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas

operaciones (por ejemplo: prefetching y depositar documentos u otros datos que se soliciten muy frecuentemente), también proporciona servicios de seguridad, o sea, incluye un cortafuegos. Permite administrar el acceso a internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

- Servidor del acceso remoto (RAS): Controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes o reconoce la petición de la red y realiza la autenticación necesaria y otros procedimientos necesarios para registrar a un usuario en la red.
- Servidor de uso: Realiza la parte lógica de la informática o del negocio de un uso del cliente, aceptando las instrucciones para que se realicen las operaciones de un sitio de trabajo y sirviendo los resultados a su vez al sitio de trabajo, mientras que el sitio de trabajo realiza el interfaz operador o la porción del GUI del proceso (es decir, la lógica de la presentación) que se requiere para trabajar correctamente.
- Servidor web: Almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos

(conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

- Servidor de Base de Datos (database server): Provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor. También puede hacer referencia a aquellas computadoras (servidores) dedicadas a ejecutar esos programas, prestando el servicio.
- Servidor de reserva: Tiene el software de reserva de la red instalado y tiene cantidades grandes de almacenamiento de la red en discos duros u otras formas del almacenamiento (cinta, etc.) disponibles para que se utilice con el fin de asegurarse de que la pérdida de un servidor principal no afecte a la red. Esta técnica también es denominada clustering.

Algunas compañías de red han desarrollado un tipo de servidor llamado servidor blade.

El servidor blade es un tipo de computadora para los centros de proceso de datos específicamente diseñada para aprovechar el espacio, reducir el consumo y simplificar su explotación.

Su diseño es adecuado para un montaje en bastidores. Cada servidor blade es una delgada "tarjeta" que contiene únicamente microprocesador, memoria y buses. Por lo que no disponen de fuente de alimentación ni tarjetas de comunicaciones.

Estos elementos más voluminosos se desplazan a un chasis que se monta en el bastidor ocupando únicamente de cuatro (4U) a seis alturas (6U). Cada chasis puede albergar del orden de dieciséis "tarjetas" o servidores blade (según fabricante). El chasis lleva integrados los siguientes elementos, que son compartidos por todos los servidores:

- Fuente de alimentación: redundante y hot-plug.
- Ventiladores o elementos de refrigeración.
- Conmutador de red redundante con el cableado ya hecho, lo que simplifica su instalación.
- Interfaces de almacenamiento. En particular, es habitual el uso de redes SAN (Storage Area Network) de almacenamiento.

Además, estos servidores suelen incluir utilidades software para su despliegue automático. Por ejemplo, son capaces de arrancar desde una imagen del sistema operativo almacenada en disco. Es posible arrancar una u otra imagen según la hora del día o la carga de trabajo, etc.



Figura 2.16 Servidor y Servidor Blade

2.1.12.1.5 Matriz de Discos

Las matrices de discos son grupo de dos (o más) unidades de disco duros físicos con múltiples enlaces entre ellos que aparecen ante el sistema como un solo disco. La ventaja de una matriz es proporcionar un mejor rendimiento de flujo y/o una tolerancia a los fallos en los datos.

Un mejor rendimiento se logra compartiendo la carga de trabajo en paralelo entre varios discos físicos. La tolerancia a los fallos se logra mediante una operación redundante de datos donde si uno (o más) discos fallan o tienen un fallo de sector, se puede encontrar una copia en espejo de los datos en otro (u otros) disco(s).

La tecnología de matriz de discos RAID (Redundant Array of Independent Disks), los arreglos de discos RAID utiliza en una serie de configuraciones opcionales ayudando a la redundancia de datos, escribe de manera que si un archivo está dañado o almacenado en un clúster no válido o el disco, puede ser sustituido de inmediato y transparente de otro disco de la matriz. Los RAID también permite el intercambio en caliente de discos malos y una mayor flexibilidad en el almacenamiento escalable.

Existen diferentes tipos de RAID:

- RAID 0: Disk Striping “La más alta transferencia, pero sin tolerancia a fallos”.
- RAID 1: Mirroring “Redundancia. Más rápido que un disco y más seguro”
- RAID 0+1/ RAID 0/1 ó RAID 10: “Ambos mundos”
- RAID 2: “Acceso paralelo con discos especializados. Redundancia a través del código Hamming”
- RAID 3: “Acceso síncrono con un disco dedicado a paridad”
- RAID 4: “Acceso Independiente con un disco dedicado a paridad.”
- RAID 5: “Acceso independiente con paridad distribuida.”
- RAID 6: “Acceso independiente con doble paridad ”Ver el anexo D de la Norma TIA-942.

2.1.13. Dispositivos o Módulos de Servicios de Seguridad

El Centro de Datos dispone de estrategias de seguridad la cual brinda una protección adecuada a la información por lo cual resulta un éxito para los servicios brindados por el mismo.

El centro de datos cuenta con dos zonas de seguridad divididas en seguridad perimetral y seguridad interna, para el caso del Centro de Datos este va a contar con seguridad interna que va a estar compuesta de módulos o tarjetas físicas que van dentro del switch de agregación en el área de Distribución Horizontal estos módulos

agregan funcionalidad de servicio de seguridad a la infraestructura del Centro de Datos.

Algunas marcas de switch vienen con ranuras para la agregación de los módulos y cada modulo de servicio será escogido por el usuario dependiendo del servicio que se va a ofrecer.

También estos módulos son dispositivos físicos agregados al gabinete. A continuación se enlistara los módulos de servicio de seguridad o dispositivos de seguridad:

- **Modulo Firewall:** Un firewall es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra evitando que los intrusos puedan acceder a información confidencial.
- **Modulo Firewall de Aplicación Web (WAF):** Es una forma de servidor de seguridad que controla la entrada , salida y/o acceso a una aplicación o servicio. Funciona mediante la vigilancia y bloquea la entrada, salida o servicio de llamadas al sistema que no cumplan con la política de configurar el servidor de seguridad.
- **Módulos de Detección de Intrusos (IDS/IPS):** Es un paso avanzado de seguridad perimetral este dispositivo ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **Módulos de Análisis de Redes:** Proporciona el servicio de monitoreo de la red reuniendo datos estadísticos del tráfico de la red para el análisis de tiempo real y buscar una solución óptima.
- **Modulo de IP Segura:** Proporciona protección a los paquetes IP, la seguridad de IP autentica los equipos y cifra los datos para su transmisión entre host en una red, intranet o extranet.
- **Modulo de equilibrio de carga:** Mejora la disponibilidad y la escalabilidad de las aplicaciones de servidor de Internet, como las utilizadas en Web, FTP, servidores de seguridad, proxy, VPN y otros servidores con funciones cruciales.
- **Modulo de Gateway XML:** Es un conjunto integrado de componentes que ofrece una solución fácil de usar con un único punto de entrada a toda la información de negocios de la empresa. Permite a los usuarios para encontrar decisiones empresariales, de forma rápida y sencilla.

2.2 Tecnología que Soporta el Cloud Computing

2.2.1 Arquitectura del Cloud Computing

Es el conjunto de capas que se encuentran acopladas entre sí para brindar la funcionalidad del sistema, en este caso la arquitectura de Cloud Computing es similar a la arquitectura de red, desde un nivel

físico hasta un nivel de aplicación. En [24] se menciona una arquitectura genérica para Cloud Computing, que tienen las siguientes capas mencionadas de abajo hacia arriba:

Aplicación: incluye servicios basados en web y software como servicio.

Plataforma: incluye componentes de aplicación como servi

Infraestructura: incluye software de plataforma como servicio.

Virtualización: incluye infraestructura virtual como un servicio.

Recursos físicos: incluyen elementos como servidores, almacenamiento y red.

Tabla 2.1 Arquitectura Cloud Computing

2.2.2 Niveles de Servicios

Los diferentes niveles de servicios que componen a Cloud Computing son IaaS, PaaS, SaaS.



Tabla 2.2 Niveles de Servicio Cloud Computing

2.2.1.1 SaaS (Software as a service)

La capa de "Software como servicio". [2] Provee la administración y hosting de aplicaciones con sus propios Datacenters, se maneja el término de múltiples inquilinos, por ejemplo Oracle CRM On Demand o Salesforce.

2.2.1.2 PaaS (Platform as a service)

La capa de "Plataforma como servicio". [2] Es entregar una plataforma de desarrollo de aplicaciones como un servicio para desarrolladores en la web. Generalmente se provee de herramientas tipo middleware, por ejemplo, Google AppEngine. Además de dicha entrega, también se ofrece un ambiente de ejecución como el servidor de aplicaciones.

2.2.1.3 IaaS (Infrastructure as a service)

La capa de "Infraestructura como servicio. [2] Es entregar tanto hardware como software como un servicio. El ejemplo más común es el *hosting*, el cual, nos provee de hardware como un servidor y de software como un *webserver*.

2.2.2 Tipos de Nubes

Con independencia del modelo de servicio utilizado (SaaS, PaaS, IaaS) hay cuatro formas principales en los que se despliegan los

servicios en la nube y según el tipo de relación entre el proveedor del servicio y los usuarios.

✓ **Nubes públicas:** Los usuarios finales no conocen qué trabajos de otros clientes pueden estar corriendo en el mismo servidor.

✓ **Nubes privadas:** Manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor.

✓ **Nubes híbridas:** Combinan los modelos de nubes públicas y privadas. El usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.

✓ **Nube comunitaria:** La infraestructura de esta nube la comparten diversas organizaciones y soporta una comunidad específica que tiene preocupaciones similares. Puede ser gestionada por las organizaciones o un tercero y puede existir en las instalaciones y fuera de ellas.

2.2.3 Virtualización del Cloud Computing

La virtualización es una tecnología de software orientado a ahorrar tiempo, dinero y energía; y usar una mejor manera el hardware disponible de la empresa. “Básicamente, la virtualización permite transformar hardware en software”, para crear una máquina virtual completamente funcional que puede ejecutar su propio sistema

operativo y aplicaciones de la misma forma que lo hace un ordenador “real”.

Varias máquinas virtuales comparten recursos de hardware sin interferir entre sí de modo que se puede ejecutar simultáneamente y de forma segura varios sistemas operativos y aplicaciones en un único ordenador.

Como medio de encapsulación de recursos físicos, la virtualización resuelve varios retos principales de administradores de centros de datos y entrega ventajas específicas, incluyendo:

- **Índice de utilización más altos:** A través de la virtualización, las cargas de trabajo pueden ser encapsuladas y transferidas a los sistemas inactivos o sin uso.
- **Consolidación de Recursos:** La virtualización permite la consolidación de múltiples recursos de TI. Más allá de la consolidación de almacenamiento, la virtualización proporciona una oportunidad para consolidar la arquitectura de sistemas, infraestructura de aplicación, datos y base de datos, interfaces, redes, escritorios, e incluso procesos de negocios, resultando en ahorros de costo y mayor eficiencia.
- **Uso/costo menor energía:** Utilizando virtualización para consolidar hace posible cortar el consumo total de energía y ahorrar dinero de una manera significativa.

- **Ahorro de espacio:** La virtualización puede aliviar la tensión mediante la consolidación de muchos sistemas virtuales en menos sistemas físicos.
- **Recuperación de desastre/continuidad de negocio:** La virtualización puede incrementar la disponibilidad de los índices del nivel de servicio en general y proporcionar nuevas opciones de soluciones para la recuperación de desastre.
- **Costo de operación reducida:** La virtualización puede cambiar el radio de servicio-a administración reducir la total carga de trabajo administrativo, y cortar el total de costos de operación.
- **Virtualización del Sistema Operativo:** El uso de virtualización de nivel-SO o partición (tal y como LPARs, VPARS, NPARS, Dominios del Sistema Dinámico, etc.) en las arquitecturas nube pueden ayudar a resolver algunos de los temas de seguridad central, y regulación que pudieran de otra manera dificultar la adopción del cloud computing.

2.3.1 Virtualización de Plataforma

Involucra la simulación de máquinas virtuales. La virtualización de plataforma permite ahorrar costes de sistemas y de gestión, consiguiendo un rendimiento adecuado, así como unificar plataformas heterogéneas y dispares, bajo un mismo sistema anfitrión.

Estos están implementados como hipervisores Tipo 1, los cuales corren directamente en el hardware, e hipervisores Tipo 2, los cuales corren a nivel superior de un sistema operativo tradicional.

2.3.2 Virtualización de Red

Involucra la simulación de recursos combinados, fragmentados o simples, permitiendo optimizar los recursos, como por ejemplo el almacenamiento, creando recursos virtuales disponibles desde un mismo recurso físico.

2.3.3 Virtualización de Aplicaciones

Encapsulando las mismas bajo un único paquete. Este método permite la portabilidad de aplicaciones sin riesgo a obtener conflictos de dependencias o de recursos propios de la misma o de terceras aplicaciones

3. DETALLE DEL DISEÑO

3.1. Recomendaciones del Cableado Estructurado

El cableado estructurado es un método para crear un sistema de cableado organizado, que puede ser fácilmente comprendido por los instaladores o administradores de red.

Para esto se debe tomar en cuenta tres recomendaciones, que nos ayudara garantizar efectividad y eficiencia para el desarrollo de nuestro Centro de Datos.

La primera recomendación es buscar una solución completa de conectividad de redes que abarque todos los sistemas que se van administrar.

La segunda recomendación es planificar teniendo en cuenta el crecimiento futuro de los diferentes equipos que se van instalar.

Y como recomendación final es conservar la libertad de elección de proveedores.

3.2 Ubicación del Centro de Datos

Como vimos en el capítulo 2, la ubicación del Centro de Datos debe ser en un lugar de terreno alto, de rápido acceso para el personal y libre de interferencia electromagnética.

Para esto se eligió la zona norte de la ciudad de Guayaquil en un terreno de 1500m² en el cual se establecerá las oficinas de personal administrativo, el centro de datos y el área de los generadores y sistema de climatización.

3.3 Cableado Horizontal

El cableado horizontal abarca la ruta de los cables que conecta desde el puerto de paneles ubicado en el cuarto de telecomunicaciones hacia las estaciones de trabajo.

La norma TIA/EIA 568-A exige que el cableado horizontal debe estar configurado en una topología en estrella. El cable seleccionado como medio de transmisión es cable UTP categoría 6, por las siguientes razones:

- No se requiere mucho ancho de banda en las estaciones de trabajo, de tal manera se descartó fibra óptica.
- Fibra óptica es de 10% a 15% más caro que el cable UTP, al igual que hardware que se requiere en fibra óptica.

Así mismo, el modulo hembra RJ-45 colocado en la estación de trabajo como el puerto de paneles deben corresponder a la misma familia de materiales que trabajen en categoría 6, por razones de compatibilidad y lograr maximizar el desempeño del sistema cableado. En nuestro Centro de datos se utilizara tuberías PVC de 2" empotradas en la pared y cajas de paso de 5"X5"x3" en las diferentes estaciones de trabajo para la obtención de puntos de red y voz, y una caja de paso de 6"X6"X3" detrás del gabinete que conduce los cables a los paneles de ponchado.

La distancia máxima del cableado horizontal es de 90m.

Se ha considerado la instalación de ocho puntos de acceso:

- 3 Cuarto de telecomunicaciones y entrada de servicios.
- 2 Sala de Centro de Operaciones.
- 2 Soporte Técnico.
- 1 Bodega

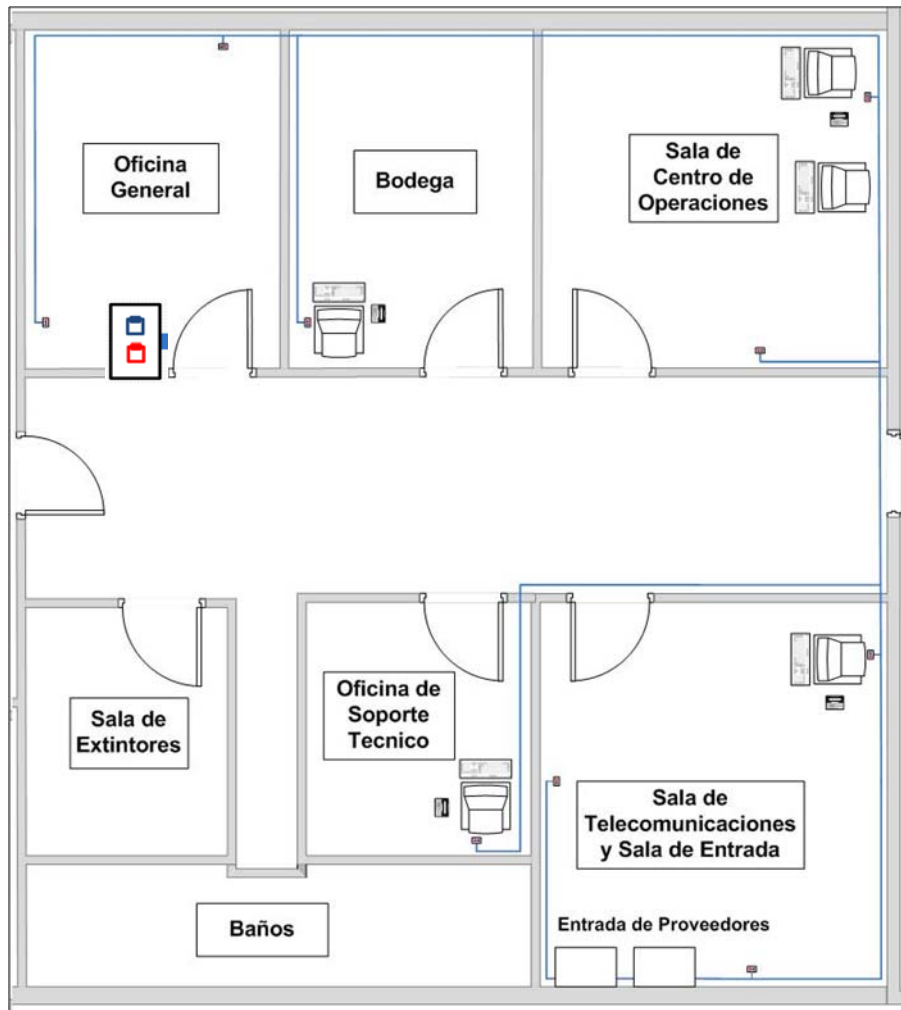


Figura 3.1 Cableado Horizontal del Centro de Datos

3.4 Cableado Vertical

La topología a implementarse es estrella tomando en cuenta la norma EIA/TIA 568A, debido que el rack ubicado en el cuarto telecomunicaciones debe enlazarse con el cuarto de cómputo y con el HUB que recibe la señal de los proveedores.

En nuestro Centro de Datos se implementara fibra óptica, la misma que se enrutará en una tubería metálica, para los diferentes enlaces. El tipo de fibra óptica a emplearse es Multimodo debido a que se trata del sistema de datos de redundancia, este cable de fibra por lo menos deberá contar con 4 hilos para lograr redundancia (dos hilos de transmisión y dos de recepción).

Cada extremo del cable de fibra debe llegar a una bandeja hecha especialmente para el manejo de las fibras ópticas, respetando los radios de curvatura.

La caja de paso tendrá una medida de 6"X6"X3" ubicada detrás del gabinete, la misma que llega al cableado horizontal.

El cableado vertical viajara desde la sala de telecomunicaciones hasta llegar al cuarto de cómputo por donde pasara por el área de distribución principal (MDA) siguiendo hasta el área de distribución horizontal (HDA) y por ultimo pasando por el área de distribución de equipos.

El camino que realizará el cableado vertical será por el techo falso del cuarto de computo donde este cableado será montado una bandeja metálica.

La bandeja metálica tendrá numerosos accesorios para llevar el cableado estos pueden ser como uniones entre bandejas, abrazaderas, soporte de techo falso.

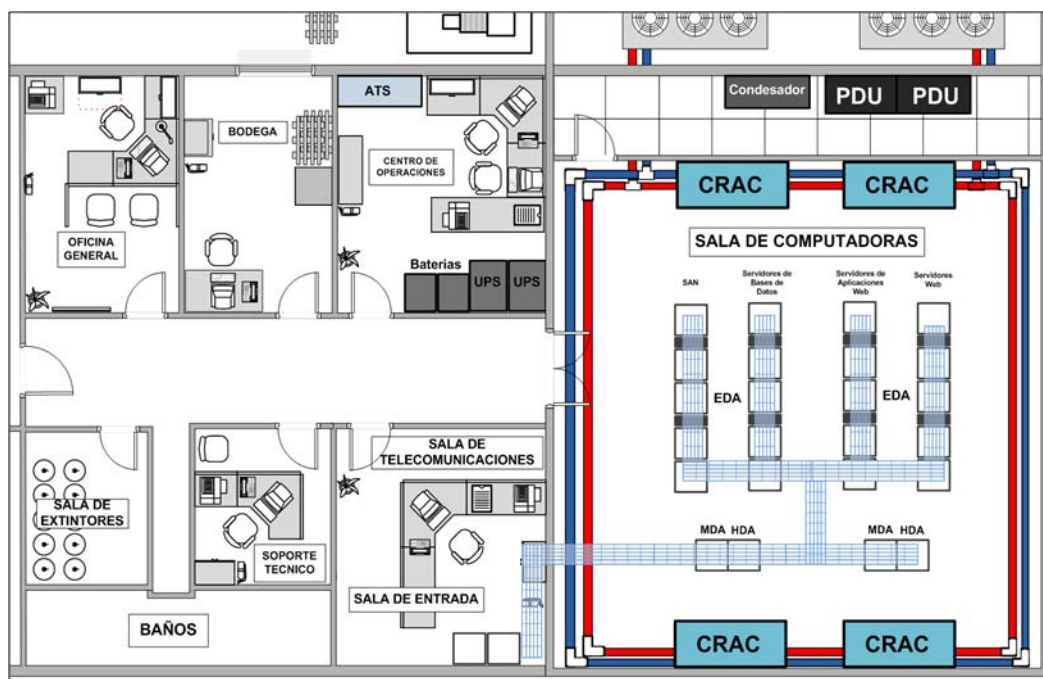


Figura 3.2 Bandeja metálica para el cableado vertical

3.5 Sala de Centro de Operaciones y Sala de Cómputo

3.5.1 Sala de Centro de Operaciones

Como revisamos en el capítulo 2, la Sala de Centro de Operaciones es donde se va a monitorear toda actividad del Cuarto de Cómputo, el Sistema de Climatización y el Sistema Eléctrico.

Para el diseño e implementación de la Sala de Centro de Operaciones los equipos e inmobiliario que van a hacer instalados son:

- 1 Escritorio
- 2 Sillas
- 2 Computadoras
- 1 Teléfono de mesa
- 1 Impresora

- 1 Porta Papeles
- 1 Anaquel Aéreo
- 2 Unidad de UPS de 160/220 kVA
- 2 Gabinete de Batería Externa de 49 pulgadas
- 1 ATS(Switch de Transferencia Automática)
- 2 Unidades de Distribución de Poder (PDU)
- 1 Extintor

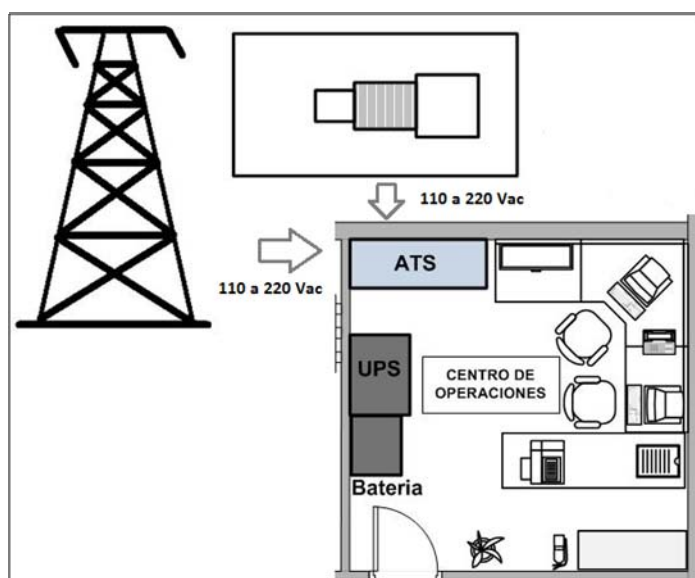


Figura 3.3 Cuarto de Centro de Operaciones

Como observamos en el gráfico, el ATS (Switch de Transferencia Automática) se instalara en la pared de la sala de centro de operaciones.

El ATS tendrá 2 conectores en la parte inferior del equipo para las líneas de los generadores de energía, la primera línea se conectara desde la

pared a la cual se alimentara de un voltaje de 220 Vac y esta será la línea de la acometida eléctrica; la segunda línea será la energía alterna del grupo electrógeno con un voltaje de 220 Vac que se encenderá cuando haya una falla de energía en la acometida eléctrica, ambos alambrado será protegidos por tubos PVC de 2 pulgadas.

Una vez conectada el ATS se procede a instalar el UPS (Sistema de Alimentación Ininterrumpida), este equipo estará al frente del ATS y junto al UPS de lado izquierdo va a estar ubicado el gabinete de Baterías de 480 V que ayudara a almacenar la energía para cualquier eventualidad en la corriente eléctrica.

3.5.2 Sala de Cómputo

El cuarto de cómputo es el lugar donde se ubicarán los principales equipos de telecomunicaciones tales como centrales telefónicas, conmutadores (switches), enrutadores (routers) y equipos de cómputo como servidores de datos o de video.

Para el diseño del cuarto de cómputo los equipos que son utilizados son:

- 20 gabinetes estándar de 42U de 19 pulgadas.
- 4 gabinetes estándar de 42U de 19 pulgadas.
- 4 unidades de CRAC.
- 2 unidades de distribución de energía

- 1 unidad condensadora

Para el cuarto de computo, se tendrá que instalar una superficie de piso de 0.20 m de alto medidos desde el piso original, que cubre parcialmente el cuarto de computo, este cuarto será el único que estará elevado mientras que las demás área conservará su revestimiento original (piso cerámico).

El piso falso se ha instalado por seguridad ante posibles inundaciones y para evitar las interferencias electromagnéticas, ya que la ruta que seguiría el cableado de voz y datos para llegar a los distintos gabinetes, estaría muy cerca de las diferentes tuberías que llevan los cables de las luminarias y electricidad. Por eso, para evitar cualquier tipo de interferencia los cables recorrerán el cuarto de cómputo por debajo del piso falso mediante bandejas sujetadas a los soportes de éste para que los cables no estén al ras del suelo.

Después de instalar el piso falso se procederá instalar los gabinetes, para nuestro centro de datos, para lo cual se utilizara la siguiente distribución de los gabinetes:

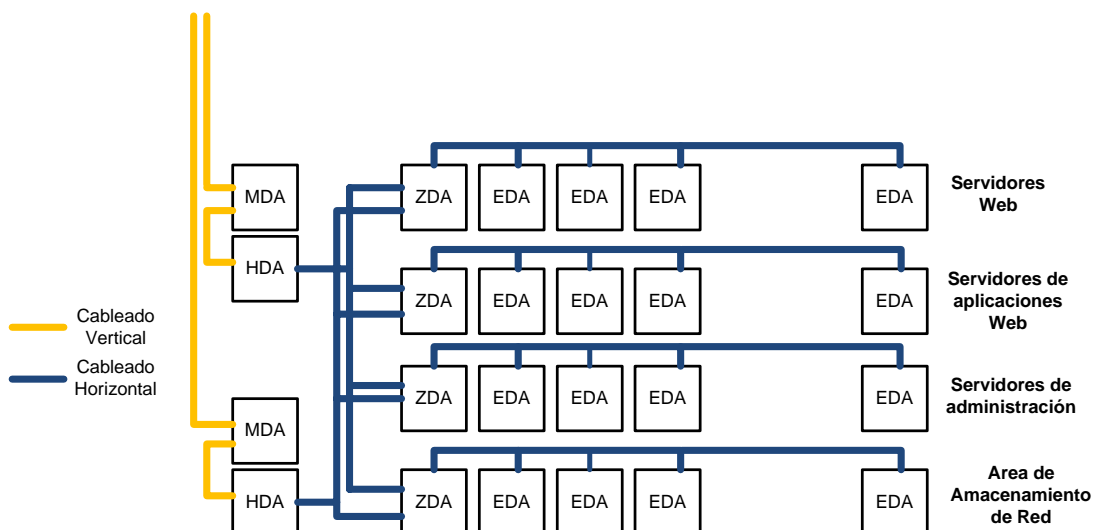


Figura 3.4 Distribución de los gabinetes en la sala de cómputo

La ubicación de cada gabinete se dividirá por zonas como está establecida en la norma TIA – 942.

3.5.2.1 Área Principal de Distribución:

El área principal de distribución se conformará de dos gabinetes situados en la parte delantera de la sala de cómputo, cada gabinete estará conformado por 2 paneles de fibra óptica que establecerá la conexión cruzada principal (cross connection) del Centro de Datos.

Esta conexión cruzada (cross connection) será el punto central de distribución para el centro de datos y usará un cableado LOMMF (Fibra Óptica Multi-Modo) de 62.5/125 um para conectarse con el cuarto de entrada.

El gabinete contará con un enrutador (router) y un conmutador de núcleo (switch core) y una regleta de alimentación eléctrica para

distribuir la energía en los equipos cuidando los equipos de trascientes de voltajes.

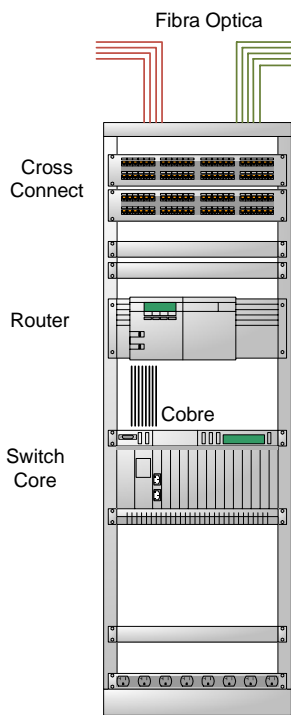


Figura 3.5 Rack del Área de Distribución Principal

3.5.2.2 Área de Distribución Horizontal:

El área de distribución horizontal es donde se ubicara las interconexiones horizontales y es el punto de distribución para el cableado hacia las áreas de distribución de los equipos.

Puede haber una o más áreas de distribución horizontal, según el tamaño del centro de datos y las necesidades de cableado.

Para el centro de datos se utilizara dos gabinetes para el área de distribución horizontal cada gabinete contara con dos paneles de fibra

óptica que se usara para la conexión cruzada horizontal y se conectarán con los gabinetes del área principal de distribución (MDA) por medio del cableado vertical o backbone.

El gabinete contará con un monitor LCD desplegable, teclado y un dispositivo KVM para la conmutación de diferentes servidores situados en los gabinetes.

Y por último un conmutador (switch) que se conectara con los gabinetes del área de almacenamiento de red (SAN) y los gabinetes del área de distribución de equipos (EDA).

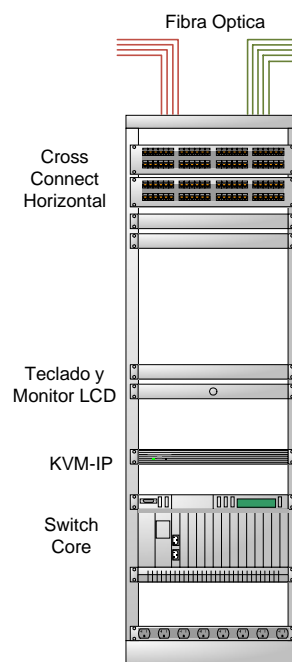


Figura 3.6 Rack del Área de Distribución Horizontal

3.5.2.3 Área de Distribución de Equipos

Es donde se ubicaran de los gabinetes con equipos y servidores. La norma específica que los gabinetes y racks se deben colocar es en una configuración pasillo caliente/pasillo frío ("hot aisle/cold aisle") para que disipen de manera eficaz el calor de los equipos electrónicos. Para nuestro centro de datos se necesitara 20 rack ubicados en 4 filas de 5 racks por cada fila.

Para la construcción del gabinete se va a utilizar dos patch panel de fibra óptica que se conectara por medio de cableado backbone con el área de distribución horizontal (HDA), dos conmutadores (switch) de distribución que se conectara con los servidores y estos pueden ser normales o de tipo blade por medio de cableado horizontal o UTP Cat

6.

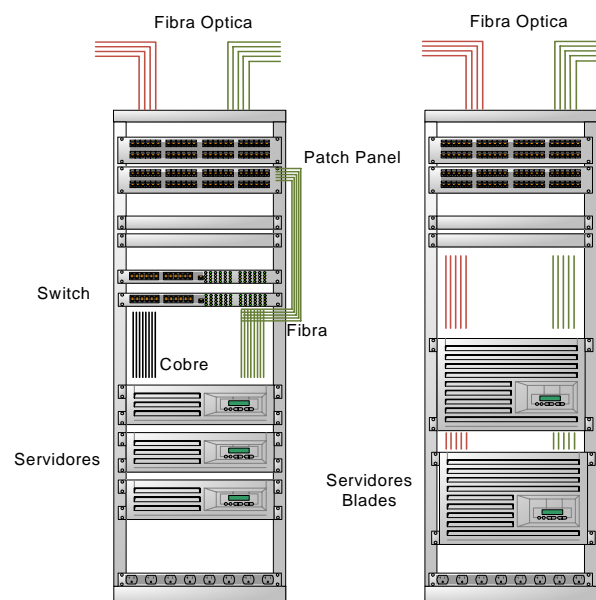


Figura 3.7 Rack del Área de Distribución de Equipos

También el área de distribución de equipos se encuentra los gabinetes donde estarán ubicados los dispositivos de almacenamiento de datos, estos grupos de gabinetes en específico son llamados área de almacenamiento de red (SAN) y están conformados de paneles de conexión de fibra óptica y de dos conmutadores (switch) de distribución que se conectara con los dispositivos de almacenamiento (storage).

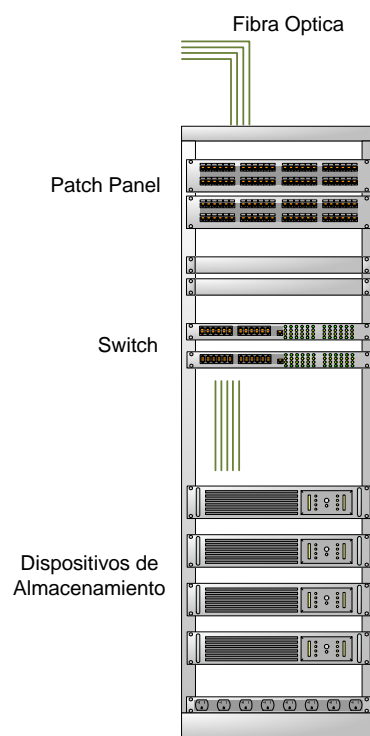


Figura 3.8 Rack del Área de Almacenamiento de Red

3.5.2.4 Climatización

El cuarto de cómputo tiene que estar a una temperatura controlada de 18° C a 22°C con una humedad del 45% al 55%, para lo cual se

instalara 4 unidades de **CRAC** para la climatización del cuarto y dos juegos de tuberías que estarán conectadas con los CRAC e instaladas debajo del piso falso.

Estos CRAC o torres de enfriamiento ayudara a absorber el aire caliente que se encuentra en el cuarto y por medio de las rejillas que tienen las baldosas del piso falso se suministrara aire frio y así el ambiente de todo el cuarto se mantendrá a una temperatura fría que es exigida por la norma.

La posición de cada unidad CRAC va a hacer en los extremos del cuarto de cómputo perpendicular a los rack.

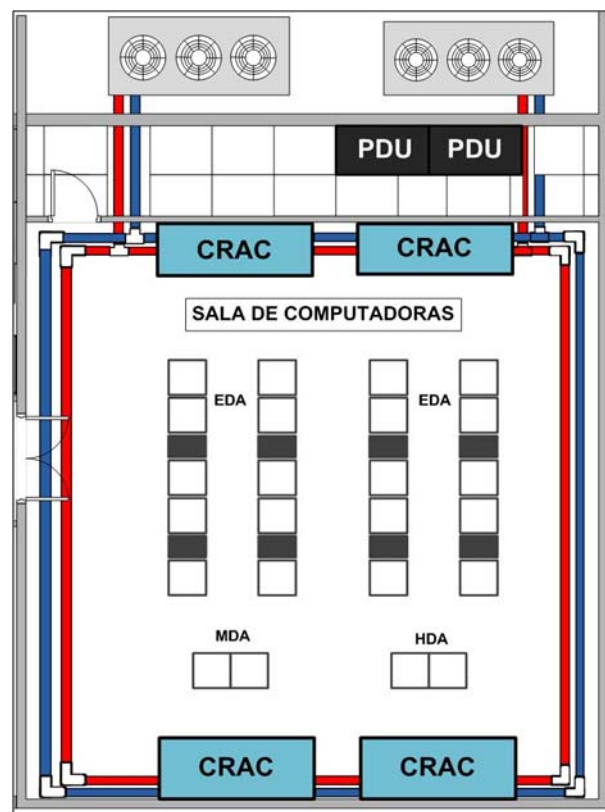


Figura 3.9 Sistema de Climatización por Chiller

Pero además se instalara un sistema de climatización para rack, este sistema se instalara en medio de los rack que contienen los servidores y funciona intercambiado el calor de los rack que están en la parte lateral del dorsal del armario para después soplar aire frío a los servidores.

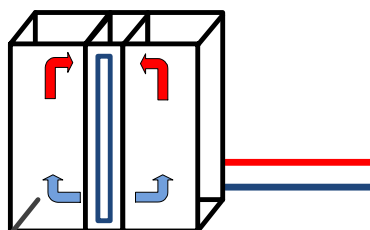


Figura 3.10 Sistema de Climatización por Rack

3.5.2.5 Unidad de Distribución de Energía

La distribución de la energía regulada de nuestro centro de datos contaremos con dos PDU los cuales van a estar instalados en la parte superior del cuarto de computo en una recamara especial.

Cada PDU se conectaran con todos los rack del cuarto de cómputo y de esta manera se establecerá redundancia entre los equipos.

El PDU trabajara con un voltaje de salida 208V/120V con lo cual va a ser administrado a los rack que estén conectados.

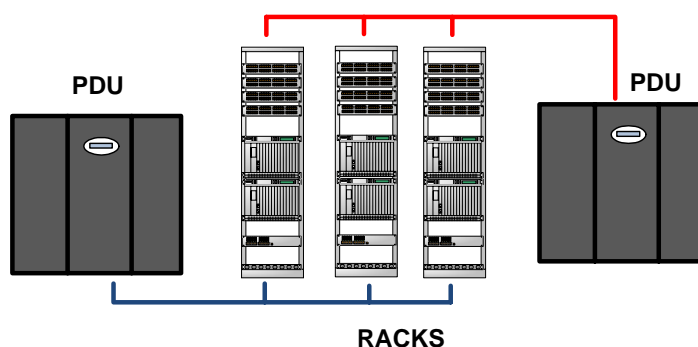


Figura 3.11 Administración de Energía en Rack

3.6 Cuarto de Telecomunicaciones y de Entrada de Servicio

Cumpliendo con las normas y requerimientos del EIA/TIA-569, el cuarto de telecomunicación deberá contar con racks cerrados de pared para la instalación, donde se ubicara los componentes del cableado.

El cuarto de telecomunicaciones contara con un gabinete el cual contiene todo el ponchado tanto para voz y datos, paneles de datos para el enlace vertical de voz y un Switch que facilite la conexión hacia el Centro de Datos a través de fibra óptica.

Según nuestro mercado objetivo se utilizara paneles de conexión de 24 puertos con organizadores de cables, las cuales son elementos necesarios para la administración y el manejo de los cables, así mismo, los organizadores de cables son originales de fábrica.

Los Patch Cord en categoría 6 son de cable UTP con conectores RJ-45 a los dos extremos de un metro de longitud, para la conexión de los equipos con el cableado horizontal.

Por lo tanto el dimensionamiento del rack en el cuarto de telecomunicaciones involucra la cantidad de puntos de datos y voz que se tomo en cuenta anteriormente. Los elementos a utilizarse son: paneles de datos o voz de 24 puertos RJ45 lo que representa una unidad de rack (1UR), organizadores de cables 60X80 dobles que representar 2UR, Switch de 24 puertos que representan 1UR.

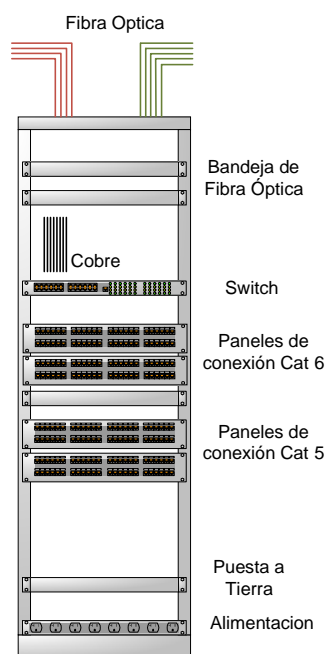


Figura 3.12 Rack del Cuarto de Entrada

Los Switch son equipos que transmiten solo al puerto o al puerto que requiere esa información.

El switch a utilizarse es de marca 3Com® modelo BaseLine 2924-SFP Plus, que es un conmutador de un GigaBit de Nivel dos de

configuración fija y administrativa, 24 puertos a velocidad de cable, 4 puertos de uso dual para conexiones de Gigabit de cobre o módulos de fibras basados en SFP y funcionalidad para un red de voz.

SFP es un modulador óptico de intercambio dinámico, es decir, puede transferir y recibir al mismo tiempo.

Característica del Switch 3Com® modelo BaseLine 2924-SFP PlusÑ

- ✓ Conmutador de Gigabit de nivel dos administrativo.
- ✓ 24 puertos 10/100/1000 y 4 puertos de Gigabit SFP, de uso dual con 4 de los puertos 10/100/1000, puerto de consola en panel frontal para la administración.
- ✓ VLAN automática que asigna el tráfico VoIP a una VLAN de voz dedicada.
- ✓ Los ajustes por defecto son aceptables.

3.7 Sistema de Puesta a Tierra

El sistema puesta a tierra debe seguir todas las recomendaciones de la Norma TIA-607 y TIA-942.

La TMBG es una barra de cobre, de 6 mm de espesor y 100mm de ancho mínimos. El largo puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella. Esta será colocada donde se encuentra la acometida eléctrica, es decir en la zona denominada Tableros Eléctricos.

La TGB es una barra de cobre, de 6 mm de espesor y 50 mm de ancho mínimos. Así mismo el largo puede variar dependiendo de los equipos que deban conectarse a ella. Se puede conectar cada TGB a la estructura metálica, con cables de diámetro mínimo 6 AWG.

La secuencia recomendada para conectar a tierra es la siguiente: el outlet se conecta a tierra en el panel de datos, y luego el panel es conectado al rack de equipos o a canalizaciones metálicas adyacentes. La secuencia básica se refleja en el siguiente diagrama:

1. El cable del UTP termina en el outlet.
2. El outlet hace contacto con la tira de conexión a tierra del panel de datos, cuando el outlet se inserta en su lugar.
3. El panel se conecta a tierra a través del rack de equipos o canalizaciones de metal adyacentes a través de un alambre de 6 AWG que se adjunta la lengüeta de tierra del panel.
4. El alambre de 6 AWG conecta el rack al TGB.

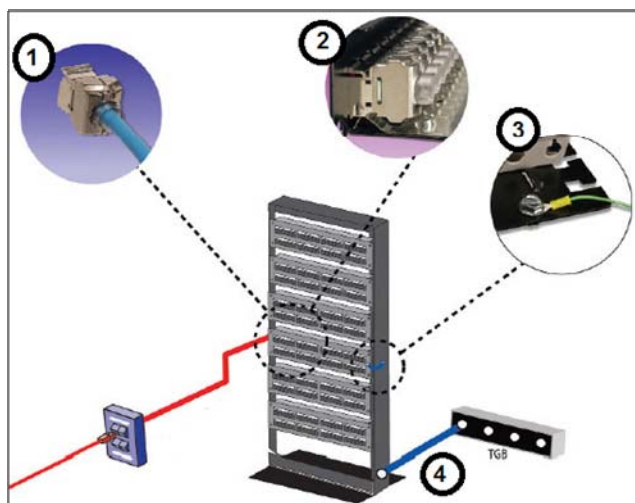


Figura 3.13 Sistema Puesta a Tierra

La ruta a tierra desde el rack de equipos hacia el TGB debe seguir los requisitos del sistema de conexión a tierra de redes de telecomunicaciones. Es de suma importancia hacer notar que los pasos de conexión a tierra dictados por los códigos aplicables son los mismos para los sistemas de cableado UTP, F/UTP y S/FTP. Aunque las normas y códigos difieren entre regiones y países, la metodología para conectar adecuadamente a tierra la red de telecomunicaciones es equivalente.

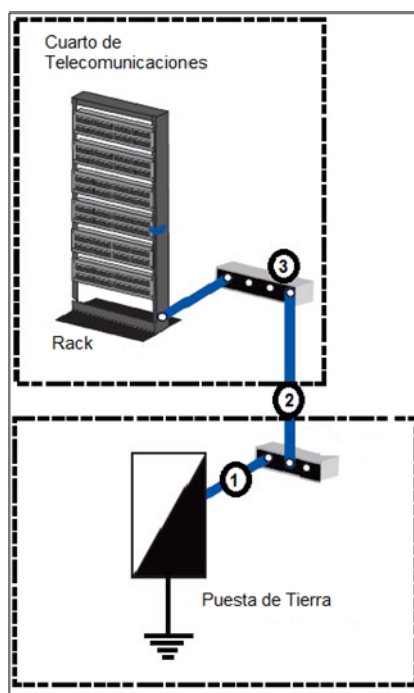


Figura 3.14 Pasos de Puesta a Tierra en una Red

Los procedimientos para unir y poner a tierra una red de telecomunicaciones son bastante claros. El sistema de cableado y el equipo se conectan a tierra por los racks de equipo o canalizaciones metálicas. Éstos a su vez son conectados al TGB. El TGB se une a la barra principal de conexión a tierra de telecomunicaciones (TMGB) a través del backbone de unión de telecomunicaciones. Finalmente, el TMGB se conecta a la tierra del servicio principal por medio del conector de unión de telecomunicaciones. Desde el rack hasta la tierra, el proceso es el mismo para la infraestructura de cableado UTP, fibra óptica.

3.8 Protección contra Incendios.

FM-200 extingue el incendio por eliminación de calor del fuego. El gas se almacena en cilindros a presión y se entrega a través de una red de tuberías y toberas de todo el centro de datos.

FM-200 (también conocido como el HFC-227ea) como heptafluoropropano y es fabricado por Great Lakes Chemical Corporation, es una alternativa del sistema de extinción de incendios, no deja residuos y no requiere costosos de limpieza, a diferencia de los aspersores y otros sistemas de protección contra incendios. Y las descargas en 10 segundos o menos, la extinción de incendios con rapidez y eficacia. No es tóxico en las personas.



Figura 3.15 FM-200 – Protección Incendios

Funcionamiento

La FM-200 es un agente extintor que suele almacenarse en cilindros o esferas. Se entrega a las lanzas a través de un sistema de tuberías de la red. Los detectores de humo detectan la presencia de fuego en las

instalaciones protegidas. La detección y el panel de control y luego suena una alarma, se apaga de tratamiento de aire, se desconecta la alimentación del equipo protegido, y luego libera agente dentro del área protegida.

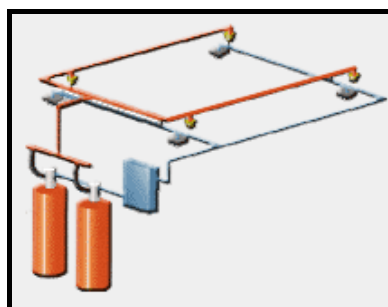


Figura 3.16 Funcionamiento FM-200

3.9 Medidas de Seguridad Física

El centro de datos está equipado con los modernos sistemas de seguridad para la prevención de accesos no autorizados, entre los que se encuentran:

- **Cámaras de Vigilancia y Monitoreo**

El circuito está dado por varias cámaras de vigilancia conectadas a monitores las 24 horas del día, que reproducen las imágenes capturadas, y a su vez son almacenadas en un dispositivo especial para dicha tarea y almacenadas en armarios ignífugo. Las cámaras son monitorizadas por un agente ubicado en la sala de seguridad, son

cámaras móviles aunque normalmente se encuentran fijas en un lugar determinado.

Las cámaras de vigilancia están situadas en lugares estratégicos para el control total del centro de datos:

- En las puertas de acceso.
- En la esquina de los cuartos del centro de dato.
- Cámaras en los pasillos, externos e internos de las instalaciones.

- **Vigilancia física y control de acceso**

Nuestro centro de datos cuenta con seguridad humana por parte de una empresa de seguridad privada las 24 horas del día y los 365 días del año, con profesionales y medios técnicos necesarios para el desarrollo de sistemas integrales de seguridad altamente sofisticados, personalizados a las necesidades específicas de cada cliente.

- **Acceso a cuartos controladas por pases magnéticos**

Todas las puertas de ingreso a cualquier cuarto en el Centro de Datos tendrá un pase magnético El sistema realiza un barrido magnético al pasar una persona por la puerta. Este chequeo se realiza para evitar que ningún usuario retire un equipo del centro de datos sin previa autorización, en caso contrario la alarma se encenderá y se procede avisar al personal de seguridad para su revisión.

- **Sistema Biométrico de Control de Acceso**

El acceso al Centro de Operaciones de Red se dará por medio de lectura de huella digital y de iris, que serán registrados en el sistema durante las 24 horas del día y son monitoreados en la consola maestra ubicada en la sala de seguridad, esta consola de control despliega el nombre e imagen de la persona que registra su acceso.

- **Cortafuegos (Firewall)**

Son dispositivos formados por uno o varios equipos que se sitúan entre la red de la empresa y la red exterior, analizando todos los paquetes que transitan entre ambas redes y filtrando los que no deben ser reenviados, de acuerdo con un criterio establecido de antemano de forma simple.

Para el centro de datos se utilizara dos tipos de cortafuegos (firewall):

- **Cortafuegos de inspección de estados (Firewall Stateful):**

Este tipo de firewall que mantiene un seguimiento del estado de las conexiones de red que pasan a través de él.

- **Cortafuegos de Aplicación de Nivel (Application Level Firewall):**

Conocido como Gateway de Aplicación, este firewall son capaces de inspeccionar hasta el nivel de aplicación, distinguiéndose por el uso de los Proxies para servicios internos de la red.

3.10 Requisitos de Hardware y Software para el servicio del Cloud

Computing

El entorno físico de los servidores deberá estar compuesto de las siguientes características:

Servidores Típicos	Intel Core 2 Quad Q6600	Mínima: 1 DIMM de 8GB. Máxima: 12 DIMM de máx. 96Gb	Servidor de alta densidad de rendimiento y flexibilidad de E/S.
Servidores Blade	Intel Core 2 Quad Q6600	Mínima: 1 DIMM de 8GB. Máxima: 48 DIMM de máx. 384Gb	Servidor de alto rendimiento y de memoria intensiva para entornos muy virtualizado de gran carga de trabajo.

Tabla 3.1 Requisitos Hardware y Software en Cloud Computing

El número de equipos con estas especificaciones es suficiente para levantar un servicio de nube computacional.

El sistema operativo anfitrión puede ser de entorno gratuito y open source como por ejemplo Ubuntu 9.04 Jaunty Jackalope. Este sistema es muy utilizado por tener diferentes funcionalidades. Además, esta versión de Ubuntu apuesta por el Cloud Computing incluyendo entre otras herramientas KVM, Eucalyptus y OpenNebula.

Actualmente existen diferentes Hipervisores en el mercado por lo cual en la siguiente tabla se muestra cada hypervisor con sus características:

Software	Características
VMware Workstation	<ul style="list-style-type: none"> ✓ Permite Multi-core y cuatro máquinas virtuales. ✓ Capacidad de impresión desde una máquina virtual sin necesidad de instalar los controladores. ✓ Protección de las máquinas virtuales de encriptación de 128-bit. ✓ Editor de Linux mejorada red virtual.
VMware Server	<ul style="list-style-type: none"> ✓ Proporciona un punto de control centralizado. ✓ Administra los servicios de infraestructura y de las aplicaciones. ✓ Posee máxima visibilidad de todos los aspectos de la infraestructura virtual. ✓ Automatización de las tareas operativas cotidianas. ✓ Escalabilidad para gestionar entornos de grandes centros de datos.
Hyper-V	<ul style="list-style-type: none"> ✓ Permite una solución de virtualización simplificada, fiable, económica y optimizada. ✓ Permite reducir costes. ✓ Mejorar el nivel de utilización de los servidores. ✓ Aprovisionar rápidamente nuevos servidores.

Tabla 3.2 Software de Virtualización Pagadas

3.10.1 Software para virtualización (Pagados)

En la siguiente tabla se ilustran algunos software para virtualización pagadas con sus respectivas características.

Aceptación en el mercado.

PAGADOS		
Software	Aceptación del mercado	Desarrollado por
VMware Workstation	48%	VMWare

VMware Server	27%	VMWare
Hyper-V	17%	Microsoft
Citrix	6%	Red Hat
Otros	3%	

Tabla 3.3 Aceptación en el Mercado Software Virtualización Pagadas

VMWare tiene una gran aceptación en el mercado.

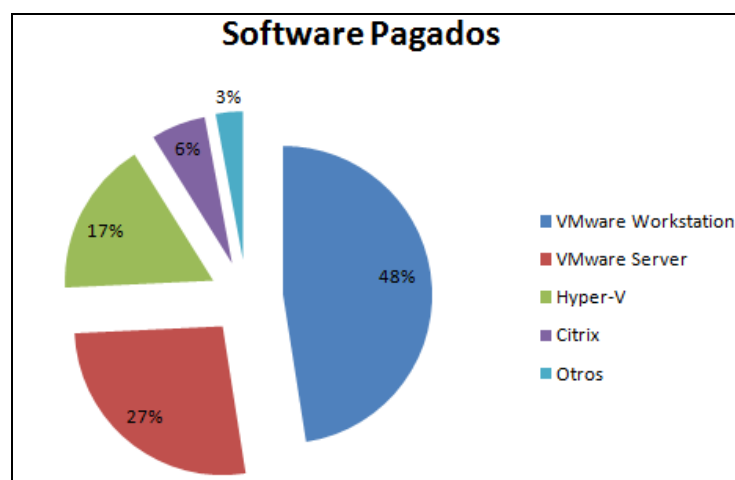


Figura 3.17 Aceptación en el Mercado Software Virtualización Pagadas

3.10.2 Software para virtualización (Libre)

Los programas de código libre que funcionan tanto en Mac OS, en Windows como en GNU/Linux, son los siguientes:

Software	Características
Xen	<ul style="list-style-type: none"> ✓ Proporciona aislamiento seguro ✓ Control de recursos ✓ Garantías de calidad de servicio ✓ Migración de máquinas virtuales en caliente
OpenVZ	<ul style="list-style-type: none"> ✓ Proporciona mejor rendimiento ✓ Escalabilidad ✓ Densidad ✓ Administración de recursos dinámicos ✓ Facilidad de administración que las

	alternativas.
VirtualBox	<ul style="list-style-type: none"> ✓ Modularidad. ✓ Uso de XML . ✓ Optimización del sistema virtual instalado.

Tabla 3.4 Software Virtualización Libre

Aceptación en el Mercado

Libre		
Software	Aceptación del mercado	Desarrollado por
KVM	50%	Red Hat
VirtualBox	28%	Oracle Corporation(todos)
Xen	16%	
OpenVZ	6%	SWsoft, Inc.(solo linux)

Tabla 3.5 Aceptación en el Mercado Software Virtualización Libres

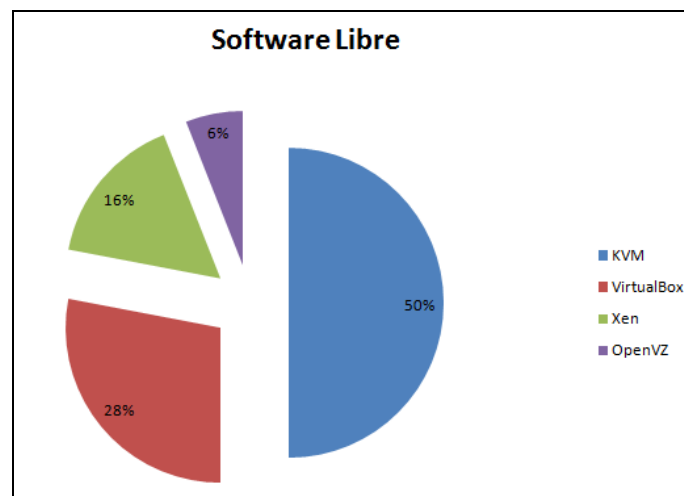


Figura 3.18 Aceptación en el Mercado Software Virtualización Libre

Cuadro comparativo de las características del Cloud Computing

Características	Xen Server	VMWare
Máximo CPU virtuales	8	4
Servidores ilimitados, VM, memoria.	SI	SI
Windows y Linux guest	SI	SI
Conversión de P2V y V2V	SI	SI
Almacenamiento compartida SAN y NAS	SI	SI
Gestión centralizada de múltiples servidores	SI	NO
Flexible arquitectura de gestión distribuida	SI	NO
Biblioteca compartida plantilla de VM.	SI	NO
Administración de configuración centralizada	SI	NO
Infraestructura virtual de gestión de parches.	SI	NO
Inteligente de la colocación inicial de VM.	SI	NO
Inteligente servidor de modo de mantenimiento.	SI	NO
Fine-grained controles de recursos de CPU.	SI	NO
Host discos intercambiables y tarjetas de red.	SI	NO

Tabla 3.6 Cuadro Comparativo de las Características del Cloud Computing

3.10.3 Ventajas Plataformas de Virtualización.

Las ventajas de la virtualización usando una plataforma Proprietario son:

A	El incremento en agilidad	29%
B	Su capacidad para optimizar recursos y reducir costes	21%
C	La aceleración en la provisión de aplicaciones	22%
D	Tolerancia a fallos y restauración	20%
E	La estabilidad	18%
F	Fácil configuración y administración	12%
G	Gestión	9%

Tabla 3.7 Ventajas Plataformas de Virtualización

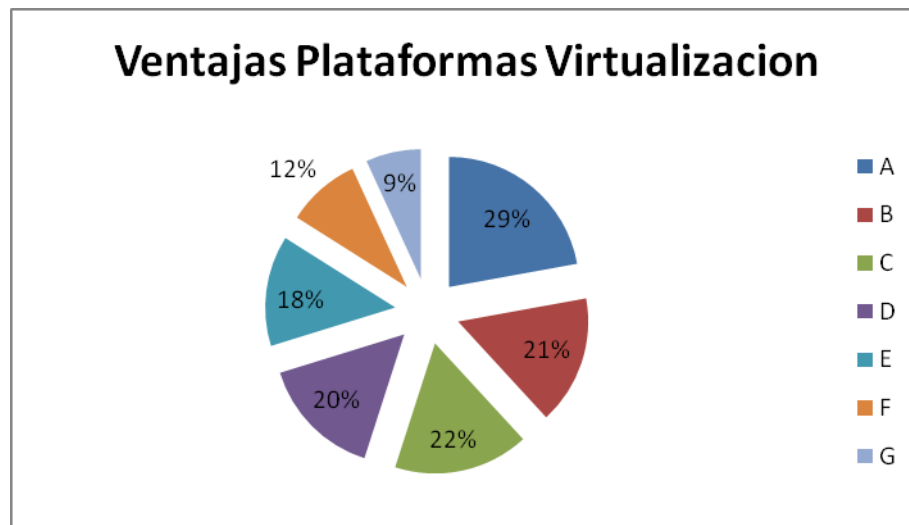


Figura 3.19 Ventajas Plataformas de Virtualización

Las desventajas de la virtualización usando una plataforma Libre son:

A	Las principales barreras para su adopción son la preocupación por la seguridad	18%
B	No son compatibles con todos los sistemas operativos.	16%
C	La dificultad para construir procesos operativos para un entorno virtualizado.	11%
D	Las configuraciones son difícil para administrar.	5%

Tabla 3.8 Desventajas Plataformas de Virtualización

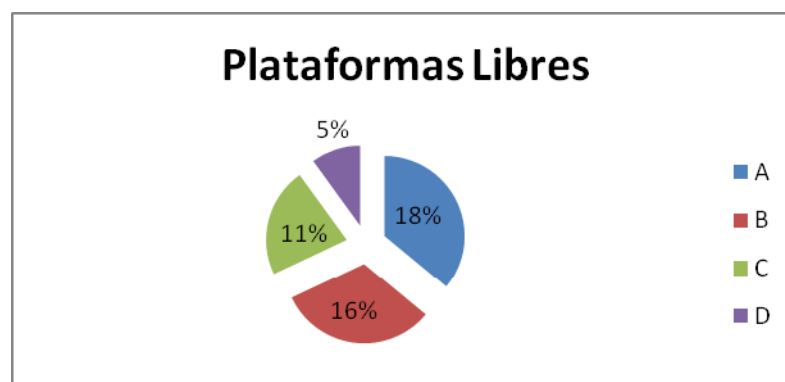


Figura 3.20 Desventajas Plataformas de Virtualización

Nota: Son características más resaltadas en las opiniones de las empresas que usan plataformas de virtualización.

4 DISEÑO TOPOLÓGICO Y SERVICIOS DEL CENTRO DE DATOS

4.1 Topología de la Red

La topología física de una red es la forma física y geométrica que como va a estar instalada la red, tanto a los terminales como a los cables.

Con la topología se intenta obtener una instalación ordenada de terminales y cables de enlace.

Y topología lógica de una red es la forma en que los hosts se comunican a través del medio.

4.1.1 Topología Física

El cableado del Centro de Datos tiene dos partes el cableado horizontal y el cableado vertical ambo cableado comparte la misma topología física en estrella que es la configuración dominante en el diseño de un centro de datos.

Para el cableado horizontal cada conector o toma de telecomunicaciones se conectara a la conexión cruzada del gabinete en el cuarto de telecomunicaciones.

Y para el cableado vertical todas las conexiones cruzadas horizontales se deben conectar a la conexión cruzada principal.

Todos los equipos que se conectan a la conexión cruzada principal se conectan a un switch de núcleo, el cual tiene un modo de funcionamiento de nodo central como dispositivo de conmutación de tramas. Una trama entrante se almacenará en el nodo y se retransmitirá sobre un enlace de salida hacia el destino.

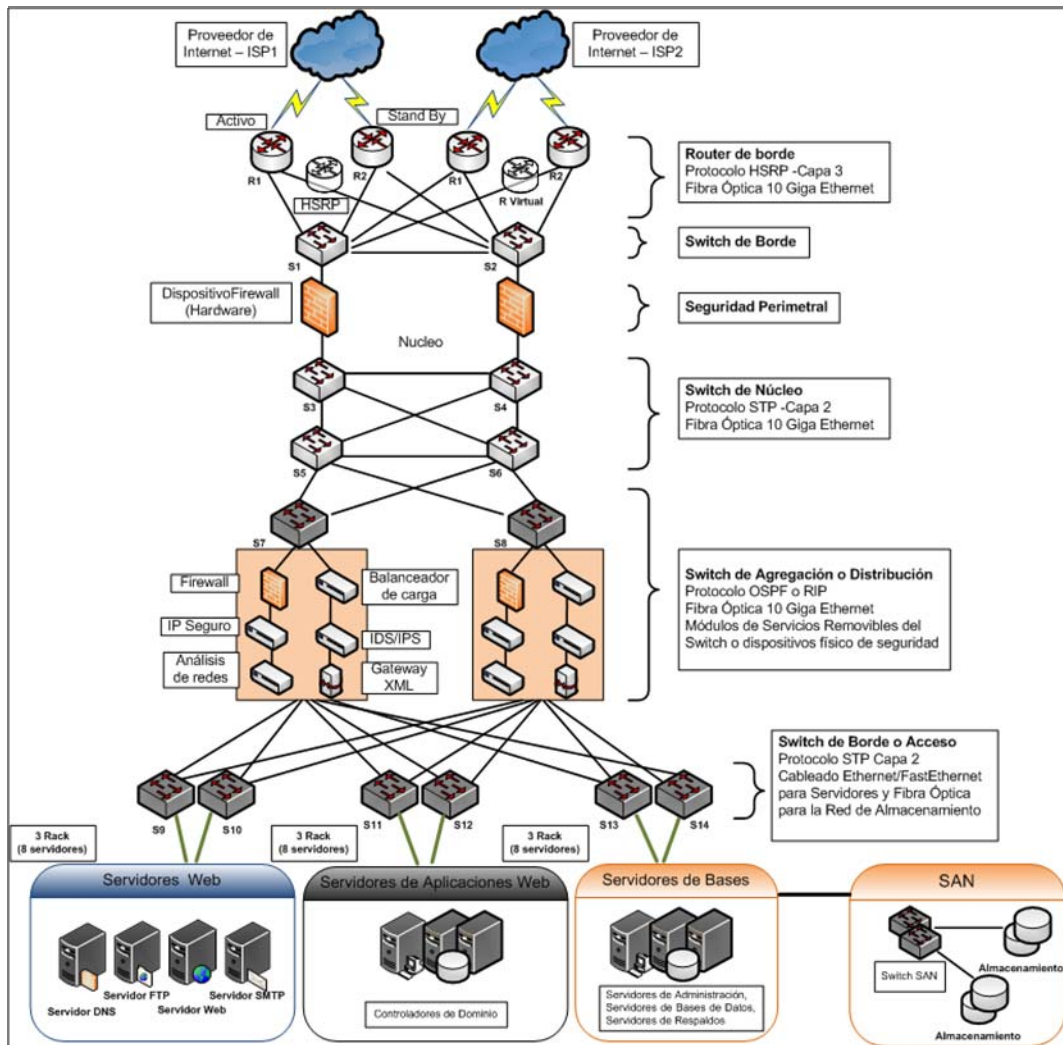


Figura 4.1 Diseño Físico del Centro de Datos

4.1.2 Topología Lógica

La red utiliza una topología lógica en estrella, debido a que los dos switch principales son los encargados de dirigir el tráfico y se tiene una conectividad con routers, switch, rack de comunicaciones y paneles de conexión.

Analizando la topología el throughput requerido en nuestro diseño es 400mpps según los dispositivos presentes.

Así mismo en tiempo de conmutación para los dispositivos es de 1 a 3 segundos

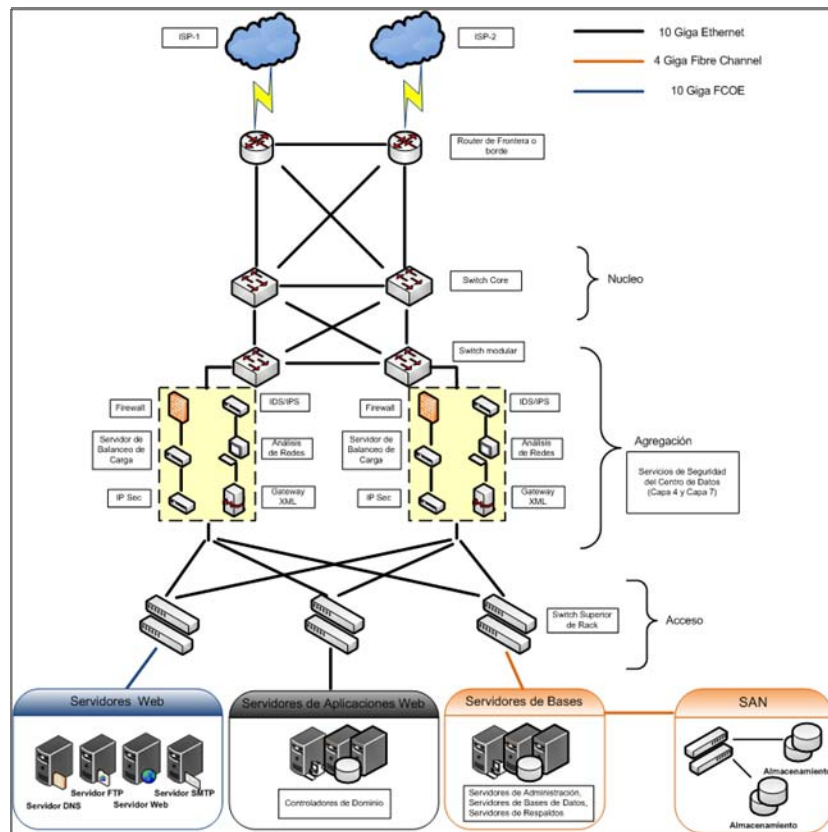
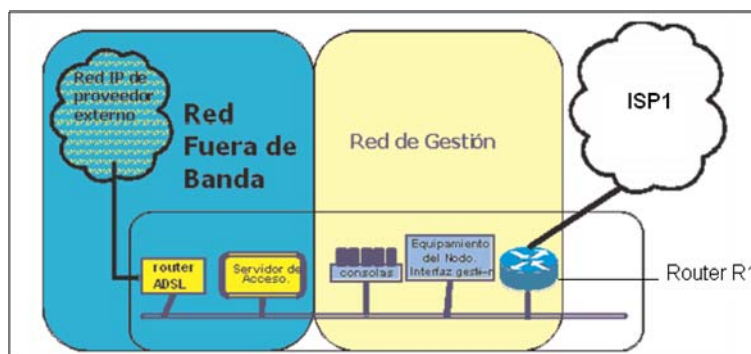


Figura 4.2 Diseño Lógico del Centro de Datos

4.1.2.1 Red Fuera de Banda

La arquitectura de red fuera de banda diseñada tiene como objetivo facilitar el acceso de los técnicos de operación de la red en general a los diferentes nodos, en el caso de que dicho nodo quedase sin



conexión por algún motivo o necesiten realizar tareas de mantenimiento que implicasen una potencial desconexión.

Figura 4.3 Diseño Lógico de la Red Fuera de Banda

La ilustración describe el esquema lógico de la red fuera de banda diseñada en nuestro ejemplo para el Router 1 y su integración con la red de gestión. En caso de que el Router 1 sufriera una desconexión por alguno de los motivos anteriormente citados la red fuera de banda facilita un camino alternativo de acceder a la red de gestión del nodo. La red fuera de banda es facilitada por un operador externo y está basada en tecnología ADSL con direccionamiento IP público-fijo.

El acceso desde el exterior usando esta red es controlado por el servidor de acceso, que en algunos casos y dependiendo de las

singularidades del nodo de la red, podría ser el mismo servidor de gestión. Una vez el operador haya accedido al servidor de acceso, este dispone tiene accesible todos los equipos de control y gestión del nodo.

Así mismo cuando la red está caída, el acceso remoto, en situaciones fuera de banda, a los puertos de consola ofrece un método eficiente de puerta trasera para recuperación. Tanto si se trata de reiniciar, reconfigurar o resolver problemas existentes en el equipo, un servidor de terminales/consolas le permite acceder a equipos de red remotos cuando más lo necesita. Esto puede lograrse a través del uso de un acceso remoto alternativo de respaldo, ya sea acceso telefónico a redes o inalámbrico GSM.

Los puertos de consola serie constituyen la forma más fiable y segura de comunicación para la administración de equipos. Esta es la razón por la que la mayoría de los dispositivos de redes de alto valor disponen de él. Con independencia de si se trata de un router, un conmutador, un firewall, un dispositivo de almacenamiento de red, etc. y de lo que le ocurra al dispositivo, el puerto serie auxiliar o de consola siempre estará en funcionamiento. Se trata de un método de confianza para averiguar qué está sucediendo, así como del medio más rápido para lograr la recuperación.

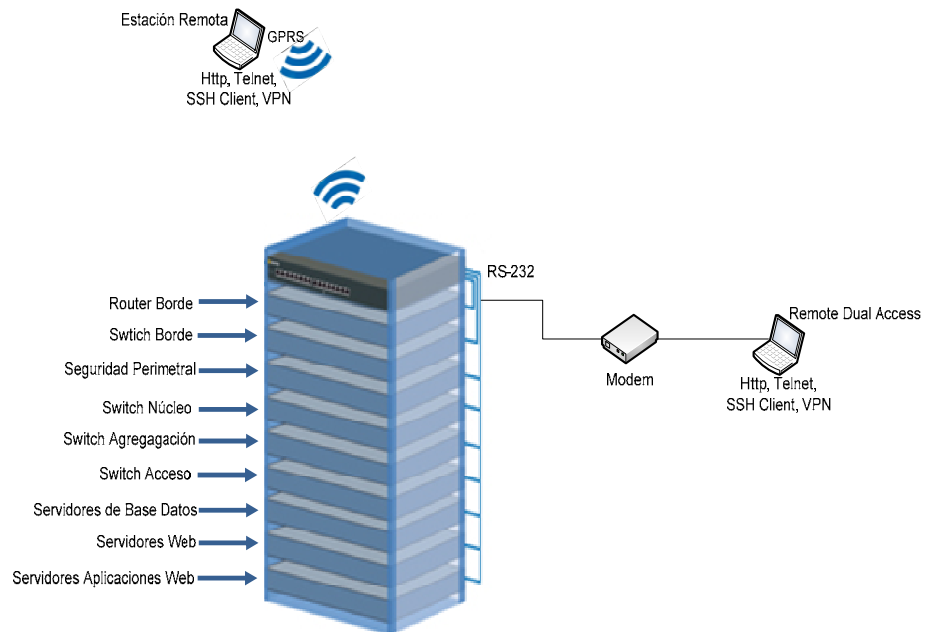


Figura 4.4 Diseño Puerto de Consola

4.1.2.2 Protocolos del Centro de Datos

Los protocolos son un conjunto de reglas usadas por la computadora para comunicarse unas con otras a través de la red.

Para la elección de protocolos de conmutación y enrutamiento se debe tener en cuenta los siguientes criterios:

- Trafico de la red
- Ancho de banda, memoria y CPU
- Capacidad para adaptare ante los cambios
- Numero de nodos soportados
- Soporte de autenticidad

Al conocer estos criterios se eligió los siguientes protocolos de enrutamiento y conmutación:

- **Protocolo HSRP:**

El Hot Standby Router Protocol es un protocolo de nivel 3 de la capa OSI, permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers.

El protocolo HSRP es utilizado en los routers de frontera del Centro de Datos mediante la siguiente configuración:

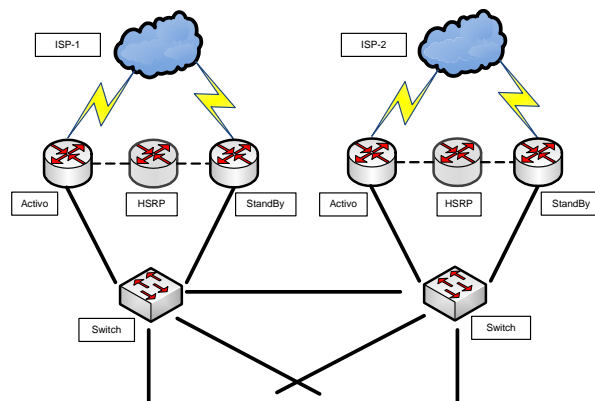


Figura 4.5 Diseño del Protocolo HSRP

Si el router primario no envía los paquetes en el momento de la transmisión por un cierto tiempo el router standby asume que el router primario está fuera de servicio y este se pone en activo.

- **Protocolo OSFP**

Open Shortest Path First (El camino más corto primero) es un protocolo de enrutamiento jerárquico de gateway interior o IGP que calcula la ruta más corta posible construyendo una base de datos con los enlaces y estado.

- **Protocolo STP**

Spanning Tree Protocol (Protocolo de árbol extendido) es un protocolo de nivel 2 de la capa OSI, automatiza la administración de la topología de la red con enlaces redundantes.

La función del protocolo es permitir rutas conmutadas duplicadas sin considerar los efectos de latencia de los loops en la red. Su algoritmo calcula la ruta libre de loops.

El protocolo STP fue estandarizado por la IEEE 802.1D.

- **Protocolo RSTP**

Rapid Spanning Tree Protocol (Protocolo rápido de árbol extendido) puede ser visto como la evolución del estándar 802.1D. El RSTP siendo más rápida que el STP conserva todos los conceptos básicos de la STP e interactúa con él también. Los usuarios familiarizados con el funcionamiento de STP puede aprender rápidamente el nuevo algoritmo ya que tanto la terminología y de base parámetros se han quedado sin cambios. es un protocolo de red de la segunda capa OSI, que gestiona enlaces redundantes.

El RSTP es utilizado en la capa de agregación y de acceso del Centro de Datos.

El protocolo RSTP fue estandarizado por la IEEE 802.1W.

- **Switch Multicapa**

Son switch que operan en capa 2 según el modelo OSI y puede ser incorporado como un enrutador funcionando en capa 3. Es decir, que tiene las funcionalidades de un enrutador para diferentes VLANs.

Para la seguridad de nuestra red ante posibles ataques maliciosos se va a establecer un protocolo de seguridad.

- **Protocolo SSH**

Secure Shell(Ordenes Securas) es un protocolo que facilita las comunicaciones seguras entre nos permite manejar por completo la computadora mediante un intérprete de comandos, utilizando la arquitectura de cliente/servidor activando el puerto 22 por default al servidor esperando que algún cliente con SSH se conecte para ofrecerle una sesión segura encriptándola de extremo a extremo.

4.2 Servicios del Centro de Datos

En la actualidad el escenario de negocios de las empresas ha sufrido cambios muy rápidos por lo que muy pocas empresas han podido controlar todos los aspectos de la infraestructura de la tecnología informática.

La solución más conveniente es la adquisición de servicios de infraestructura de tecnología informática de un Centro de Datos y pagarlo de acuerdo con lo que se utilice por una simple tasa mensual siguiendo el acuerdo SLA.

Los requisitos que el Centro de Datos va a tener para un buen funcionamiento:

- Disponibilidad de conexión y servicio las 24/7.
- Protección contra incendio y otras catástrofes naturales. Igualmente no debe existir en este espacio ningún material que no haga parte de los equipos, es decir material inflamable como el papel o cartón (incluyendo la completa limpieza de los pisos)
- Control constante del ambiente del espacio, es decir que la temperatura y la humedad estén en constante control y entre un rango recomendado para los Centro de Datos.
- Sistema inteligente para el acceso a los equipos. Toda persona que ingrese a este espacio debe ser un usuario autorizado y con la seguridad necesaria.
- El cableado debe estar perfectamente identificado para no tener confusiones, incluyendo identificación de los canales por donde pasa.
- Tener un sistema ininterrumpido como UPS, para garantizar que no se caigan los servidores, y por supuesto que soporten los equipos

4.3. Servicio ofrecidos por el Centro de Datos

El Centro de Datos ofrecerá diferentes tipos de servicios que varía dependiendo del mercado local como son PYMES, Corporaciones, Entidades Financieras y Servicios Privados.

Los servicios del Centro de Datos son:

- Servicios Compartidos
- Servidores Dedicados
- Hosting Dedicados
- Servidores Virtuales
- Servicio de Colocación

4.3.1.1 Servicios Compartidos

Una plataforma compartida le permite tener disponibilidad de servicios básicos para asegurar su presencia en internet de forma económica y segura, no importa si requiere una base de datos, correo electrónico u hospedaje de un sitio web o de una aplicación.

Cuenta con:

- Sistema Operativo Linux
- Hospedaje de Aplicaciones (Java, PHP, Perl, CGI)
- Hospedaje de Sitios Web (HTML,PHP,JSP,Servlets)
- Servicios de Correo Electrónico (SMTP, POP3,IMAP)
- Servicios de FTP – SSL Compartido

- WebServer: Apache, Tomcat
- Servicios de Bases de Datos (MySQL, Postgresql y SQL Server)
- RespalDOS Diarios
- SSL
- Seguridad en Puertos
- Tasas de Transferencia Fijas.

4.3.1.2 Servidores Dedicados (Hosting)

El hospedaje de servidores dedicado que ofrecemos, le permite hacer uso de un servidor con las mejores características de seguridad y accesibilidad desde cualquier parte del país o del mundo, asegurando la disponibilidad de sus sistemas.

También ofrecemos servidores alquilados de cualquier marca de última generación o el cliente puede traer su propio servidor siguiendo las especificaciones del Centro de Datos.

Servidores Sin Administración			
Administración por parte del cliente	✓	✓	✓
Firewall Compartido	✓	✓	✓
Montaje en Rack Cerrado	✓	✓	✓
Acceso Restringido al Centro de Datos	✓	✓	✓
UPS Redundante N+1	✓	✓	✓
Cuentas de hosting ilimitadas	x	✓	✓
Cuentas de Email ilimitadas	x	✓	✓

1 IP Publica Fija	✓	✓	✓
Descripción: El Servicio consta de un servidor por parte del cliente, en Rack cerrado Los contratos tienen duración de 24 Meses. Este servicio cuenta con visitas programadas y de emergencia al Centro de Datos.			

Tabla 4.1 Servidores Dedicados sin Administración

El servicio de servidores dedicados cuenta con un sistema operativo con aplicaciones alojado dentro del Centro de Datos. El precio de este servicio varia por las características del servidor, el sistema operativo, las aplicaciones adicionales y el ancho de banda.

Servidores Con Administración			
Procesador	Core 2 Duo 2,9 GHz	i5 - Quad Core - 2,66 Ghz	2x Xeon Quad Core 2,26 GHz Nehalem H/T
Memoria	4 GB de RAM	6 GB de RAM	8 GB RAM DDR3
Disco Duro	160 GB SATA2	320 GB SATA2	3 Discos de 146 GB 15K SAS 3 GB/s
Tarjeta de Red 10/100	✓	✓	✓
Administración por parte del cliente	✓	✓	✓
Firewall Compartido	✓	✓	✓
Montaje en Rack Cerrado	✓	✓	✓
Acceso Restringido al Centro de Datos	✓	✓	✓
UPS Redundante N+1	✓	✓	✓

Cuentas de hosting ilimitadas	X	✓	✓
Cuentas de Email ilimitadas	X	✓	✓
1 IP Publica Fija	✓	✓	✓
Descripción: El Servicio consta de un servidor por parte del proveedor en Rack cerrado Los contratos tienen duración de 12 o 24 Meses Este servicio no cuenta con visitas al centro de Datos.			

Tabla 4.2 Servidores Dedicados con Administración

Los servidores alquilados cuenta con:

- Linux Server
- Servidores Intel y AMD
- Hospedaje de Aplicaciones
- Hospedaje de Sitios Web
- Servicios de Correo Electrónico
- Servicios de FTP
- Servicios de Bases de Datos (SQL Server, Oracle, MySql)
- RespalDOS Diarios
- Expansión de Discos SATA
- Expansión de Memoria
- Tasas de Transferencia Fijas e ilimitadas

--	--	--	--

Características de Hosting			
Capacidad en Megabytes	500	750	1GB
Cantidad de casillas Email POP3	35	50	80
Transferencia Mensual	ilimitado	ilimitado	ilimitado
Ancho de Banda Nacional	1024 Mb	3100 Mb	4100 Mb
Sistema Operativo(Linux Debian , Fedora, Centos)	✓	✓	✓
Acceso WebMail y POP3	✓	✓	✓
Servidor de Correo mail.sudominio.cl	✓	✓	✓
Autorespondedores de Correo	✓	✓	✓
Redireccionamiento de Correo	✓	✓	✓
Paginas de error personalizables	✓	✓	✓
Panel de Control / Administración	✓	✓	✓
Carpetas Protegidas	✓	✓	✓
FTP Ilimitado 24x7x365	✓	✓	✓
Soporte Vía Email 24 x 7	✓	✓	✓
Filtro Antivirus para Correo	✓	✓	✓
Filtro Anti-Spam para Correo	✓	✓	✓
Soporte Perl	✓	✓	✓
Soporte PHP	✓	✓	✓
Soporte SSL	✓	✓	✓
Bases de Datos MySql, SQL Server y Oracle	3	4	5
Administración Mysql con PhpMyAdmin	✓	✓	✓

Tabla 4.3 Características de los Servicios Alquilados

4.3.1.3 Servidores Virtuales

Los servidores virtuales son una opción alterna a los servidores dedicados y el servicio de colocación. Este método de particionar un servidor en varios le asegura por un precio menor una cantidad predefinida de recursos (memoria, disco duro y procesamiento).

Las aplicaciones que se pueden ejecutar en este tipo de servidores deben cumplir con ciertas características que se adapten favorablemente a este modelo de servicios, tales como frecuencia escritura/lectura en disco y procesamiento.

La virtualización de servidores se lo hace por planes de servicios para los diferentes mercados y clientes:

- **Bronce:** El servicio Bronce se establece con el uso de uno o dos máquinas virtuales, cada máquina virtual cuenta con un núcleo de procesamiento de 1.5 GHz, con una memoria de 2GB hasta 8GB y un espacio de almacenamiento de datos de 100GB a 500GB.

El servicio de Bronce cuenta con 1 Raid de 5 dispositivos de almacenamientos o storage, los cuales usan conectores de tipo SATA para conectarse entre sí y con el servidor en donde está instalada la máquina virtual.

La máquina virtual del servicio de Bronce está conectada a una sola VLAN es decir que en ella residirán los tres servicios juntos como son: Servicios Web, Servicios de Aplicaciones Web y de

Base de Datos. También cuenta con un buen procesamiento de datos y utilización de recursos de red dentro de la nube computacional.

Este servicio de Bronce cuenta con firewall que va a bloquear el acceso no autorizado, permitiendo al mismo tiempo solo comunicaciones autorizadas a los servicios y con un analizador de red o rastreador de puerto que permitirá supervisar el tráfico de la red.

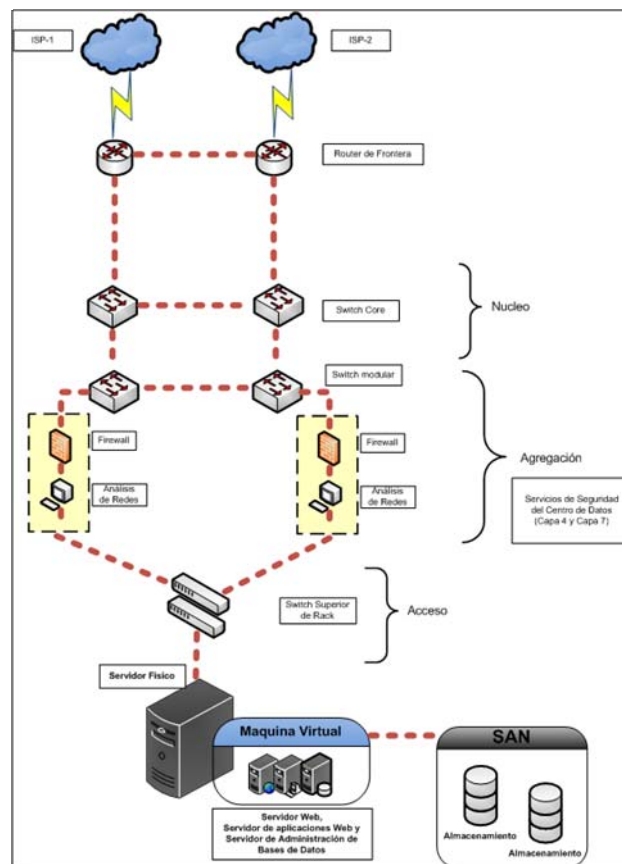


Figura 4.6 Diseño Topológico del Plan de Servicio Bronce

Máquinas Virtuales	1 o 2 máquinas instaladas en un servidor
Núcleo de Procesamiento	1.5 GHz
Memoria RAM	2 Gb a 8 Gb
Espacio de Almacenamiento	100 Gb a 500 Gb
Raid de almacenamiento	1 Raid con 5 dispositivos
Servicio de Seguridad	Firewall y analizador de red

Tabla 4.4 Característica del Servicio de Bronce

- **Plata:** El servicio de Plata de nuestro Centro de Datos consistes en dos máquinas virtuales que están instaladas en el uno o dos equipos de servidores que están montados en los gabinetes de la sala de computo, cada máquina virtual cuenta con un núcleo de procesador es de 2GHz de 2GB hasta 8 GB de memoria y un espacio de almacenamiento de datos de 1 TB.

El servicio de Plata cuenta con 2 Raid de 5 dispositivos de almacenamiento o storage los cuales usan conectores de tipo SATA y cableado de fibra canal de 10k, los cuales se conectaran entre sí y con los servidores donde correrán las máquinas virtuales.

Las 2 máquinas virtuales del servicio de Plata están conectadas a una sola VLAN, por lo que en cada máquina virtual residirán los tres servicios: servicios Web, servicios de Aplicaciones Web y de Base de Datos. Estos servicios están instalados en dos máquinas virtuales para hacer redundancia y carga de balanceo de datos.

El servicio de Bronce cuenta con firewall que bloqueea cualquier acceso no autorizado, balanceo de carga en múltiples máquinas virtuales para el tráfico de datos, analizador de red para la supervisión de la red y módulos de IDS/IPS que contralara el acceso a la red de ataques y abusos. También cuenta con un mejor esfuerzo en el procesamiento de datos y de recursos de red que son utilizados en la nube computacional.

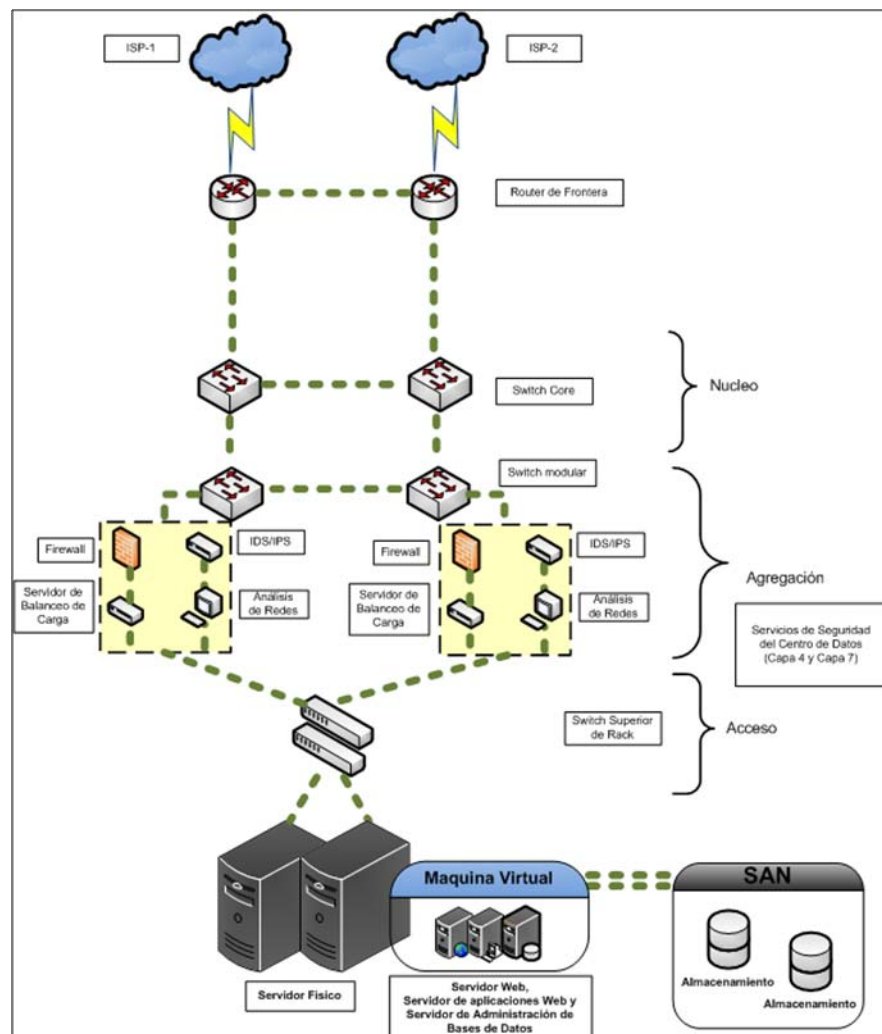


Figura 4.7 Diseño Topológico del Plan de Servicio Plata

Máquinas Virtuales	2 máquinas instaladas en dos servidores
Núcleo de Procesamiento	2 GHz
Memoria RAM	2 Gb a 8 Gb
Espacio de Almacenamiento	1Tb
Raid de almacenamiento	2 Raid con 5 dispositivos cada uno
Servicio de Seguridad	Firewall, IDS/IPS, Balanceador de carga y analizador de red

Tabla 4.5 Característica del Servicio de Plata

- **Oro:** El servicio de Oro de nuestro Centro de Datos consiste en tres máquinas virtuales que estarán instaladas en dos equipos de servidores que están montados en los gabinetes de la sala de computo, cada máquina virtual cuenta con un doble núcleo de procesador es de 3GHz de 8 GB hasta 16 GB de memoria y un espacio de almacenamiento de datos de 2 TB.

El servicio de Oro cuenta con 3 Raid de 10 dispositivos de almacenamiento o storage para el almacenamiento de datos, cada dispositivo usa un cableado de fibra canal de 15k, 10k y conectores SATA, los cuales se conectarán entre sí y con los servidores donde correrán las máquinas virtuales.

Las 3 máquinas virtuales del servicio de Oro están conectadas a 3 VLAN cada máquina virtual tiene un solo servicio que puede ser: servicio Web, servicio de Aplicaciones Web y de Base de Datos. Y todos estos servicios están instalados en 5 máquinas virtuales para tener redundancia y carga de balanceo de datos También cuenta con el mejor procesamiento de datos y la mejor utilización de recursos de red dentro de la nube computacional.

Este servicio cuenta con firewall, carga de balanceo en múltiples máquinas virtuales, analizador de red, módulos de IDS/IPS, Gateway XML y servicio WAF.

Máquinas Virtuales	3 máquinas instaladas en dos servidores
Núcleo de Procesamiento	3 GHz
Memoria RAM	8 Gb a 16 Gb
Espacio de Almacenamiento	2Tb
Raid de almacenamiento	3 Raid con 10 dispositivos
Servicio de Seguridad	Firewall, IDS/IPS, Balanceo de carga, Gateway XML, IP Seguro y analizador de red

Tabla 4.6 Característica del Servicio de Oro

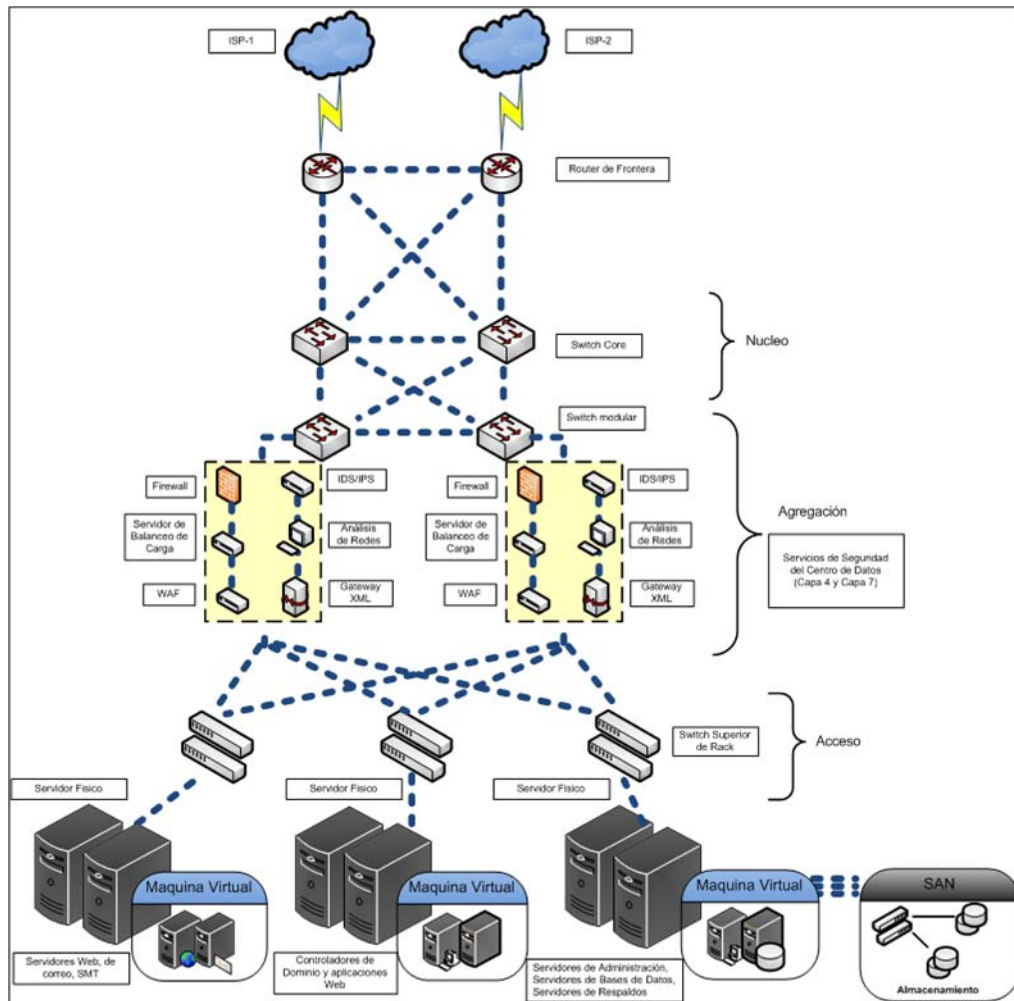


Figura 4.8 Diseño Topológico del Plan de Servicio Oro

4.3.1.4 Servicios de Colocación

Este servicio le permite a los clientes que ya poseen servidores trasladarlos a nuestras instalaciones con el fin de que estos equipos funcionen en un ambiente diseñado principalmente para brindar las condiciones óptimas de operación, tales como protección y respaldo eléctrico, seguridad física y lógica, protección contra incendios, ambiente controlado (humedad y temperatura adecuadas para equipos de cómputo), anchos de banda por demanda, respaldos de información y otros.

El servicio de colocación o housing permitirá al cliente arrendar un espacio físico para el alojamiento de equipos, los espacios disponibles ofrecidos son:

- Espacio en Rack(1 rack y ½ rack)
- Espacio en Jaula(metro cuadrado)

El servicio de arrendamiento de espacio físico cuenta con firewall, detección de intrusos, VPN's, respaldo de datos, sistemas eléctricos y generadores redundantes.

5 ANÁLISIS DE COSTOS Y ELÉCTRICO

5.1 Presupuesto

En el presente capítulo se realizará una estimación de los costos de inversión para la implementación de un Centro de Datos, únicamente se considerará los costos de los enrutamiento, rack, sistema de cableado, sistema eléctrico, sistema mecánico, puesta a tierra, centro de operaciones y cuarto de computo.

A continuación se presenta la inversión que se requiere sólo en materiales para la implementación de un Centro de Datos

Enrutamiento.

Cantidad (Unidades)	Descripción	Valor Unitario	Valor Total
455	Canaleta de Ranura	37.80	17,199.00
455	Unión de Canaletas	3.84	1,747.20
1300	Soporte de Canaleta Metálica	3.00	3,900.00
169	Tubería Metálica 1"	6.56	1,108.64
450	Tubería Metálica 3/4"	4.50	2,025.00
195	Uniones de Tubería 1"	0.70	136.50
195	Conectores de tubería 1"	0.72	140.40
400	Conectores de Tubería 3/4"	0.48	192.00
520	Uniones de tubería 3/4"	0.48	249.60
260	Cajas de Revisión	0.96	249.60
325	Cajas Rectangulares	0.96	312.00
400	Material de Sujeción	2.40	960.00
			28,219.94

Tabla 5.1 Presupuesto de Enrutamiento

Sistema Cableado

Subsistemas	Componentes	Cantidad	Unidad	Valor Total
Cableado Horizontal	Cable UTP Cat 6	100	1.30	130
	Jacks RJ-45 Cat 6	500	13.2	6,600
Area de Trabajo	Patch Cord UTP Cat 6	25	3.72	93
Cuarto de Telecomunicaciones y Equipo	Patch Panel Cat 6 con 24 puertos RJ-45	13	96	1,248
	Organizador horizontal 60x80	13	63.5	825.5

	Patch Cord UTP Cat 6	25	11.85	296.25
	Fibra Optica	50	5.15	257.50
				8,624. 75

Tabla 5.2 Presupuesto de Sistema Cableado

Sistema Eléctrico

Descripción	Cantidad	Precio	Total
Switch de Transferencia Automatica	1	6,000	6,000
Power Distribution Unit (PDU)	2	14,772 .86	29,545.72
UPS 40-200kVA, 480V, 60Hz	2	50,192 .55	100385.1
Generador 290KW a 60 Hz	1	4,100	4,100
			140,030.82

Tabla 5.3 Presupuesto de Sistema Eléctrico

Sistema Mecánico

Descripción	Cantidad	Precio	Total
Aire Acondicionado del Cuarto de Computo(CRAC)	4	1467.25	5869

Tabla 5.4 Presupuesto de Sistema Mecánico

Puesta a Tierra

Descripción	Unidad	Cantidad	Precio	Total
Cable de cobre	metro	116	9.95	1,154.2

desnudo 2 AWG				
Tira para enlace a tierra	unidad	12	103.35	1,240.2
Kit RGCBNJ660P22 (jumper #6 + HTAP)	unidad	18	7,2387	1,311.66
Kit RGEJ1024PFY (jumper #10 + 2 conectores doble perforación)	unidad	45	40.41	1616.4
Barra de tierra para rack	unidad	8	20	160
TGB	unidad	8	88	704
TMGB	unidad	8	132.84	1,062.72
Abrazadera de aterrizaje U-Bolt de bronce	unidad	70	10.80	756
Conector de bandejas Grifequip	unidad	70	11.70	819
Cable #6 AWG	metro	428	3.38	1446.64
Cable #3/0 AWG	metro	70	10.42	729.4
Cable #1AWG	metro	20	13.18	263.6
				11,263.8

				2
--	--	--	--	----------

Tabla 5.5 Presupuesto de Sistema Puesta a Tierra

Cuarto de Cómputo

Rack	Puede contener hasta 42U. Dimensiones 19" X 24".	13	894	11,622
Gabinete para rack	5UR de 19 pulgadas	4	2,320	9,280
Bandeja	Bandejas Deslizables/ Bandejas Extraíbles, peso máximo 16 Kg	500	28.62	14,310
Servidores Blades 3 c/rack (HDA)	1 Tb Intel, Xeon Quad Core, 2.26 Ghz, 6 Gb de RAM	15	3,494.43	52,416.45
Servidores 2 c/rack (HDA)	120 Gb X3430 1P 2GB-U SATA, 4LFF de 6 puertos, conexión en frío, 400 W, PS.	10	1,449.30	14,493.00
Almacenamiento 4 c/rack(SAN)	Servidor de almacenamiento NAS con montaje en rack, discos de 2TB	20	1,500.54	30,010.80
Router	Wireless-G Broadband Router (802.3/3u, 802.11b/g) hasta	3	1,239.00	3,717.00

	54Mbps			
Monitor	Pantalla LCD de 17 pulgadas, consta de 8 puertos.	13	1,643.14	21,360.82
Teclado, mouse	Teclado de elegante diseño con Funciones Multimedia. Mouse Óptico de alta resolución para trabajar eficientemente.	13	94.99	1,234.87
Multiplexor KVM	Tiene 8 puertos para montaje en Rack	13	1,979	25,727
Por cada Rack	Patch Paneles de 24 puertos	13	103,00	1,339.00
Por cada Rack	Bandeja de Fibra Óptica	13	133,00	1,729.00
Por cada Rack	Patch Cord Fibra Óptica 2m	13	58,70	763.10
Por cada Rack	Switch 3Com Baseline Switch 2924-SFP Plus	13	564,48	7,338.24
				195,341.28

Tabla 5.6.Presupuesto de Cuarto de Cómputo

Centro de operaciones

Computadoras		2	200.00	400.00
Teléfono	Agenda: 50 registros, puerto datos, restricción de llamadas, rellamada, tecla R (flash), manos libre.	1	165.00	165.00
				565.00

Tabla 5.7 Presupuesto de Centro de Operaciones

A continuación se resume el costo total que se requiere para la implementación del presente proyecto.

Enrutamiento	28,219.94
Sistema de Cableado	8,624.75
Sistema Eléctrico	140,030.82
Sistema Mecánico	2934.5
Puesta a Tierra	11,263.82
Cuarto de Computo	195,341.28
Centro de Operaciones	565
	386,980.11

Tabla 5.8 Costo del Proyecto

En toda empresa es necesario realizar la evaluación del Proyecto, para así determinar su viabilidad; considerando varios aspectos que permitan determinar en qué medida el Proyecto va a ser rentable, la evaluación se basa normalmente en el estudio.

5.2 Análisis Eléctrico del Centro de Datos

Como habíamos revisado en los capítulos anteriores el análisis eléctrico del centro de datos se lo resume de la siguiente manera:

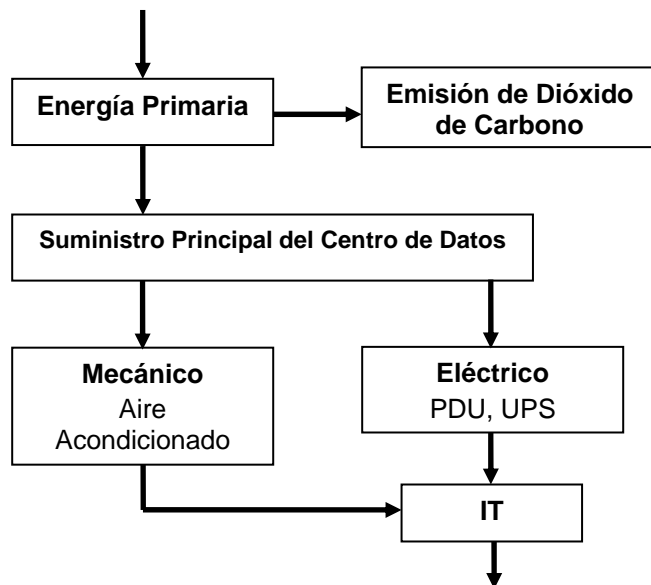


Figura 5.1 Análisis Eléctrico del Centro de Datos

La energía primaria proviene de dos fuentes eléctricas la de las líneas eléctricas de la ciudad y la del generador de energía, ambas proporcionan un voltaje alterno que deberá estar conmutado por el ATS.

El Centro de Datos tendrá una planta de generación redundante con una autonomía de 96 horas continuas de suministro de 100% de carga,

La planta de energía constará de tres generadores de 800kW sincronizados con capacidad de carga de 1,6 MW más 800 kW de reserva, estableciendo una redundancia N+1. Al estar conectados los generadores en paralelo se incrementarán el coste, pero mejorarán la fiabilidad estadística en comparación con un solo generador primario.

Para establecer un estimado de potencia que consumirá el centro de datos se debe sumar las potencias de los equipos que van a utilizarse entre ellos están: equipos de refrigeración, UPS, PDU e iluminación y

servidores. Por lo cual se ha establecido un aproximado de consumo de potencia de energía en la siguiente tabla.

Descripción	Consumo Eléctrico (KW)	Metros Cuadrados	Watt / metros ²
Todo el edificio	2990	15000	0.1993333
Carga de los servidores del Centro de Datos	2000	9000	0.0222222
Unidades CRAC del Centro de Datos	738		0,082
Torre de Enfriamiento	114		0.012666
Contenedor de Pasillos Calientes	2000		0.2222222
Acondicionamiento de espacio de oficina	41	4000	0.01025
Alumbrados	73	1000	0.073
Otros	402	1000	0.402

Tabla 5.9 Consumo de Potencia de Energía

La tabla no indica que el 60% del espacio del centro de datos será se la sala de computo donde se ubicaran los rack y el sistema de refrigeración, el otro 40% se distribuirá entre las oficinas donde habrá un consumo de potencia por lo equipos de computación y aire acondicionado.

Con estos valores se podrá determinar el tamaño de los equipos necesarios en una instalación de centro de datos, tomando en cuenta utilizar un valor de densidad de energía, expresada en vatios por metro cuadrado (W / m^2).

Según los modelos de servidores instalados en los rack y de la carga de trabajo que tenga cada uno de los servidores, el consumo eléctrico oscila de entre ocho a 10 kilovatios por rack para los diferentes servidores. En el mantenimiento de la temperatura de operación se suele necesitar, al menos, un 50 por ciento de la energía consumida por los servidores.

Para valorar la eficiencia energética de los centros de datos, suele utilizarse el indicador *Power Utilization Effectiveness* (PUE). El PUE es la relación entre la electricidad que consumen todos los elementos del Centro de Datos y la que consumen exclusivamente los servidores. Un Centro de Datos será más eficiente cuanto más se acerque su PUE a 1.

5.3 Análisis del Mercado Objetivo versus al servicio ofrecido

A continuación presentemos un breve análisis que debería contar nuestro mercado objetivo, especificando que tipo de servicio ellos deberían contar:

MERCADO	SERVICIO	DESCRIPCION
PYMES	BRONCE - PLATA	Para este tipo de mercado podemos utilizar un servicio Bronce, por lo que las PYMES como su nombre lo dice son empresas que manejan pequeñas cantidades de información y no sería factible ocupar demasiado recursos en el Data Center. También se podría

		ofrecer un servicio Plata más seguro en comparación con el de Bronce, a un coste mayor. Esto depende de las necesidades del mercado, y de cuanto desea invertir en tecnología, para ello existen estas dos alternativas.
CORPORACIONES	PLATA	Este mercado se puede adaptar a la forma de un servicio de Plata debido a que se ofrece un servicio más seguro, garantizado la disponibilidad de sus sistemas. Para este tipo de servicio se usan equipos de seguridad más avanzados, los cuales no se ofrecen en un servicio de Bronce, por ello es muy importante definir en las entidades Corporativas sus políticas de seguridad para definir las en nuestro servicio del Data Center.
ENTIDADES FINANCIERAS	ORO	Para el mercado de las Entidades Financieras se va a ofrecer el servicio de Oro, por el motivo que al ser una entidad financiera maneja mucha información de alta confidencial de muchas personas o negocios por lo que los datos deben estar seguro para cualquier ataque ya sea físico o lógico y disponible para los usuarios en cualquier momento utilizando la tecnología del cloud computing. Junto a este servicio se adjuntara el servicio de recuperación de desastres que consisten en respaldo.
SERVICES PROVIDER	ORO - PLATA	El mercado de Services Provider o proveedores de servicios están muy ligados a los servicios de SaaS del Cloud Computing ofreciendo servicios de aplicaciones o software a sus usuarios finales por lo cual va a utilizar los servicios de Oro y

		<p>Plata.</p> <p>Los dos tipos de servicios contarán con la disponibilidad de conexión que requieren los servicios de aplicaciones y al ser servicios de tipos web deben contar con la seguridad correspondiente para cualquier ataque y tener un buen manejo para servidores dedicados.</p>
--	--	--

Tabla 5.10 Mercado Objetivo Vs. Servicios

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones son:

1. Las diferentes normas necesarias para el diseño de infraestructura de red, se puede concluir que no siempre se cumplirán en su totalidad ya que las características de las instalaciones de un edificio y las exigencias del cliente serán las que definan el diseño real. Lo que se debe procurar es buscar solución que más se acerque a las recomendaciones de las diferentes normas.
2. La solución que se plantea es independiente de la tecnología y equipos que se usen, prueba de esto es que todo fue diseñado sin referencia alguna de las técnicas que utilizarán los dispositivos mostrados.
3. El diseño de una red en la actualidad debe ser analizado profundamente, es importante citar algunos factores que influyen para lograr un buen diseño, entre estos tenemos: la flexibilidad con respecto a los servicios soportados, la vida útil requerida, el tamaño de las instalaciones, la cantidad de usuarios que requerirán los servicios de una red y lo esencial los costos que implican. Al tomar en cuenta estos factores no se debe dudar en utilizar el mecanismo que provea las facilidades de estandarización, orden, rendimiento, durabilidad, integridad y la facilidad de expansión como lo provee el cableado estructurado.

4. Para la instalación de los componentes y accesorios utilizados dentro de las diferentes áreas del sistema de cableado estructurado, tales como: rack's de piso o pared, paneles de conexión, conectores de fibra o cualquier otro tipo de hardware se deben seguir las instrucciones proporcionadas por el fabricante de cada elemento con el objeto de realizar una instalación correcta.
5. Para mejorar el consumo eléctrico del Centro de Datos se instalara en los servidores maquinas virtuales mejorando la eficiencia y disminuyendo tanto la carga que consume los equipos como el espacio en los rack.
6. Teniendo en cuenta las medidas del Centro de Datos se estableció un aproximado de cuanto es la potencia consumida por el Centro de Datos y con esto se podrá instalar los diferentes equipos de suministros de energía de la mejor manera para compensar la potencia consumida.
7. Usando la tecnología de los IPS/IDS en puntos estratégicos de la red, nos permite ofrecer mayor confiabilidad y robustez en el desempeño de nuestros servicios, garantizando la seguridad de la red en el Data Center. Por tanto es muy importante al momento de escoger y configurar los equipos, la persona encargada de administrar debe tener un amplio conocimiento en cuanto al desempeño, características y coste de los equipos para poder aprovechar las funcionalidades que ofrecen los IPS/IDS.

8. Además del establecimiento de políticas de red en las organizaciones se podrá dar una verdadera solución de seguridad a la red y sus respectivos usuarios.
9. El Cloud Computing en la actualidad está en auge, debido a su gran utilidad en el mercado, y apoyo a las entidades de cualquier área de negocio.
10. Tiene muchas ventajas la virtualización porque ayuda a reducir costos, reduce el tiempo de espera en recuperación a fallo, puede garantizar la seguridad en los activos de la empresa a una menor inversión.

Las principales recomendaciones para este tipo de proyectos son:

1. Una coordinación constante tanto con el cliente como con el arquitecto del edificio. Ya que lo ideal es que la infraestructura de telecomunicaciones este prevista desde el inicio de la construcción del edificio y no tratar de acoplarla luego que la construcción esté finalizada, como sucedió en este caso.
2. Se recomienda que al implementarse esta solución, se haga una certificación de la red ya que los estándares lo recomiendan. Esto será de suma importancia para ubicar posibles fallas en la instalación.
3. Se recomienda asegurar que los voltajes requeridos para los equipos deben ser menores o iguales al del generador central, para así evitar algún tipo de sobrecarga al mismo.
4. Seleccionar una buena plataforma de virtualización que cumpla con las necesidades que se desea alcanzar.
5. Definir de una manera adecuada los equipos a utilizarse, tomando en consideración la plataforma de virtualización escogida, y así evitar que se produzca errores en la ejecución de las aplicaciones de los clientes.
6. Se debe profundizar aún más los conocimientos relativos a la seguridad en redes, para poder estar preparados con un plan de recuperación ante cualquier posible amenaza que pueda surgir, una vez que se encuentre en producción los servicios del Data Center.

7. Se debe cumplir con las políticas de seguridad de la organización, antes de realizar cualquier modificación en los parámetros de configuración de los dispositivos de red, ya que es importante extraer copias de seguridad de la información que es relevante para la organización.
8. Para realizar una administración adecuada de la red se recomienda considerar aspectos como el monitoreo, atención a fallas y seguridad, por lo que se deberá contar con un administrador de red que la mantenga activa, resuelva problemas eventuales que se puedan presentar en cuanto a permisos y autorizaciones de acceso y además realice un mantenimiento periódico tanto de hardware como de software.
9. El aumento y la gravedad de los ataques hoy en día hacen que los sistemas de detección de intrusos sean una parte indispensable de la seguridad. El sistema IDS/IPS reportará las amenazas que pueden respaldar las sospechas de que la red de la compañía está siendo atacada. Además, entender la frecuencia y los tipos de ataques le permite a la organización determinar los controles de seguridad que se deben adoptar.
10. El sistema IDS/IPS también simplifica la tarea de verificar y categorizar las amenazas en los informes que se presentan a la administración

ejecutiva. Esta información sólida ayuda a la dirección a aceptar la administración de la seguridad adicional.

11. Para evitar los falsos positivos se recomienda utilizar sensores, que puedan detectar anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

BIBLIOGRAFÍA

- 1.- George Gilder, "Las fábricas de la información",
http://www.wired.com/wired/archive/14.10/cloudware.html?pg=1&topic=cloudware&topic_set=, Octubre del 2006
- 2.- Salesforce.com Spain S.L, "Cloud Computing según Salesforce",
<http://www.salesforce.com/es/cloudcomputing/>, 2010
- 3.- Movistar, "Cloud Computing", <http://www.mcloud.cl/>, 2010
- 4.- Zeroth, "Concepto general de la Wikipedia sobre el Cloud Computing",
http://es.wikipedia.org/wiki/Computaci3n_en_nube, 11 de Febrero del 2011.
- 5.- Andrea Cummins, "Ventajas y desventajas de la computaci3n en nube",
<http://geeksroom.com/2010/04/16293/16293>, 14 de Abril del 2010
- 6.- Víctor Fernández y Javier Leyton, "Aplicando el Cloud Computing",
<http://profesores.elo.utfsm.cl/~agv/elo322/1s10/project/reports/cloudcomputing-10s01.pdf>, 14 de Julio del 2010.
- 7.- Tango/04 Computing Group, "Referencia de acuerdos de SLA para los Data Center en España",
<http://www.barcelona04.com/publicdocs/SLA.doc>, Mayo del 2001
- 8.- Giovanni Silva, "Centro de Datos de Alta Disponibilidad",
http://www.amereiaf.org.mx/congreso2008/materiales/experiencias/Datacenter_dealta_disponibilidad.pdf, 27 de Noviembre del 2008

- 9.- AST Security IT Infrastructure, “CDP del Futuro Seguro, Modular, Escalable y Ecológico”,
http://tunelcarpiano.s3.amazonaws.com/contenido/datacenter09/Ponencia_02_Datacenter09-AST-EL_CPD_del_Futuro.pdf, Junio del 2009
- 10.- Osmo Kuusisto, “La Arquitectura de un Data Center Eficiente”,
http://www.isertec.com/datacenter_summit/_pres_pdf/003-10a_m_-Osmo_Kuusisto_La_Arquitectura_en_un_Data_Center_Eficiente.pdf, 26 de Febrero de 2010
- 11.- WordPress & the Atahualpa, “Centro de Referencia TIC del Noroeste”,
<http://blog.centrodereferenciatic.es>, 20 de Diciembre de 2010,
- 12.- Ing. Marjorie Montalvo Morán, Jefe Data Center R1 - Telconet S.A, 2010.
- 13.- PIEME LTDA - Soluciones integrales de Sistematización, “Tipos de seguridad en una red”,
http://www.pieme.us/home/index.php?option=com_content&view=article&id=64&Itemid=, Octubre del 2010
- 14.- BluePlanet, “Servidores Dedicados”,
http://www.blueplanet.cl/servidores_dedicados.php, Julio del 2009
- 15.- Cisco, “Seguridad y Virtualización en el Data Center”,
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.html, Octubre del 2010
- 16.- My IT Provider, “Descripción del Cableado y Servicios en una Red”,
http://www.my-it-provider.com/structured_cabling.html, Agosto del 2009

17.- Jhon Cárdenas, "Protocolos de Seguridad en un Data Center",

http://www.slideshare.net/JHONCARDENAS/seguridad-protocolos-3156630?src=related_normal&rel=3195926, Noviembre del 2009

18.- Hostalia, "Contrato SLA para un Data Center",

<http://www.hostalia.com/contratar/contrato.html>, Septiembre del 2001

ANEXOS

Anexo 1: Cuestionario de Certificación para la Norma PCI-DSS

Atestación de cumplimiento, SAQ C

Instrucciones para la presentación

El comerciante debe completar esta Atestación de cumplimiento como una declaración de su estado de cumplimiento con los *Requisitos de la Norma de seguridad de datos de la industria de tarjetas de pago (PCI DSS) y procedimientos de evaluación de seguridad*. Complete todas las secciones aplicables y remítase a las instrucciones de presentación en “Cumplimiento con la PCI DSS: Pasos para completar el proceso” en este documento.

Parte 1. Información de la empresa del evaluador de seguridad certificado (QSA) (si corresponde)

Nombre de la empresa:		
Nombre del contacto del QSA principal:		Cargo:
Teléfono:		Correo electrónico:
Dirección comercial:		Ciudad:
Estado/Provincia:		País: Código postal:
URL:		

Parte 2. Información de la organización del comerciante

Nombre del contacto:		
DBA (S):		Cargo:
Teléfono:		Correo electrónico:
Dirección comercial:		Ciudad:
Estado/Provincia:		País: Código postal:
URL:		

Parte 2a. Tipo de empresa comerciante (marque todo lo que corresponda):

<input type="checkbox"/> Comercio minorista	<input type="checkbox"/> Telecomunicaciones	<input type="checkbox"/> Tiendas de comestibles y supermercados
<input type="checkbox"/> Petróleo	<input type="checkbox"/> Comercio electrónico	<input type="checkbox"/> Pedidos por correo/teléfono
<input type="checkbox"/> Otros (especifique):		

Enumere las instalaciones y ubicaciones incluidas en la revisión de la PCI

DSS:

Parte 2b. Relaciones

¿Está relacionada su empresa con uno o más terceros proveedores de servicios (por ejemplo, puertas de enlace, empresas de hosting web, agentes de reservas aéreas, agentes de programas de lealtad, etc.)?

<input type="checkbox"/> Sí	<input type="checkbox"/> No
-----------------------------	-----------------------------

¿Está relacionada su empresa con más de un adquiriente?

<input type="checkbox"/> Sí	<input type="checkbox"/> No
-----------------------------	-----------------------------

Parte 2c. Procesamiento de transacciones

Aplicación de pago en uso:	Versión de la aplicación de pago:
----------------------------	-----------------------------------

Parte 2d. Elegibilidad para completar el SAQ C

El comerciante certifica que es elegible para completar esta versión abreviada del Cuestionario de autoevaluación porque:

- El comerciante tiene un sistema de aplicación de pago y una conexión a Internet o a la red pública en el mismo dispositivo.
- El sistema de aplicación de pago/dispositivo de Internet no está conectado a ningún otro sistema dentro del entorno del comerciante.
- El comerciante no almacena datos del titular de la tarjeta en formato electrónico.
- Si el comerciante almacena datos del titular de la tarjeta, éstos sólo están en informes impresos o copias de recibos impresos y no se reciben electrónicamente.

- El proveedor del software de la aplicación de pago del comerciante utiliza técnicas seguras para proporcionar asistencia remota al sistema de aplicación de pago del comerciante.

Parte 3. Validación de la PCI DSS

Según los resultados observados en el SAQ C de fecha *(fecha en que se completó)*, *(nombre de la empresa comerciante)* declara el siguiente estado de cumplimiento (marque uno):

- En cumplimiento:** Se han completado todas las secciones del SAQ de la PCI y se ha respondido “sí” a todas las preguntas, lo que resulta en una calificación general de **EN CUMPLIMIENTO**, y se ha completado un escaneo de aprobación con un proveedor aprobado de escaneo del PCI SSC, por lo tanto *(nombre de la empresa del comerciante)* ha demostrado un cumplimiento total con la PCI DSS.
- Falta de cumplimiento:** No se han completado todas las secciones del SAQ de la PCI, o se ha respondido “no” a algunas preguntas, lo que resulta en una calificación general de **FALTA DE CUMPLIMIENTO**, o no se ha completado un escaneo de aprobación con un proveedor aprobado de escaneo del PCI SSC, por lo tanto *(nombre de la empresa comerciante)* no ha demostrado un cumplimiento total con la PCI DSS.

Fecha objetivo para el cumplimiento: Es posible que se exija a una entidad que presente este formulario con un estado de Falta de cumplimiento que complete el Plan de acción en la Parte 4 de este documento. *Verifique con su adquirente o con las marcas de pago antes de completar la Parte 4, ya que no todas las marcas de pago requieren esta sección*

Parte 3a. Confirmación del estado de cumplimiento

El comerciante confirma que:

- El Cuestionario de autoevaluación C de la PCI DSS, Versión (*versión del SAQ*), se completó de acuerdo con las instrucciones correspondientes.
- Toda la información dentro del arriba citado SAQ y en esta atestación representa razonablemente los resultados de mi evaluación en todos los aspectos sustanciales.
- He confirmado con mi proveedor de la aplicación de pago que mi sistema de pago no almacena datos confidenciales de autenticación después de la autorización.
- He leído la PCI DSS y reconozco que debo mantener el pleno cumplimiento de dicha norma en todo momento.
- No hay evidencia de almacenamiento de datos de banda magnética (es decir, de pistas)¹, datos de CAV2 (Valor de autenticación de la tarjeta 2), CVC2 (Código de validación de la tarjeta 2), CID (Número de identificación de la tarjeta) o CVV2 (Valor de verificación de la tarjeta 2)²ni

de datos de PIN3 después de la autorización de la transacción en NINGÚN sistema revisado durante esta evaluación.

Parte 3b. Acuse de recibo del comerciante

Firma del director ejecutivo del comerciante	Fecha
Empresa comerciante representada	Cargo
Nombre del director ejecutivo del comerciante	

Parte 4. Plan de acción para el estado “Falta de cumplimiento”

Seleccione el “Estado de cumplimiento” correspondiente para cada requisito. Si responde “NO” a alguno de los requisitos, deberá indicar la fecha en que la empresa estará en cumplimiento con dicho requisito y una breve descripción de las medidas que se están tomando para tal fin. *Verifique con su adquirente o con las marcas de pago antes de completar la Parte 4, ya que no todas las marcas de pago requieren esta sección.*

Requisito de la PCI DSS	Descripción del requisito	Estado de cumplimiento (seleccione uno)		Fecha y medidas de Corrección (si el estado de cumplimiento es “NO”)
		SÍ	NO	
1	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.			

2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.			
3	Proteger los datos almacenados del titular de la tarjeta.			
4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.			
5	Usar y actualizar periódicamente un software antivirus.			
6	Desarrollar y mantener sistemas y aplicaciones seguros.			
7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.			
8	Asignar una ID exclusiva a cada persona que tenga acceso por computadora.			
9	Restringir el acceso físico a los datos del titular de la tarjeta.			
11	Probar			

	periódicamente los sistemas y procesos de seguridad.			
12	Mantener una política que aborde la seguridad de la información.			

Anexo 2: Acuerdo SLA

El presente acuerdo tiene por objetivo regular las condiciones en las que el contraparte accede y utiliza los SERVICIOS DE PLAN elegido, así como fijar las condiciones y forma de remuneración del contraparte a SCDCP.

De otra parte, el Servicio Centro de Dato Cloud Computing (SCDDC) el contraparte (en adelante Cliente), persona física o jurídica que cumplimenta el formulario de contratación y declara conocer y aceptar libremente, tras informarse del servicio y su funcionamiento, el presente contrato.

Ambas partes, SCDCP y CLIENTE, están interesadas en formalizar el presente contrato aceptando los términos y condiciones establecidos en las siguientes condiciones y cláusulas.

1. Servicios regulados por este contrato

Las condiciones recogidas en este contrato serán de aplicación a los siguientes Planes:

- Servicios Compartidos
- Servidores Dedicados
- Hosting Dedicados
- Servidores Virtuales
- Servicio de Colocación

Las características técnicas de cada uno de los servicios, vienen determinadas en este contrato y en sus anexos y se encuentran

permanentemente actualizadas en la página web de www.centrodatos.com/servicios.

SCDCP se reserva el derecho de modificar las características y condiciones de los Servicios regulados por este contrato. Para ello no deberá cumplir más formalidad que la de publicar en su página dicha modificación, informando al cliente con un aviso on-line y/o remitirlo por correo electrónico.

El cliente, una vez le sea comunicada la modificación correspondiente, dispone del plazo de 7 días para resolver el contrato si no estuviera de acuerdo con las nuevas circunstancias, obteniendo la devolución del pago de la parte proporcional no consumida. Ahora bien, pasado este plazo sin comunicación en contrario, se entenderá que acepta las nuevas condiciones y, por lo tanto, la baja antes del vencimiento no dará lugar a devolución alguna, salvo en aquellos casos en los que la legislación vigente prevea lo contrario.

2. Precio y forma de pago

Por la disponibilidad del Servicio contratado, el cliente pagará a SCDCP el precio correspondiente que se recoge en este contrato y en sus anexos y siempre actualizado en nuestra página web.

La periodicidad de pago de los Servicios será trimestral o anual, según cual haya sido la elección del cliente, durante la contratación, de entre las

ofrecidas por SCDCP para cada Servicio y recogidas en los anexos de este contrato.

Las ampliaciones contratadas para los Servicios tendrán la misma periodicidad (trimestral o anual) que tenga al Servicio que se asocien, excepto en el caso de la transferencia que será siempre mensual.

La Forma de pago de los Servicios será siempre por adelantado en el momento de su contratación y se realizará domiciliación bancaria o transferencia bancaria.

La renovación de los Servicios también se abonará por adelantado, mediante domiciliación bancaria en la cuenta corriente facilitada por el cliente (método recomendado) o a través de transferencia.

En el caso de las ampliaciones, la forma de pago será mediante domiciliación bancaria o transferencia bancaria en su primera contratación y su renovación se realizará de forma automática mediante domiciliación bancaria (método recomendado) o a transferencia.

SCDCP no iniciará las gestiones relativas a la solicitud correspondiente mientras no reciba el importe de estos servicios a través de los medios de pago indicados en cada caso.

SCDCP se reserva el derecho a suspender la prestación del servicio contratado ante cualquier incidencia experimentada en el cobro hasta la resolución de la misma. Si el cliente no procediera a su pago después del

previo aviso y de la suspensión temporal causará baja definitiva el servicio por incumplimiento del contrato por su parte.

La desactivación por impago supondrá la eliminación de todos los datos asociados al Plan de Hosting. Si el cliente vuelve a contratar dicho Plan, deberá dar de alta de nuevo todos los datos.

SCDCP se reserva el derecho a modificar el precio a los Servicios regulados por este contrato. En dicho caso, se notificará al cliente tal modificación antes de que se vea afectado por la variación en la siguiente factura que se le emita, de manera que si no estuviera de acuerdo en aceptar dicho cambio ejercite el derecho a resolver el presente contrato causando la baja del servicio en el momento que finalice el periodo que tuviera pagado.

3. Entrada de vigor, duración y prórroga

El presente contrato entra en vigor en el momento de su formalización, es decir, cuando una vez abonado el Servicio contratado, el cliente tiene la posibilidad de acceder al mismo.

El contrato tendrá duración trimestral o anual, dependiendo del plazo de facturación elegido por el cliente en el formulario de contratación, a partir de la formalización del contrato y se prorrogará de forma automática por idénticos periodos de tiempo.

El contrato no se dará por finalizado mientras el cliente no proceda a dar de baja el Servicio mediante notificación escrita a SCDCP. La baja será

automática y se producirá en ese mismo momento, lo que deberá ser tenido en cuenta para evitar la pérdida de la información alojada en el servidor.

Las ampliaciones para el Servicio contratado pueden activarse o desactivarse en cualquier momento mientras el Servicio se encuentre activo y al corriente del pago; ahora bien si una ampliación tiene un coste mensual adicional, el hecho de desactivarla antes de que venza el mes pagado por adelantado no supone la devolución de la parte proporcional no consumida, salvo en aquellos supuestos en los que la legislación vigente prevea lo contrario.

4. Obligaciones y responsabilidades de SCDCP

SCDCP no puede garantizar que la disponibilidad de los Servicio sea continua e ininterrumpida durante el periodo de vigencia del contrato, debido a la posibilidad de problemas en la red Internet, averías en los equipos servidores que son compartidos y otras posibles contingencias imprevisibles.

SCDCP se reserva el derecho a interrumpir el Plan contratado en función de reparaciones técnicas y de mantenimiento de los equipos, así como para la mejora de los propios servicios. Aunque las tareas de mantenimiento se planifican normalmente en horarios de 00:00 h a 06:00 h con una previa notificación, de darse la necesidad se podrán acometer tareas de reparación y mantenimiento en otros horarios.

Por lo tanto, el cliente acepta soportar dentro de los límites razonables riesgos e imperfecciones o indisponibilidad de los servidores y renuncia expresamente a reclamar cualquier responsabilidad, contractual o extracontractual, daños y perjuicios a SCDCP por posibles fallos, lentitud o errores en el acceso y uso del Servicio contratado, sin perjuicio de lo dispuesto en la legislación vigente.

SCDCP no es responsable de aquello que le sea exclusivamente imputable al cliente. El acceso y uso de los Servicios es responsabilidad exclusiva del cliente, de tal manera que SCDCP no se hace responsable de ninguna manera (ni directa ni subsidiaria) de cualquier daño directo o indirecto, que el cliente pudiera ocasionar a terceros.

No obstante todo lo anterior, si SCDCP incumpliera los compromisos asumidos en este contrato por prestar un servicio ineficiente durante un periodo ininterrumpido superior a 24 horas, la responsabilidad de SCDCP se limitará a la devolución del dinero cobrado por el Servicio afectado durante dicho periodo de interrupción calculado de manera proporcional.

SCDCP realiza copias de seguridad, sin embargo no se responsabiliza de la pérdida o del borrado accidental de los datos. De igual manera, no se garantiza la reposición total de estos datos debido a que en el tiempo transcurrido entre la última copia y el borrado, los datos han podido cambiar. El Servicio contratado no incorpora en el precio la reposición de los contenidos salvados a través de las copias de seguridad realizadas por

SCDCP cuando esta pérdida sea provocada por causa imputable al cliente; la reposición sólo queda incluida en el precio del Servicio cuando la pérdida del contenido sea debida a causas atribuibles a SCDCP.

Por este motivo, SCDCP se reserva el derecho a suspender, total o parcialmente, el cumplimiento del contrato en el caso de que advierta, detecte y/o compruebe en sus labores de mantenimiento un consumo excesivo de memoria, de recursos o cualquier otra alteración que ralentice el servidor en el que se encuentra ubicado, de tal manera que perjudique o conlleve un menoscabo en la prestación del servicio o de los derechos de los clientes o terceros que con él comparten el servidor.

SCDCP no se responsabiliza:

- ✓ Del contenido alojado en el espacio atribuido al cliente por el Servicio.
- ✓ De los errores producidos por los proveedores de acceso.
- ✓ De la contaminación por virus en los equipos, cuya protección incumbe al cliente.
- ✓ De las intrusiones de terceros en el Servicio del cliente aunque se hayan establecido medidas razonables de protección.
- ✓ De la configuración defectuosa por parte del cliente.
- ✓ De los deterioros de los equipos o mal uso (responsabilidad del cliente).

Como consecuencia de la naturaleza del Filtro Antivirus Antispam Avanzado, SCDCP no se hace responsable, ni acepta, ninguna reclamación del cliente o

de un tercero, por el rechazo de algún mensaje de correo electrónico legítimo (tanto entrante como saliente), debido, entre otros motivos, a la posible concurrencia con medios técnicos externos de los que disponga el propio cliente.

5. Obligaciones y Responsabilidades del CLIENTE

El cliente debe cumplir con todos los términos y condiciones de este contrato en el ejercicio de su actividad profesional, además deberá actuar lealmente y de buena fe.

El cliente no utilizará el Servicio contratado de una manera contraria a la buena fe, al orden público y a la legislación vigente.

Mediante la contratación de este Servicio, el cliente se compromete a:

- ✓ Guardar por su cuenta una copia de seguridad de los archivos de los Servicio con el fin de reponerlos si fuese necesario.
- ✓ Vigilar el tamaño de la transferencia con el fin de evitar que sufra consecuencias su servicio por corte del mismo al excederse del contratado.
- ✓ El cliente se obliga a mantener operativa, activa y actualizada la dirección e-mail proporcionada en el formulario de contratación para las comunicaciones con SCDCP, ya que constituye el medio de comunicación preferente para la gestión ágil y fluida en la prestación del Servicio solicitado. Si el cliente quiere cambiar la dirección e-mail

facilitada en el formulario de contratación como dirección de contacto deberá comunicarlo a SCDCP, de manera que en ningún momento quede interrumpida la comunicación entre ambas partes contratantes.

El cliente indemnizará a SCDCP por los gastos que ésta tuviera por imputarle en alguna causa cuya responsabilidad fuera atribuible al cliente, incluidos honorarios y gastos de los abogados de SCDCP, incluso en el caso de decisión judicial no definitiva.

Debido a que los Servicios están compartiéndose en los equipos el cliente debe desarrollar y/o administrar su Servicio respetando los estándares técnicos dispuestos por SCDCP. En caso contrario será de aplicación lo dispuesto anteriormente.

6. Nivel de servicio contratado y Fuerza Mayor

El Acuerdo de Nivel de Servicio para los productos indicados en este documento está definido por la disponibilidad y el tiempo de respuesta a incidencias y consultas sobre el servicio.

Se define “disponibilidad” como el cociente entre el tiempo en el que el servicio está disponible y opera correctamente dividido entre el tiempo total.

$$D = \frac{(TSA - TP)}{T} * 100$$

Donde:

- D es la disponibilidad en %

- TSA es el tiempo de servicio acordado (24 horas, 7 días a la semana, excluyendo el tiempo en el que ocurran incidencias de Fuerza Mayor.)
- TP es el tiempo de parada (tiempo durante el que la publicación de páginas web no funciona)
- T es el periodo considerado en el cálculo

Ninguna de las partes será responsable por el incumplimiento de las obligaciones derivadas del contrato cuando dicho incumplimiento se deba a causas de Fuerza Mayor. Si la suspensión en la prestación del servicio por esta circunstancia es superior a 2 meses este contrato se podrá cancelar a petición de cualquiera de las partes.

Se define “tiempo de respuesta” como el tiempo transcurrido desde que se recibe un aviso de incidencia hasta que el personal de SCDCP inicia las tareas de resolución de la incidencias. El horario de asistencia será, en general, el horario de oficina de SCDCP, aunque puede contratarse servicio técnico 24x7 para emergencias. De no tener contratado servicio 24x7 para emergencias, o si la incidencia notificada no interrumpe gravemente el servicio, si el aviso se recibe fuera del horario laboral, se considerará como hora de recepción de un aviso la primera hora de la siguiente jornada laboral. En los servicios indicados en este documento los parámetros de nivel de servicio son:

- Disponibilidad garantizada del 99,5% anual.

- Horario de atención a incidencias: 8x5 (Lunes a Viernes, no festivos, de 9:00 a 14:00 y de 16:00 a 19:00h).
- Tiempo de respuesta de 8 horas laborables.

En caso de no poder cumplir este acuerdo de nivel de servicio por motivos imputables a SCDCP, y tras notificación del cliente, se realizará un descuento sobre la siguiente factura según el siguiente cuadro:

Disponibilidad Alcanzada	Descuento
99%	10%
98%	15%
97%	20%
93%	50
<93%	75%

7. Finalización

El contrato finalizará cuando, las causas legalmente establecidas y las dispuestas en las distintas cláusulas de este contrato, concorra alguna de las siguientes:

- Mutuo Acuerdo de las partes.
- Finalización del período inicial de duración o de las sucesivas prórrogas.
- Resolución por incumplimiento de alguna de las partes de las obligaciones derivadas del Contrato.

Si el incumplimiento del cliente fuera la causa de resolución del contrato, SCDCP se reserva el derecho a terminar de forma anticipada el

presente contrato y, por lo tanto, a desposeer al cliente del servicio sin previo aviso, sin derecho a indemnización ni a devolución de cantidad alguna.

En caso de rescisión del contrato, por las causas anteriormente citadas o cualesquiera otras admitidas en derecho, el cliente deberá cumplir las obligaciones asumidas con anterioridad a la resolución del contrato frente a SCDCP y frente a terceros.

A la finalización del contrato, SCDCP podrá, a su discreción, borrar los contenidos almacenados en el espacio del Servicio. No existirá obligación por parte de SCDCP de eliminar los contenidos de las copias de seguridad. De existir algún software provisto o licenciado por SCDCP al CLIENTE para la ejecución del servicio, éste deberá desinstalarlo al finalizar el contrato.

8. Confidencialidad

Toda información o documentación que cualquiera de las partes aporte a la otra en desarrollo y ejecución del presente contrato se considerará confidencial y exclusiva de quien lo aporte y no podrá comunicarse a terceros sin su consentimiento.

Las partes excluyen de la categoría de información confidencial toda aquella información que sea divulgada por la parte que la posea, aquella que se convierta en pública, aquella que haya de ser revelada de acuerdo con las leyes o con una resolución judicial o acto imperativo de autoridad competente

y aquella que sea obtenida por un tercero que no se encuentre bajo la obligación de confidencialidad alguna.

Esta obligación de confidencialidad persiste hasta dos (2) años después de finalizar este contrato. Ninguna de las partes adquirirá ningún derecho sobre cualquier información confidencial u otros derechos de propiedad de la otra parte como resultado de este contrato.

9. Protección de datos personales

SCDCP adopta las medidas técnicas y organizativas necesarias para garantizar la seguridad, integridad y confidencialidad de los datos de carácter personal conforme a lo dispuesto en la Ley Orgánica 15/99 sobre Protección de Datos de Carácter Personal (LOPD).

SCDCP, observando la normativa vigente en esta materia, informa de que los datos personales que se recogen a través de los formularios de contratación se incluyen en ficheros automatizados específicos de la empresa para el cumplimiento de los servicios, así como para el desempeño de las tareas de información, comercialización y otras actividades propias del grupo.

En aquellos casos en que SCDCP figure como encargado del tratamiento asumirá las obligaciones establecidas en la LOPD y únicamente tratará los datos según las instrucciones del responsable del tratamiento, sin

utilizarlos con fines distintos a los recogidos en el contrato celebrado al efecto.

El interesado podrá, en cualquier momento, ejercitar los derechos de acceso, oposición, rectificación y cancelación reconocidos en la citada LOPD a través de cualquiera de las formas establecidas por la normativa aplicable.

SCDCP no se hace responsable del incumplimiento por parte del cliente de la LOPD en aquello que a su actividad le corresponda y que se encuentre relacionado con la ejecución de este contrato.

El cliente manifiesta que todos los datos facilitados por él son ciertos y correctos, y se compromete a mantenerlos actualizados, enviando un mensaje a SCDCP. El cliente responderá de la veracidad de sus datos y será el único responsable de cuantos conflictos o litigios pudieran resultar por la falsedad de los mismos.

10. Limitación de Garantía y Responsabilidad

En ningún supuesto SCDCP, ni los gerentes y altos cargos, administradores, accionistas, agentes o trabajadores dependientes de ella contraerán responsabilidad alguna por causa, directa o indirecta, relacionada con la utilización que haga el cliente del servicio de SCDCP.

Las partes reconocen que la puesta en vigor de este contrato, no supone ningún tipo de representación, delegación, garantía u otros acuerdos distintos a los expresamente descritos en este contrato; y de acuerdo con

ello, todos los términos, condiciones, garantías u otros aspectos implicados por convenios o reglamentación general, quedan explícitamente excluidos hasta los límites permitidos por la Ley.

12. Acceso a los servicios

12.1. Servicio Compartidos

Si el cliente adquiere este servicio cuenta con las siguientes características.

- ✓ Sistema Operativo Linux
- ✓ Hospedaje de Aplicaciones (Java, PHP, Perl, CGI)
- ✓ Hospedaje de Sitios Web (HTML, PHP, JSP, Servlets)
- ✓ Servicios de Correo Electrónico (SMTP, POP3, IMAP)
- ✓ Servicios de FTP – SSL Compartido
- ✓ WebServer: Apache, Tomcat
- ✓ Servicios de Bases de Datos (MySQL, PostgreSQL y SQL Server)
- ✓ RespalDOS Diarios
- ✓ SSL
- ✓ Seguridad en Puertos
- ✓ Tasas de Transferencia Fijas.

12.2 Servicio Dedicados (Hosting)

Si el cliente alquila este servicio contará con:

- ✓ Linux Server

- ✓ Servidores Intel y AMD
- ✓ Hospedaje de Aplicaciones
- ✓ Hospedaje de Sitios Web
- ✓ Servicios de Correo Electrónico
- ✓ Servicios de FTP
- ✓ Servicios de Bases de Datos (SQL Server, Oracle, MySql)
- ✓ Respaldos Diarios
- ✓ Expansión de Discos SATA
- ✓ Expansión de Memoria
- ✓ Tasas de Transferencia Fijas e ilimitadas

12.3 Servicios Virtuales

El cliente al solicitar este servicio podrá elegir entre tres planes:

✓ Bronce

Características	Bronce
Maquinas Virtuales	1 o 2 maquinas instaladas en un servidor
Núcleo de Procesamiento	1.5 GHz
Memoria RAM	2 Gb a 8 Gb
Espacio de Almacenamiento	100 Gb a 500 Gb
Raid de almacenamiento	1 Raid con 5 dispositivos
Servicio de Seguridad	Firewall y analizador de red

✓ Plata

Características	Plata
Maquinas Virtuales	2 maquinas instaladas en dos servidores
Núcleo de Procesamiento	2 GHz
Memoria RAM	2 Gb a 8 Gb
Espacio de Almacenamiento	1Tb
Raid de almacenamiento	2 Raid con 5 dispositivos cada uno
Servicio de Seguridad	Firewall, IDS/IPS, Balanceador de carga y analizador de red

✓ Oro

Características	Oro
Maquinas Virtuales	3 maquinas instaladas en dos servidores
Núcleo de Procesamiento	3 GHz
Memoria RAM	8 Gb a 16 Gb
Espacio de Almacenamiento	2Tb
Raid de almacenamiento	3 Raid con 10 dispositivos
Servicio de Seguridad	Firewall, IDS/IPS, Balanceo de carga, Gateway XML, IP Seguro y analizador de red

12.4 Servicio de Colocación

El servicio de colocación o housing permitirá al cliente arrendar un espacio físico para el alojamiento de equipos, los espacios disponibles ofrecidos son:

- Espacio en Rack(1 rack y ½ rack)
- Espacio en Jaula(metro cuadrado)

El servicio de arrendamiento de espacio físico cuenta con firewall, detección de intrusos, VPN's, respaldo de datos, sistemas eléctricos y generadores redundantes.

13. Plan de Recuperación de Desastres

Bajo algún desastre en el SCDDC puede ser desde una caída de energía eléctrica por un tiempo mayor a un cierto intervalo, hasta circunstancias de

fuerza mayor como un desastre natural. Automáticamente se realizara el plan de recuperación de desastre que consiste en la recuperación de toda la información que estaba contenido en los diferentes servidores del Centro de Datos.

Fallo de la Energía Eléctrica: Si existe un corte de energía por algún desastre natural o problema en las líneas eléctricas el generador de energía se encenderá automáticamente en treinta segundos y en ese intervalo de tiempo los equipos como computadoras y servidores del SCDDC se mantendrán levantados por las unidades de almacenamiento de energía (PDU).

Incendio fuera del Centro de Datos: Si ocurre un incendio afuera del centro de datos no tendría mayor impacto debido que las paredes cuentan con un revestimiento anti-incendio y alarmas contra-incendios dentro de las instalaciones.

Fallo de Router: Si un router de borde llegara a fallar automáticamente se pondría en funcionamiento el protocolo HRSP, donde el router secundario (stand-by) tomaría la función router principal ayudado por el router virtual.

Fallo de Switch: Si un switch llegara a fallar automáticamente el otro switch tomaría el lugar del switch principal esto se logra usando el protocolo STP.

Backups: Al suceder algún desastre natural o previsto por la seguridad del SCDDC automáticamente se realizara un backup de la información guardada en los servidores para así volver al estado anterior antes del desastre.

Para hacer una correcta realización y seguridad del backups se deberá tener en cuentas los siguientes puntos:

- El almacenamiento de los backups se debe realizar en lugares diferentes en donde reside la información primaria.
- Se debe verificar periódicamente la integridad de los backups que se están almacenando.
- Se debe contar con una política para garantizar la privacidad de la información que se respalda en medios de almacenamiento.