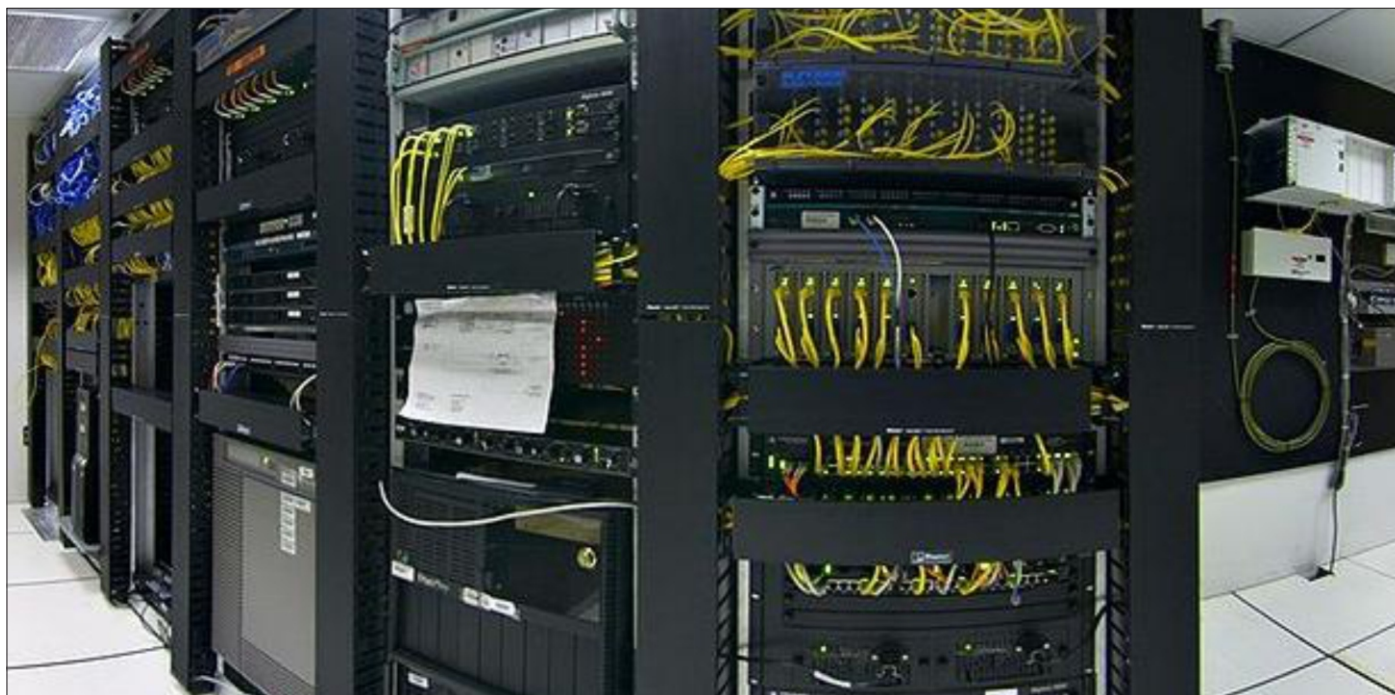




DATACENTER

UNA MIRADA POR DENTRO

Este libro es fruto de un trabajo extenuante de mucho tiempo y esfuerzo, dedicado a los alumnos de Ingeniería de la Universidad Tecnológica Nacional Facultad Regional Tucumán.

Este ejemplar explica los estándares más importantes para un diseño desde cero de una Centros de Datos o Datacenter, desde el inicio hasta la puesta en funcionamiento y explotación.

La ingeniería es una ciencia de integración de conocimiento, transitando por el Diseño Arquitectónico del recinto, El Desarrollo Eléctrico, Elección de la arquitectura del hardware de conectividad y la formación de los Recursos Humanos Administradores.

En estas páginas trate con esfuerzo, de desarrollar una lectura amena al lector, que satisfaga las teorías mas usadas, y que desarrolle la practicidad en puntos de interés a mi criterio importantes. Como ser, niveles de redundancia tanto eléctrica como a equipos de comunicaciones se refiere, topologías de telecomunicaciones y nuevos paradigmas de diseño de procesamiento y/o explotación de información.

Víctor Gabriel Galván Argentino, nacido en la provincia de San Miguel de Tucumán, curso sus estudios universitarios en la Universidad Tecnológica Nacional Facultad Regional Tucumán. Actualmente se desempeña como encargado del Área informática de un Organismo Público del Estado Nacional ORSEP, además de ello es Docente Auxiliar de la Cátedra de Cálculo Numérico.

Actualmente está cursando la Maestría en Administración de Empresas en la Universidad Nacional de Tucumán. Desarrolla consultorías en temas referentes al Diseño y puesta en marcha de Centros de Procesamiento de Información (Datacenter).

ISBN 978-987-33-3467-2



9 789873 334672

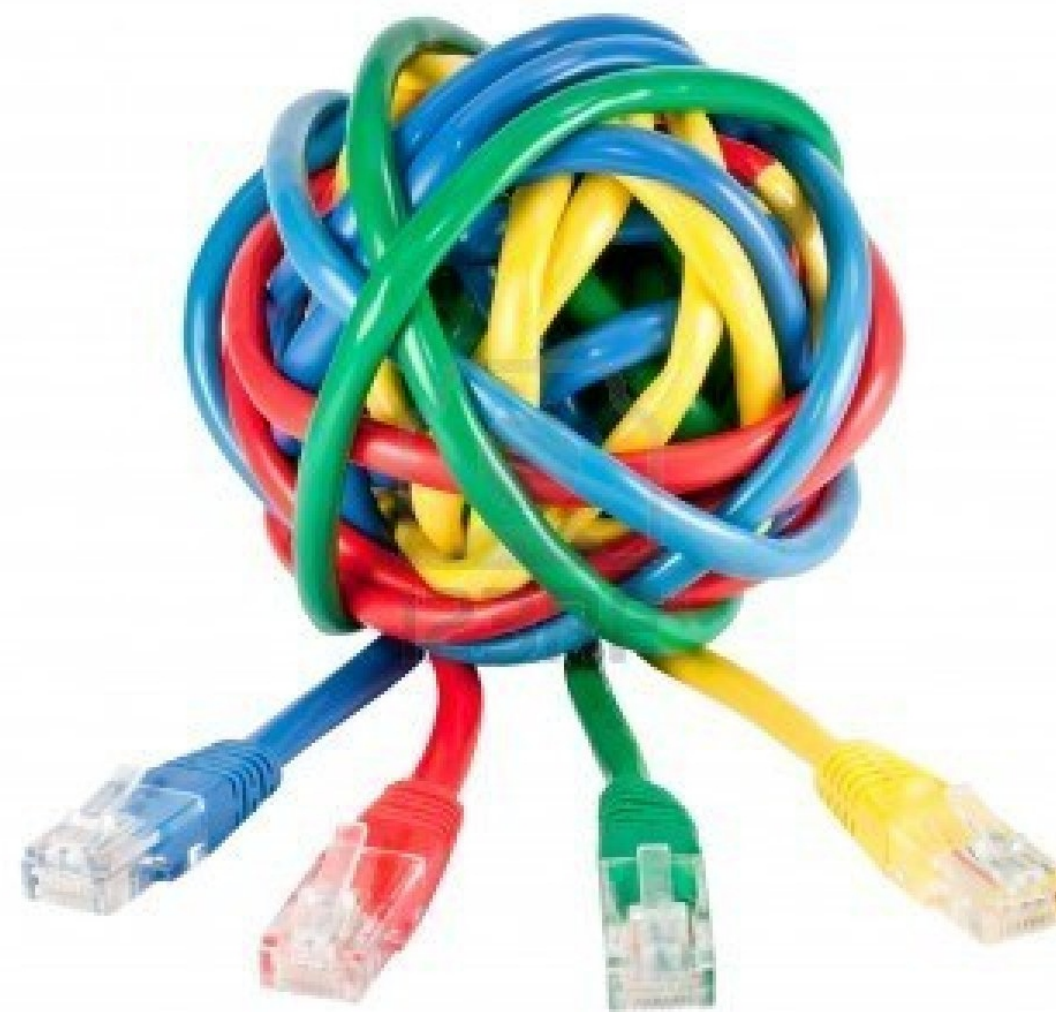
UNA MIRADA POR DENTRO

DATACENTER

Victor Gabriel Galván

DATACENTER

UNA MIRADA POR DENTRO



Ediciones indigo

DATACENTER

UNA MIRADA POR DENTRO

Víctor Gabriel Galván

Ediciones Índigo

Composición y armado: Lic. Diego Ríos.
Diseño de Tapa: Ediciones Índigo.
Corrección: Dra. Silvana Gabriela González.
Prof. Villena Rojas Juan.

Víctor Gabriel Galván

DATACENTER

Una mirada por dentro

1a ed. - SM de Tucumán: Ediciones Indigo,
2013.

190p.; 18x25 cm.

ISBN 978-987-33-3467-2

2014: Ediciones Índigo.
E-mail: indigo-grafica@hotmail.com

Quedan prohibidos, dentro de los límites establecidos en la ley y bajo los apercibimientos legales previstos, la reproducción total o parcial de esta obra por cualquier medio o procedimiento, ya sea electrónico o mecánico, el tratamiento informático, el alquiler o cualquier otra forma de cesión de la obra sin la autorización previa y por escrito del copyright.

Printed and made in Argentina
Hecho e impreso en la República Argentina
ISBN 978-987-33-3467-2

Para papá y mamá que supieron guiarme por el camino
del trabajo, la humildad y la justicia.

Mis hermanas, Adriana, Carolina, Silvina y sobrinas Jazmín y Guillermina,
y la persona que siempre está presente, Silvana,
y por último, mis amigos que supieron acompañarme en este desafío.

La motivación

A lo largo de la escritura de este libro, me di cuenta de la dificultad que conllevó no tanto su escritura ni tampoco el desconocimiento temático sino simplificar conceptos complicados de entender en una lectura y así lograr que puedan quedar en la mente del lector.

La escritura, y la necesaria reescritura, hasta llegar a lo que uno deseaba plasmar, me fue muy placentera, aunque me llevó más de dos años el desafío de superar horas de trabajo frente a una pantalla y repensar técnicas y métodos que se usaban antes y que son usadas, con respecto a lo abordado en este libro, y mejor aún pensar, y porque no soñar, el futuro en lo que se refiere a nuevas tecnologías.

Hoy el sueño de escribir un libro es una realidad al igual que mi profesión, la ingeniería en sistemas de información, que me brinda muchas satisfacciones personales y laborales, ya que es una pasión que llevo en mi corazón y que en momentos como éste que uno se siente extremadamente feliz por poder aportar lo poco o mucho que conoce, ya sea en el pizarrón, en una charla entre colegas y amigos o en un libro como éste.

Simplemente Gracias.

Agradecimientos

Me siento afortunado sabiendo que cumplí con un objetivo más en mi vida, debo agradecer a todos las personas que de una u otra forma me guiaron por el camino del pensamiento, me enseñaron a escuchar y ser crítico, y a emitir juicio justo sobre temas de mi interés, quiero agradecer a la Universidad Tecnológica Nacional Facultad Regional Tucumán, que es mi segunda casa, al Departamento de Sistemas que me llevo por las sendas de mi profesión actual, al Departamento de Electrotecnia donde siento que está mi lugar como docente y alumno, al “ORSEP” Organismo Regulador Seguridad de presas, dependiente de la Secretaria de Obras Públicas de la Nación, Regional Norte, donde desempeño actualmente tareas de mi especialidad. A los colegas del MBA 2012 de la UNT Facultad de Ciencias Económicas, a la comunidad de guardianes de Perón y a ediciones Índigo que realizó todo el diseño del libro.

Por último quiero agradecer a aquellas personas que me ayudaron incondicionalmente en el desarrollo de esta primera edición, que no son pocas.

Ing. Víctor Gabriel Galván

Primer Prólogo

He leído este libro de texto y apreciado su contenido.

Humildemente y sin sentirme especialista en la materia, siento la dedicación y la pasión del autor en cada línea del texto.

Evidentemente el autor estructuró estas líneas, para todas aquellas personas que de algún modo, les interesen el diseño, funcionamiento, métodos y normas, de lo que significa un Datacenter o Centro de Datos.

Me pareció un texto apropiado para estudiantes y técnicos de esta especialidad de la ingeniería, aunque no pueda definir cuál es esa especialidad.

En este libro de texto, el autor aborda con distintos matices, como estructurar diversas tecnologías con un objetivo principal, brindar su investigación de campo para diseñar y proyectar y poner en funcionamiento un Datacenter.

Definitivamente debo decir que me resulto un texto ameno y con aportes importantes para quienes empiezan a transitar este camino impuesto por la cultura de la humanidad, de hoy en día.

Ing. Luis G Pezza

Segundo Prólogo

Luego de leer el libro, la primera sensación que tuve fue una enorme satisfacción por el contenido del mismo. Es un libro de texto de consulta para estudiantes y profesionales, que presenta un pormenorizado análisis sobre el diseño, funcionamiento, métodos y normas de un Datacenter.

Es gratificante ver que jóvenes ingenieros argentinos estén aplicando estas tecnologías en favor del crecimiento y desarrollo de nuestro país. Intervenciones como estas en las ciencias duras, que además se realizan desde Tucumán, continúan aportando al desarrollo de polos tecnológicos en el interior del país.

En este tiempo, donde se recuperaron las banderas de la producción y del trabajo, y cuando se plantea claramente que para seguir en la senda del desarrollo es fundamental fortalecer la formación de nuestros recursos humanos, este tipo de libros son un aporte importante para el crecimiento con inclusión, ya que el conocimiento es el capital más importante de una empresa, de un organismo, de un país.

Argentina posee recursos humanos de excelencia, reconocidos internacionalmente, que en los últimos años vio fortalecidos su sistema universitario y científico-tecnológico, alcanzando estándares de primer nivel. Este libro del ingeniero Víctor Gabriel Galván es un buen exponente de estos objetivos.

Ing. José Francisco López

Secretario de Obras Públicas de la Nación

Índice

La motivación

Agradecimientos

Primer Prólogo

Segundo Prólogo

Breve Resumen Técnico

CAPÍTULO 1 - Introducción

Introducción 15

Que es un Datacenter DC – Centro de Datos – Centro de Respaldo 15

Diseño del Datacenter - DC 15

Diseño de un centro de respaldo 19

Diseño de un Datacenter - El Sincronismo de los datos 20

El Datacenter en un contexto de plan de contingencia 21

El Datacenter - La Información – La Empresa 21

Tendencias de los Datacenter - Componentes 21

CAPÍTULO 2 - Diseño físico

Planeación y diseño de un Datacenter 23

El estándar EIA/TIA-942 23

Objetivos del diseño 23

Detalle del estándar EIA/TIA-942 24

La Infraestructura y el estándar TIA-942 25

TIER I 27

TIER II 28

TIER III 29

TIER IV 30

Conclusión del estándar 33

Requerimientos generales para la implementación de un Datacenter -Estándares 34

CAPÍTULO 3 - Requerimientos

Sistema de aire acondicionado de precisión 37

Diseño del sistema UPS (sistema de energía ininterrumpible) 42

Sistemas de configuraciones UPS más utilizadas en el mercado 45

Estructuras de racks y montajes de equipos de IT 59

Sistemas de conexión a tierra para equipos de cómputo, comunicaciones y/o telecomunicaciones 60

Sistemas de monitoreo ambiental y físico del Datacenter 64

Sistema de detección y extinción de incendios 64

Detectores de incendios 69

Sistema eléctrico 69

Instalación de tableros de distribución eléctrica redundantes requeridos 69

Sistema de iluminación automatizado 69

Adecuaciones físicas 70

Distribución física propuesta del Datacenter 70

Sistema de seguridad y control de acceso 71

CAPÍTULO 4- Cableado

Sistema de cableado estructurado 72

Tipos de organizaciones de estándares de cableado 75

El estándar de cableado estructurado EIA/TIA-568 fue diseñado para 76

Los 6 subsistemas del cableado estructurado 76

Topología física del Datacenter 80

Elementos del cableado estructurado del Datacenter TIA-942 80

Beneficios del sistema de cableado 80

Consideraciones del diseño 81

Detalles del sistema de transmisión de datos 81

Topología básica del Datacenter - componentes EIA/TIA-568-B 84

CAPÍTULO 5 - Cooling

Enfriamiento (Cooling) 86

Consideraciones 87

El exceso de calor produce 88

La ventilación 91

Gráfico: El flujo de aire en un rack 92

Gráfico: Enfriamiento dentro del rack 93

Arquitecturas de enfriamiento 95

Pasillos calientes, pasillos fríos 95

Gráfico: Enfriamiento (40-50 KW pasillo caliente central, tipo sala) 97

Gráfico: Enfriamiento (40-50 KW pasillo frío central, tipo sala) 98

Gráfico: Enfriamiento por fila (in-row) 99

Gráfico: Detalle del aire acondicionado circulando por pasillos abiertos 100

Gráfico: Aire acondicionado en pasillos cerrados 101

Gráfico: Vista 3D de la sala de rack 101

Factores que afectan la distribución del aire 102

CAPÍTULO 6- Adecuación física

Piso falso 103

Recubrimiento MICARTA 103

Perforaciones del piso para la circulación del aire acondicionado 105

Techo Falso 105

Perforaciones para cables 105

Iluminación principal y de emergencia 106

Red eléctrica regulada 106

CAPÍTULO 7 - Políticas

Definición de la política general 108

Política 108

Introducción 108

Definiciones 109

Objetivos de la política 109

Elementos adicionales a la política general 109

Políticas relacionadas 110

Roles y responsabilidades 110

Violaciones a la política de seguridad 110

Revisión de la política 111

Aspectos específicos sobre la política de seguridad física 111

Seguridad en el perímetro físico 111

Recomendaciones y controles adicionales 111

Control de acceso físico a áreas seguras 112

Usos de máquinas fax/módems 113

Usos de impresoras 113

Presencia de extraños en las instalaciones 114

Áreas de cargas y descarga 114

Seguridad de los equipos 115

Instalación y mantenimiento del cableado 116

Mantenimiento de los equipos 117

Equipos fuera de las instalaciones 117

Destrucción de equipos y re-uso 118

Políticas de escritorios y pantallas limpias 118

CAPÍTULO 8 - SAN/NAS/DAS

Introducción al storage área network (SAN) 119

Evolución de las tecnologías de almacenamiento 120

Network attached storage (NAS) 122

SAN a bajo nivel 123

SAN sobre IP 124

Topología FCIP 125

Elementos y componentes típicos de una red de almacenamiento 126

Redes de almacenamiento de arquitecturas mezcladas 128

Evolución de las normas para (SAN) 129

Conclusión 130

CAPÍTULO 9 - Servicios

Servicios que brinda un Datacenter 131

Descripción de capas 132

Arquitectura de tres capas básicas en una empresa 134

Acceso al edificio 134

Distribución del edificio 134

El núcleo (Core) 134

Administración de la red 135

Campus empresarial 135

Extremo empresarial 135

Extremo del proveedor de servicios 135

Tipo de tráfico en el Datacenter 135

Aplicaciones y la administración del tráfico 137

Priorización del tráfico de un Datacenter 138

Detalle del tráfico en un Datacenter 138

Documentar un Datacenter 140

Plan de continuidad del Datacenter 142

Plan de seguridad del Datacenter 142

Plan de mantenimiento de la red del Datacenter 142

Acuerdo del nivel de servicio (SLA) 143

Centro de operaciones de red (NOC) 143

Factores a tener en cuenta en el diseño de un Datacenter 146

Funcionamiento del sistema de alimentación sobre Ethernet (POE) 147

Seguridad del Datacenter 148

Conexión del Datacenter con servicios externos 149

Funcionamiento de un router 150

Funcionamiento de un switch 152

CAPÍTULO 10 - Arquitectura

Arquitectura de red del Datacenter 157

Sistemas y tecnologías que brinda un Datacenter 158

Interconexión del Datacenter 158

Servicios interactivos de capas 159

Servicios de seguridad 160

Servicios de computación 160

Desarrollo de la capa de la infraestructura de red 161

Funcionamiento de una red de granja de servidores 162

Paradigma de la computación de alto rendimiento HPC 162

Evolución de la tecnología SAN 162

Topologías de soluciones SAN - Replicación de la información - Ejemplos 164

Solución: anillo de óptico 164

Solución: fiber channel sobre sonet/sdh 165

Solución: fcip transporte sobre sonet/sdh, metroethernet o lan transparente 166

Solución: fcip transporte sobre servicios wan 167

Canal de fibra 167

Topología del enlace de fibra 167

Bus de comunicaciones infiniband 168

Virtualización del Datacenter 169

Modelo de un Datacenter Multi-capas 170

Integración de servidores Blade 171

Reducción del espacio, un concepto de consolidación 173

El concepto de Datacenter móvil 174

CAPÍTULO 10 - RRHH

Equipos de trabajo 175

Experiencia del equipo de trabajo asignado al proyecto 175

Profesional con experiencia en redes de datos 175

Profesional con experiencia en cableado estructurado 175

Profesional con experiencia en redes eléctricas 176

Profesional con experiencia en aires acondicionados de precisión 176

Capacitación de recursos humanos 176

Plan de trabajo 177

CAPÍTULO 11 - Documentación

Documentación 178

Garantías del equipamiento 180

Aspectos técnicos adicionales 180

Resultados obtenidos 181

Conclusiones 181

CAPÍTULO 12 - Anexo

¿Qué es un sistema UPS? 182

¿Cuántos tipos de sistemas UPS existen en el mercado? 182

¿Qué tipo de sistema UPS, debo considerar para mi Datacenter? 183

¿Qué significa autonomía o tiempo de respaldo de un sistema UPS? 183

¿Qué mantenimiento debe tener un sistema de UPS? 184

¿Qué significa un sistema redundante? 184

¿Es determinante la condición ambiental de operación para los equipos de respaldo dentro del Datacenter? 184

Problemas típicos que pueden ocurrir en un sistema de UPS 185

Consecuencias de una mal suministro energético 186

Sistema de UPS con tecnología ON- LINE 187

Referencias 190

Bibliografía 190

Breve resumen técnico

¿Por qué diseñar un Datacenter? ¿Qué conceptos debo entender?

Definido el Core Business de nuestro Datacenter diseñaremos con detalle las diferentes partes que forman un Datacenter, son: el sistemas de energía, el sistemas de detección y extinción de incendios, el sistema de cableado, el sistema de acondicionamiento, el sistema de seguridad y la ubicación geográfica.

Diseñar un Datacenter que ofrezca servicios **(24x7x365)** bajo un esquema de alta disponibilidad e interoperabilidad, donde la infraestructura física esté alineada con los estándares de facto, nos da competitividad en un mercado donde la demanda por nuevas soluciones tecnológicas son requeridas en el corto plazo.

El Datacenter debe brindar una infraestructura tecnológica escalable e independiente, de plataformas, de aplicaciones y poseer una re-ingeniería muy acorde a la coyuntura tecnológica.

Además implementar nuevas tecnologías de telecomunicaciones a nivel de transporte como pueden ser DWDM, SDH, Metro Ethernet, MPLS, es necesario.

Entender y aplicar el paradigma de la virtualización en un entorno de Datacenter distribuido en capas, nos da una ventaja competitiva frente a nuestros competidores.

Comprender el concepto de medir la potencia requerida para satisfacer la demanda de energía de la carga crítica del Datacenter, es estratégico, comprendiendo las necesidades de disponibilidad, tolerancia a contingencias y costos asociados, con estas premisas los diseñadores debemos ser capaces de realizar el diseño que cumpla las necesidades actuales, pero no debemos perder de vista cuales son las tendencias del mercado y cómo haremos la re-ingeniería necesaria de nuestro Datacenter con el objeto de no quedar obsoleto en el tiempo.

CAPÍTULO 1 - Introducción

Introducción

Este libro es resultado de un arduo trabajo, que conllevó mucho tiempo y esfuerzo, dedicado a los alumnos de Ingeniería de la Universidad Tecnológica Nacional, Facultad Regional Tucumán.

Este ejemplar explica desde cero los estándares más importantes para el diseño de un Centro de datos o Datacenter, o sea desde el principio hasta la puesta en funcionamiento y explotación.

La ingeniería es una ciencia de integración de conocimiento que transita desde el diseño arquitectónico del recinto, el desarrollo eléctrico, la elección de la arquitectura del hardware de conectividad hasta la formación de los recursos humanos.

En estas páginas traté, con esfuerzo, de brindar y posibilitar una lectura amena al lector, que satisfaga las teorías más usadas y sea práctico en zonas a mi criterio importantes. Como ser niveles de redundancia tanto eléctrica como a equipos de comunicaciones se refiere, topologías de telecomunicaciones y nuevos paradigmas de diseño de procesamiento y/o explotación de la información.

Que es un Datacenter DC – Centro de Datos – Centro de Respaldo

Se denomina Centro de Proceso de Datos o Datacenter a aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización.

Dichos recursos consisten esencialmente en unas dependencias, debidamente acondicionadas, de computadoras y redes de comunicaciones. Se suelen denominar por su acrónimo: CD o Datacenter (en inglés), Centro de Cómputo o Centro de Datos.

Diseño del Datacenter - DC

Un Datacenter es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamientos electrónicos. Suelen ser creados y

mantenidos por grandes organizaciones con el objeto de tener acceso a la información necesaria para sus operaciones en todo momento, por ejemplo un banco puede tenerlo con el propósito de almacenar todos los datos de sus clientes y las operaciones que estos realizan sobre sus cuentas. Prácticamente todas las compañías, ya sean medianas o grandes, tienen algún tipo de Datacenter, mientras que las más grandes llegan a tener varios.

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

Grandes organizaciones, tales como bancos o administraciones públicas, no pueden permitirse la pérdida de información ni el cese de operaciones ante un desastre en su Centro de Proceso de Datos. Terremotos, incendios o atentados en estas instalaciones son infrecuentes, pero no improbables, por ese motivo, y muchos más nace la idea de Datacenter o Centro de Datos.

El diseño comienza por la elección de su ubicación geográfica, y requiere un balance entre diversos factores:

Evaluación económica:

- Costo del terreno.
- Impuestos asociados.

Infraestructuras disponibles en las cercanías:

- Distribuidores de energía eléctrica.
- Vías de acceso.
- Acometidas de electricidad.

Análisis de riesgo:

- Posibilidad de inundaciones.
- Incendios.
- Robos, terremotos.

Una vez seleccionada la ubicación geográfica es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Algunos requisitos de las dependencias son:

- Doble acometida eléctrica.
- Muelle de carga y descarga.
- Montacargas y puertas anchas.
- Altura suficiente de las plantas.
- Medidas de seguridad en caso de incendio o inundación: Drenajes, extintores, vías de evacuación, puertas ignífugas.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración del edificio.
- Almacenes y/o depósitos.

Aún cuando se disponga del local adecuado, siempre es necesario algún despliegue de infraestructuras en su interior:

- Falsos suelos y falsos techos.
- Cableado de red y teléfono.
- Doble cableado eléctrico.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
- Instalación de alarmas.

Una parte especialmente importante de estas infraestructuras son aquellas destinadas a la seguridad física de la instalación, lo que incluye:

- Cerraduras electromagnéticas.
- Cámaras de seguridad.
- Detectores de movimiento.
- Tarjetas de identificación.
- Una vez acondicionado el habitáculo se procede a la instalación de los equipamientos informáticos del que constará nuestro centro de datos. Esta tarea requiere de un diseño físico de organización del equipamiento en general, y otro lógico de seguridad de acceso en lo que respecta a la red interna.
 - Creación de zonas desmilitarizadas (**DMZ**).
 - Segmentación de redes locales y creación de redes virtuales (**VLAN**).
 - Despliegue y configuración de la electrónica de red: Routers, switch.
 - Creación de los entornos de explotación, pre-explotación, desarrollo de aplicaciones y gestión en red.
 - Creación de la red de almacenamiento **NAS** o **SAN**.
 - Instalación y configuración de los servidores y periféricos.

Generalmente, todos los grandes servidores se suelen concentrar en una sala denominada sala fría, nevera o pecera, por lo que esta sala requiere de un sistema específico de refrigeración para mantener una temperatura baja, entre 21 y 23 Grados Centígrados, para evitar averías en las computadoras a causa del sobrecalentamiento. Según las normas internacionales establecen que la temperatura exacta debe ser 22.3 Grados Centígrados.

Las salas suelen contar con medidas estrictas de seguridad en el acceso físico, así como medidas de extinción de incendios adecuadas al material

eléctrico, tales como extinción por agua nebulizada o bien por gas INERGEN, dióxido de carbono o nitrógeno.

Diseño de un centro de respaldo

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

En segundo lugar, el equipamiento electrónico e informático debe ser absolutamente compatible con el existente en el Datacenter principal. Esto no implica que el equipamiento deba ser exactamente igual, ya que, normalmente, no todos los procesos del Datacenter principal son críticos. Por ese motivo no es necesario duplicar todo el equipamiento, ni tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar un hardware menos potente.

La sala de un Centro de Respaldo recibe estas denominaciones en función de su equipamiento:

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

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

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

Diseño de un Datacenter - El Sincronismo de los datos

- La copia sincrónica de datos, asegura que todo dato escrito en el CD principal también se inscriba en el centro de respaldo antes de continuar con cualquier otra operación. La Información espejada rápidamente, alto tráfico por la red en horarios picos de trabajo.
- La copia asincrónica de datos, no asegura que todos los datos escritos en el Datacenter principal se escriban inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros. Latencia importante en lo que respecta a la información reflejada bajo tráfico por la red en horarios picos, siendo así se debe desarrollar un plan de replicación de la información acorde a las necesidades requeridas.

La copia asincrónica puede tener lugar Off-line o fuera de línea, en este caso el centro de respaldo utilizará la última copia de seguridad existente del Datacenter principal y esto lleva a la pérdida de los datos de operaciones de varias horas como mínimo hasta días (lo habitual). Esta opción es viable para negocios no demasiado críticos, donde es más importante la continuidad del negocio que la pérdida de datos. Por ejemplo, en cadenas de supermercados. No obstante, es inviable en negocios como el bancario, donde es impensable la pérdida de una sola transacción económica. En los demás casos, la política de copia suele descansar sobre la infraestructura de almacenamiento corporativo, generalmente, se trata de redes **SAN** (Storage Área Network) o arreglos de discos con suficiente inteligencia como para implementar dichas políticas.

Tanto para la copia sincrónica como asincrónica, es necesaria una extensión de la red de almacenamiento entre ambos centros, es decir, un enlace de telecomunicaciones entre el Datacenter y el Centro de Respaldo. En el caso de la copia asincrónica es imprescindible que dicho enlace goce de baja latencia, motivo por el que se suele emplear un enlace de fibra óptica, que limita la distancia máxima a decenas de kilómetros. Esta es esencial en negocios de las finanzas, donde no es posible la pérdida de ninguna transacción. Por consiguiente, la copia asincrónica es viable en la mayoría de

los casos, ya que el desfase temporal de la copia se limita a unos pocos minutos.

El Datacenter en un contexto de plan de contingencia

Un centro de respaldo por sí sólo no basta para hacer frente a una contingencia grave. Es necesario disponer de un Plan de Contingencias Corporativo y éste contiene tres sub-planes que indican las medidas técnicas, humanas y organizativas necesarias en cuatro momentos claves:

1. El plan de respaldo, contempla las actuaciones necesarias antes de que se produzca un incidente y que son, esencialmente, mantenimiento y prueba de las medidas preventivas.
2. El plan de emergencia considera las actuaciones necesarias durante un incidente.
3. El plan de recuperación, contempla las actuaciones necesarias después de un incidente e indica, básicamente, cómo volver a la operación normal.
4. El centro de respaldo no es la única manera de articular el plan de contingencia. Sino también es posible el Outsourcing de servicios similares.

El Datacenter - La Información – La Empresa

Hoy en día, las compañías saben que su activo más importante es la información y es por esto que procuran su disponibilidad y seguridad. Aquellas empresas que ofrecen esta fluidez de información, así como servicios de storage y respaldo hacia otras compañías, están construyendo instalaciones de tecnología de punta globalmente. El núcleo de estas instalaciones es la infraestructura de **TI** y uno de sus principales elementos es la infraestructura del sistema de cableado y éste es uno de los componentes más importantes.

Tendencias de los Datacenter - Componentes

Los Datacenters almacenan la información de aplicaciones diversas, desde **ERP** (Enterprise Resource Planning), aplicaciones de e-commerce,

convergencia de video/voz/datos, aplicaciones de **B2B** (Business to Business), así como las aplicaciones de backoffice que son críticas en la operación de una empresa. Por ende, un riesgo muy importante es el **downtime** (tiempo de inactividad), que se traduce en pérdidas monetarias. En consecuencia, las empresas que ofrecen equipos y componentes para los Datacenters son sensibles a todo esto y han conseguido grandes avances en proveer soluciones viables para los requerimientos de comunicación y almacenamiento.

Los Datacenters están compuestos de un sistema de redes de comunicaciones de alta velocidad y demanda, que son capaces de manejar el tráfico de las redes **SAN** (Storage Área Network), **NAS** (Network Attached Storage), granjas de servidores de archivos/aplicaciones/redes y otros componentes que se localizan en un ambiente controlado. Las comunicaciones hacia adentro y hacia fuera se hacen a través de enlaces **WAN**, **CAN/MAN**, **METRO ETHERNET**, en una variedad de configuraciones dependiendo de las necesidades de cada centro.

Un diseño adecuado ofrecerá disponibilidad, accesibilidad, capacidad de crecimiento y confiabilidad las 24 horas del día, los 7 días de la semana y los 365 días del año, exceptuando cualquier **Downtime** que se programe para su mantenimiento. Los Datacenters que son críticos se monitorean a través de un **NOC** (Network Operations Center) el cuál es advertido a través de alarmas de detección de problemas tales como sobrecalentamiento, apagones y fallas, gracias a una serie de disparadores que son configurados. Todo este diseño es sumamente importante, considerando la complejidad de todos los componentes que se entrelazan, por ello se definen una serie de estándares que contemplan cada parte del sistema en su totalidad.

CAPÍTULO 2 - Diseño físico

Planeación y diseño de un Datacenter

Los Datacenter deben ser cuidadosamente planificados antes de comenzar su construcción para asegurar la alineación con cualquier estándar y códigos aplicables. Es importante estimar el número de usuarios, tipos de aplicaciones y plataformas, unidades de rack requeridas para montar equipos y, más importante aún, considerar el crecimiento esperado. Éste tomará vida propia y debe tener la capacidad de responder a cualquier cambio de equipo, estándar y demanda, y al mismo tiempo permanecer administrable y, sobre todo, confiable. Es fundamental que el proyectista, maneje esta información con el fin de desarrollar un sistema escalable, actualizable y confiable que dé cobertura a las necesidades actuales y futuras.

El estándar EIA/TIA-942

El estándar **EIA/TIA-942** define la Infraestructura de Telecomunicaciones para Datacenter en general. La topología y el desempeño del cableado de cobre y fibra, así como otros aspectos de la infraestructura de **TI** que permitirán a las instalaciones alinearse rápidamente a las nuevas tecnologías tales como redes de 10GB/s, son lineamientos que desarrolla el estándar. La **EIA/TIA** ha adoptado recientemente la **EIA/TIA-942** que es el estándar donde desarrolla las directrices básicas de un Datacenter. Entonces, los requerimientos a considerar son: La capacidad de flexibilidad, confiabilidad y administración de espacio. En tanto que el cableado puede ser de cobre (**UTP/STP**) o fibra (**SM/MM**) que dependerá de la interfaces del equipo al cual se conecte.

Objetivos del diseño

Los cuatro objetivos más importantes a tener en cuenta a la hora de diseñar cualquier Datacenter con un alto performance, son:

1. Seguridad.
2. Disponibilidad.

3. Escalabilidad.

4. Gestión.

El planeamiento de diseño comienza por la elección de una ubicación geográfica que sea propicia para tal fin. Para eso se debe tener en cuenta el terreno (si es zona de inundaciones, robos o incendios) y la disponibilidad de infraestructura en sus alrededores (energía eléctrica, centrales de telecomunicaciones, etc.), como parte de este planeamiento, se generó, internacionalmente, un consentimiento para considerar estándares que entreguen a las empresas aquellas guías de diseño e instalación. A nivel americano la **TIA** (Telecommunication Industry Association) formó el estándar **TIA-942** Infraestructura de Telecomunicaciones para Datacenter, con casi 2 años en el mercado, este estándar contempla Datacenters por topología, y entrega las especificaciones de los cuatro pilares de un Datacenter:

1. **Arquitectura** (cableado de racks, acceso redundante, cuarto entrada, área distribución).
2. **Mecánica** (seguridad física, protección de incendios).
3. **Eléctrica** (sistemas de **UPS**, generadores, puesta a tierra).
4. **Comunicaciones** (redundancia de enlaces, tipos de infraestructura física de cobre y de fibra óptica).

Si alguno de estos pilares nombrados falla, el resto también tambaleará. Por ello es importante entender que en el diseño de un Datacenter interactúan varios grupos de trabajo, varios especialistas, todos dependientes unos de otros. Cada (**CIO Chief Information Officer**), administrador de redes, o encargado del Datacenter, debe conocer el negocio de su empresa, y poder identificar qué tipo de Datacenter requiere. De esta manera, se recomienda realizar un check list dentro del estándar, en el cual se identifiquen todos los puntos a tener en cuenta para el diseño.

Detalle del estándar EIA/TIA-942

El estándar **EIA/TIA-942** establece las características que deben ejecutarse en los componentes de la infraestructura para los distintos grados de

disponibilidad. Dentro del mundo **TI** se encuentran algunas propiedades intrínsecas de la información, como la disponibilidad que se debe preservar para asegurar la continuidad de las operaciones y del negocio. También en este mundo convergen algunos factores de riesgo externos a la información como el fuego, el cual puede destruirla y causarle a la organización grandes pérdidas.

Hay que tener en cuenta que no todas las actividades requieren el mismo nivel de disponibilidad y esto surgirá de un análisis previo llamado (**BIA Business Impact Analysis**) que cuantifica económicamente el impacto que produce una parada del Datacenter en el negocio de la organización. En líneas generales se puede establecer a priori una clasificación aproximada de la criticidad de los sistemas para distintas áreas de actividad.

En la siguiente gráfica se puede observar una medición de los riesgos.



La infraestructura y el estándar TIA-942

En abril de 2005, la *Telecommunication Industry Association* publicó su estándar **TIA-942** con la intención de unificar criterios en el diseño de áreas de tecnologías y comunicaciones. Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, avanza sobre los subsistemas de infraestructura, generando los

lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar. En su anexo G (informativo) y basado en recomendaciones del **Uptime Institute**, establece cuatro niveles (**Tiers**) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99.995%.

A su vez, divide la infraestructura de un Datacenter en cuatro subsistemas a saber:

1. • Telecomunicaciones.
2. • Arquitectura.
3. • Sistema Eléctrico.
4. • Sistema Mecánico.

Uno de los mayores puntos de confusión en el campo del **uptime (tiempo disponible de los sistemas)**, es la definición de Datacenter confiable, ya que lo que es aceptable para una persona o compañía no lo es para otra. Empresas competitivas con infraestructuras de Datacenter completamente diferentes proclaman poseer alta disponibilidad, aunque no obstante esto pueda ser cierto, dependerá de la interpretación subjetiva de disponibilidad que se realice para el tipo de negocio en que se encuentre una compañía. Lo cierto es que para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto en el Datacenter como en la infraestructura que le da soporte.

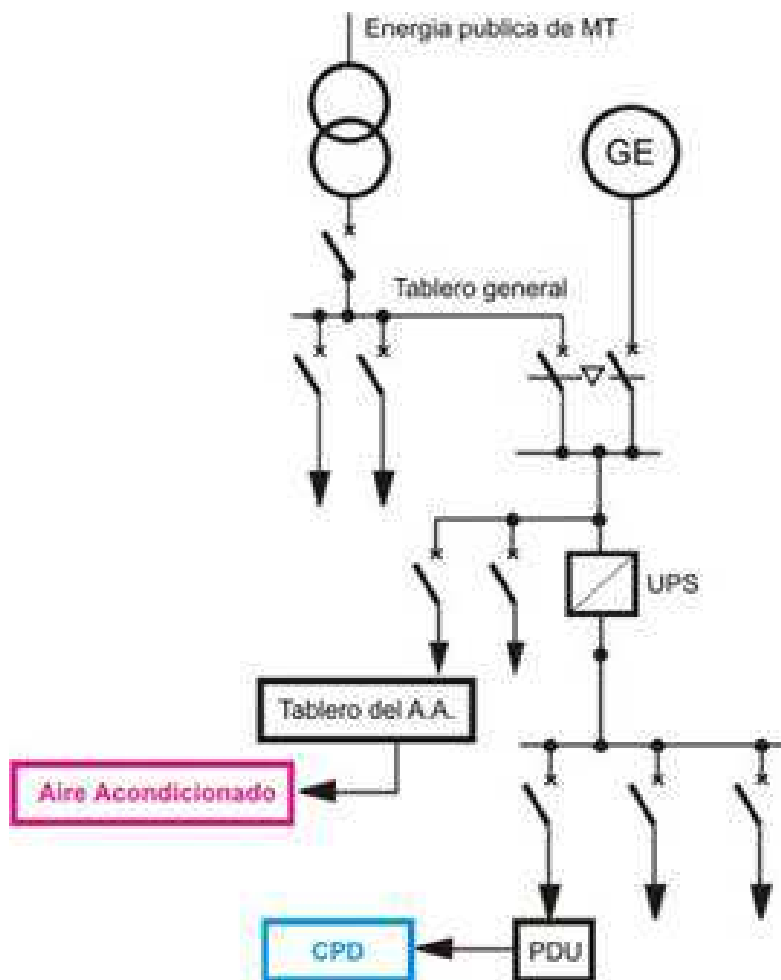
Los cuatro niveles de **Tiers** que plantea el estándar se corresponden con cuatro niveles de disponibilidad, teniendo en cuenta que a mayor número de Tier mayor disponibilidad y lo que implica también mayores costos constructivos. Siendo esta clasificación aplicable en forma independiente a cada subsistema de la infraestructura. Hay que tener en cuenta que la clasificación global del Datacenter será igual a la de aquel subsistema que tenga el menor número de Tier. Esto significa que si un Datacenter tiene todos los subsistemas Tier IV excepto el eléctrico que es Tier III, la clasificación global será Tier III. Es importante tener en cuenta esto porque cuando se pretende la adecuación de Datacenter actuales a Tier IV, en

lugares como América Latina, hay limitaciones físicas difíciles de salvar en los emplazamientos edilicios actuales. Prácticamente para lograr un Datacenter Tier IV hay que diseñarlos de cero con el estándar en mente como guía. Un ejemplo claro de esto es que es muy difícil lograr la provisión de energía de dos sub-estaciones independientes o poder lograr la altura que requiere el estándar en los edificios existentes (3 metros mínimo sobre piso elevado y no menor de 60 cm, entre el techo y el equipo más alto). Por lo que la norma describe, resumidamente, los distintos Tiers de la siguiente manera:

TIER I

Datacenter Básico: Un Datacenter Tier I puede ser susceptible a interrupciones tanto planeadas como no planeadas. Cuenta con un sistema de aire acondicionado y distribución de energía; pero puede o no tener piso técnico, sistema de UPS o generador eléctrico, si los posee pueden no tener redundancia y existir varios puntos únicos de falla. La carga máxima de los sistemas en situaciones críticas es del 100%. La infraestructura del Datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Situaciones de urgencia pueden motivar paradas más frecuentes y errores de operación o fallas en los componentes de su infraestructura que causarán la detención del Datacenter. La tasa de disponibilidad máxima del Datacenter es 99.671% del tiempo.

Gráfica: TIER I.

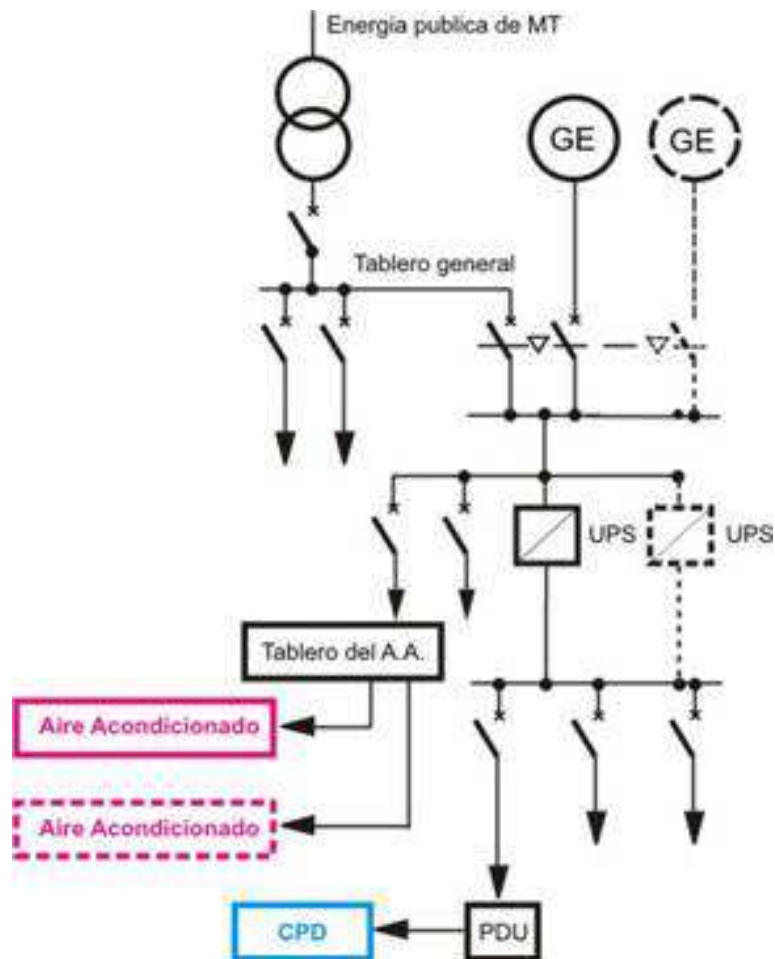


TIER II

Componentes Redundantes: Los Datacenter con componentes redundantes son ligeramente menos susceptibles a interrupciones, tanto los planeados como los no planeados. Estos Datacenter cuentan con piso falso, sistemas de UPS y generadores eléctricos, pero están conectados a una sola línea de distribución eléctrica. Su diseño es “lo necesario más uno” (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 puede causar una interrupción del procesamiento. La tasa de disponibilidad máxima del Datacenter es 99.749% del tiempo.

Gráfica: TIER II.



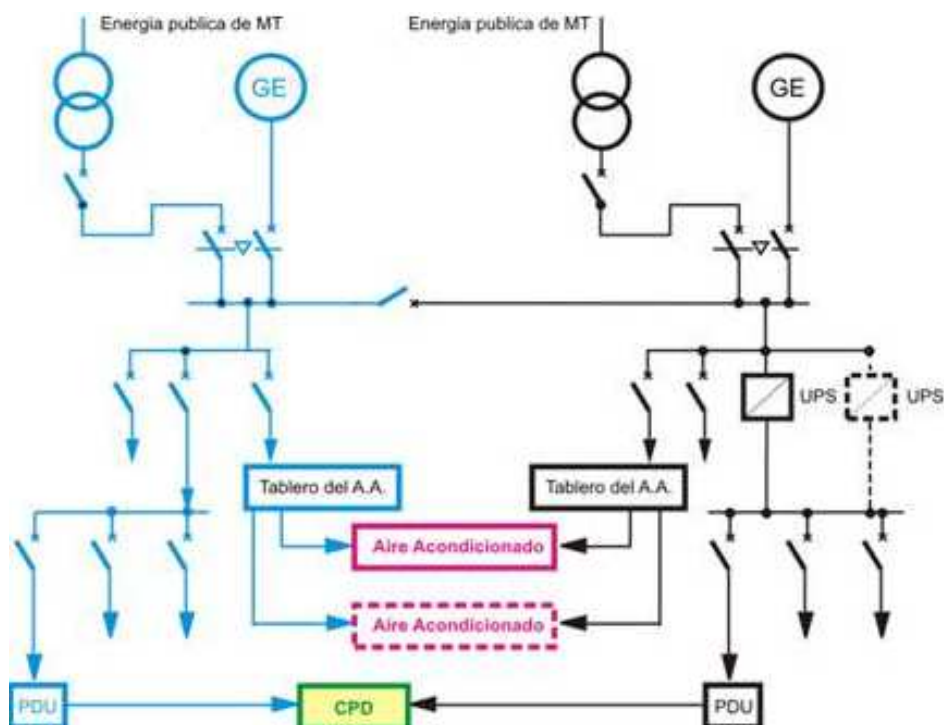
TIER III

Mantenimiento Concurrente: Las capacidades de un Datacenter de este tipo le permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura sin interrupciones en la operación. Las actividades planeadas incluyen mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, agregar o eliminar elementos y realizar pruebas

de componentes o sistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua significa doble conjunto de tuberías, 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, mientras que la otra atiende la totalidad de la carga.

En este Tier, actividades no planeadas como errores de operación o fallas espontáneas en la infraestructura además de causar una interrupción del Datacenter. La carga máxima en los sistemas en situaciones críticas es de 90%. Muchos Datacenter Tier III son diseñados para poder actualizarse a Tier IV, cuando los requerimientos del negocio justifiquen el costo. La tasa de disponibilidad máxima del Datacenter es 99.982% del tiempo.

Gráfica: TIER III.



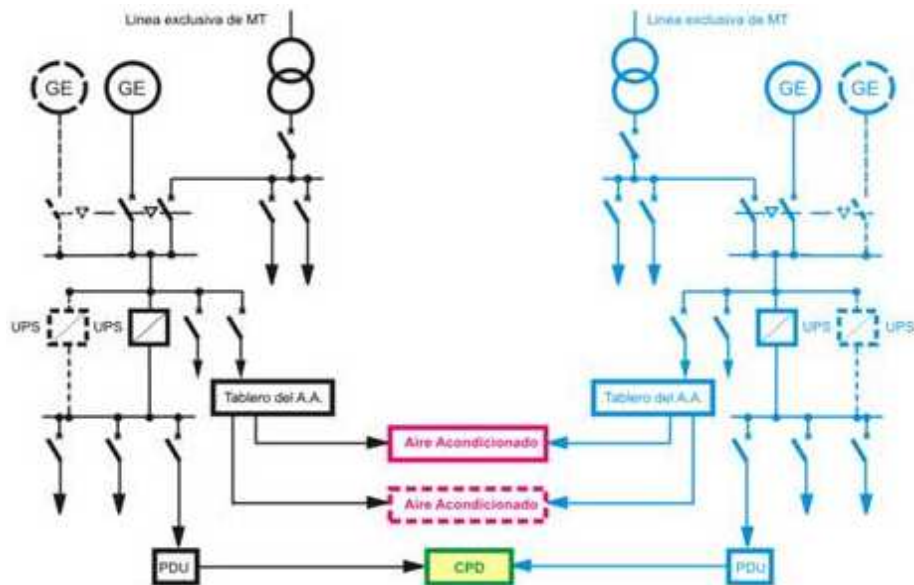
TIER IV

Tolerante a fallas: Este Datacenter provee capacidad para realizar cualquier actividad planeada sin interrupciones en las cargas críticas, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando aun ante un evento crítico no planeado. Esto requiere dos líneas de

distribución simultáneamente activas, típicamente en una configuración system + system; eléctricamente esto significa dos sistemas de UPS independientes, y cada uno con un nivel de redundancia N+1. La carga máxima de los sistemas en situaciones críticas es de 90% y persiste en un nivel de exposición a fallas, por el inicio de una alarma de incendio o porque una persona inicie un procedimiento de apagado de emergencia o Emergency Power Off (**EPO**), el cual debe existir para cumplir con los códigos de seguridad contra incendios o eléctricos.

La tasa de disponibilidad máxima del Datacenter es 99.995% del tiempo. Para poner en perspectiva la tasa de disponibilidad que se pretende para los distintos Tiers, en la gráfica de categorización de tiers, expresa su significado en el tiempo de parada anual del Datacenter. Estos porcentajes deben considerarse como el promedio de cinco años y hay que tener en cuenta que para un Tier IV se contempla que la única parada que se produce es por la activación de un **EPO** y esto sólo sucede una vez cada cinco años. No obstante, para la exigencia que demanda un Tier IV algunas empresas u organizaciones manifiestan necesitar una disponibilidad de “cinco nueves”, lo que significa un 99,999% de disponibilidad. Esto es poco más de cinco minutos anuales sin sistemas.

Gráfica: TIER IV.



Gráfica: Categorización de TIERS.

Tier	% Disponibilidad	% Parada	Tiempo Parada Año
Tier I	99.671 %	0.329 %	28.92 Horas
Tier II	99.741 %	0.251 %	22.68 Horas
Tier III	99.982 %	0.018 %	1.57 Horas
Tier IV	99.995 %	0.005 %	52.56 Minutos

Gráfica: Disponibilidad según TIER.

Niveles TIER	TIER I	TIER II	TIER III	TIER IV
Redundancia	N	N+1	N+1	2(N+1)
Número de alimentaciones eléctricas	1	1	1 activo 1 pasivo	2
Mantenimiento en operación	no	no	sí	sí
Posibles puntos de falla	Muchos	Muchos	Algunos	Incendio, fallo humano
Interrupción de operación por mantenimiento al año	2 de más de 12 horas	1.5 de más de 12 horas	0	0
Tiempo parada al año	28,92 horas	22,68 horas	1,57 horas	52,56 minutos
Disponibilidad del servicio	99,671%	99,741%	99,982%	99,995%

Conclusión del estándar

El propósito del estándar es proveer una serie de recomendaciones para el diseño e instalación de un Datacenter, con la intención de que sea utilizado por los diseñadores que necesitan un conocimiento acabado del sistema de cableado y el diseño de redes. El estándar **EIA/TIA-942** y la categorización de Tiers se encuentran en pleno auge en América Latina, y esto es bueno porque lleva al replanteo de las necesidades de infraestructura de una manera racional y alineada con las necesidades propias de disponibilidad del negocio en que se encuentran las organizaciones. En todo caso, para

cualquier tipo de negocio que necesité proyectar un Datacenter propio, por sus necesidades específicas, el estándar tratado hasta el momento es una buena guía con respecto a las buenas prácticas acerca de cómo reglar las arquitecturas básicas de procesamiento de información.

Requerimientos generales para la implementación de un Datacenter - Estándares

El diseño del Datacenter debe estar basado en estándares para un óptimo funcionamiento, administración y excelente mantenimiento, para lo cual el planteamiento debe seguir como mínimo las siguientes normas y recomendaciones:

- EIA/TIA-942 Telecommunications Infrastructure Standard for Data Centers. La norma EIA/TIA-942 incluye especificaciones y requerimientos mínimos para Datacenter y la descripción de diferentes niveles de disponibilidad, redundancia y seguridad denominados TIER.
- EIA/TIA-568-B.1, B.2, B.3 Commercial Building Wiring Standard y sus boletines de actualización, TSB-36 y TSB-40, permite la planeación e instalación de un sistema de cableado estructurado que soporte, independientemente del proveedor y sin conocimiento previo, los servicios y dispositivos de telecomunicaciones que serán instalados durante la vida útil del edificio.
- EIA/TIA-569 Commercial Building Standard for Telecommunications Pathways and Spaces, que estandariza prácticas de diseño y construcción dentro o entre edificios, que son hechas en soporte de medios y/o equipos de telecomunicaciones tales como canaletas y guías, facilidades en la entrada al edificio, armarios y/o armarios de comunicaciones y cuartos de equipos.
- EIA/TIA-606 Administration Standards for the Telecommunications Infrastructure of Commercial Buildings, da las guías para marcar y administrar los componentes de un sistema de cableado estructurado.

- EIA/TIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunication, describe los métodos para distribuir las señales de tierra a través de un edificio.
- EIA/TIA-568 B.2-AD10, ISO 11801 Class E Edition 2.1 y el borrador propuesto en IEEE STD 802.3an con requerimientos de canal para soportar 10GBASE-T.
- IEEE 1100-1999, recommended practice for powering and grounding electronic equipment. Recomendaciones y puesta a tierra de equipos electrónicos.
- NFPA 2001 es un estándar sobre sistemas de extinción mediante agentes limpios.

El nuevo Datacenter deberá estar diseñado para soportar las demandas actuales y futuras requeridas por las plataformas críticas de informática y comunicaciones que sean necesarias. El diseño contemplará las tecnologías ampliamente reconocidas y probadas en el mercado, siguiendo aspectos funcionales como:

- Arquitectura basada en componentes ampliamente reconocidos y probados en el mercado.
- Arquitectura modular, que facilite el crecimiento futuro bajo demanda.
- Sistemas de contingencias contra fallas y facilidad para restauración inmediata del servicio.
- Funcionalidades de gestión integradas dentro de una misma plataforma, reduciendo la complejidad y costos de administración de la infraestructura del Datacenter.

- Sistemas con alta eficiencia energética que permitan una operación con bajos costos de energía para la entidad.
- Cada línea de rack deberá contar con un sistema independiente de **UPS**, que está pensado para brindar una solución en corto tiempo, dando una respuesta instantánea a un pico de demanda ante la interrupción del sistema estándar de red, es decir, otorga el tiempo suficiente para la entrada en servicio de los conjuntos de generadores o grupos electrógenos. Lo que le da una baja confiabilidad.
- En el sistema de refrigeración, en general, se recomienda usar un sistema único para la sala con arquitectura redundante (N+1). El sistema de distribución tiene fundamental importancia en la eficiencia del sistema de refrigeración.

CAPÍTULO 3 - Requerimientos

Sistema de aire acondicionado de precisión

Los sistemas de aire acondicionado tienen el propósito de mantener la temperatura adecuada en el centro de cómputo, y obligado a seleccionar la mejor arquitectura de acondicionamiento según las características del recinto y la ubicación geográfica. Además otro punto que no es menor y que se debe analizar son la factibilidad, los costos operativos y la confiabilidad del sistema.

El incremento exponencial de las nuevas tecnologías informáticas lleva a los diseñadores de Datacenter a plantearse nuevos paradigmas de enfriamiento, esto es consecuencia del incremento de las cargas térmicas, por lo que una demanda de mejoras tecnológicas de enfriamiento que garanticen un funcionamiento exento de fallas. La demanda por el almacenamiento y procesamiento de datos al igual que el costo del suministro de energía para los sistemas de refrigeración, va en aumento produciendo un aumento en el consumo energético del Datacenter, y esto es un punto a tener en cuenta cuando se ponderan los costos de operaciones.

Características de un sistema de aire acondicionado de precisión

1. Caudal de aire: Tiene un caudal de aire grande y un salto de temperatura pequeño a través del serpentín de enfriamiento.
2. Temperatura de evaporación del refrigerante: Alta temperatura positiva, 5 a 8 grados centígrados.
3. Superficie del serpentín de evaporación a igual velocidad de pasos de aire: Grande, por motivo del gran caudal de aire.
4. Capacidad sensible: De 90 - 100 % de la capacidad total.
5. Capacidad latente: De 0 - 10 % de la capacidad total.
6. Formación de hielo en el evaporador en invierno: No se forma hielo gracias a una regulación de presión de condensación constante en el circuito de refrigeración, la cual mantiene estable la temperatura de condensación, independientemente de las temperaturas exteriores.
7. Humificación: Tiene humidificador integrado.

8. Deshumificación: Tiene el proceso de deshumificación controlado, tiene pos-calefacción para corregir la desestabilización de la temperatura en la sala.
9. Selección de calidad de componentes: Componentes de larga vida.
10. Nivel de ruido: Nivel de ruido mediano - alto por tener caudales de aire grandes.
11. Costo del equipo: Alto costo.
12. Ubicación del compresor: Dentro del climatizador.
13. Desnivel entre el compresor y el evaporador: Compresor inferior al evaporador limitado por el motivo del retorno del líquido.
14. Control inteligente: Amplia prestación, control de temperatura y humedad relativa en estrechas tolerancias, síntesis de fallas, integra la filosofía de redundancia (N+1), rotación de equipos, enclavamientos.

En relación con el sistema de aire acondicionado de precisión, se deberá ejecutar los siguientes trabajos:

1. Conexión con el sistema eléctrico de potencia, (acometidas para aires acondicionados).
2. Construcción, adecuación e instalación de ductería y elementos de conexión y refrigeración del sistema de aire acondicionado.
3. Rotulación, marcación e identificación de todos los componentes del sistema de aire acondicionado solicitado.
4. Instalación y ejecución de pruebas, mediciones del sistema, en presencia del supervisor del proyecto, para garantizar la entrega y satisfacción.
5. Entrega de documentación definitiva del sistema: Planos conforme a obras de toda la instalación, eléctrica, mecánica e edilicia.

Para cumplir con estos requisitos, el ordenamiento de gabinetes se establece como la norma indica, creando corredores fríos y calientes. Adicionalmente, y

dada la evolución en la concentración de densidad de los servidores en los racks, como por ejemplo los tipo Blades¹, la alta densidad de calor debe ser removida en los puntos críticos donde se van a acomodar dichos equipos y el crecimiento a futuro. Por ello el sistema de aire acondicionado de precisión deberá cumplir con los siguientes puntos.

- Controlar adecuadamente la temperatura y la humedad del centro de cómputo.
- Soportar trabajo pesado.
- Garantizar alta eficiencia.
- Garantizar bajo nivel de ruido, de tal manera que no se afecte al personal de operación y se garantice un ambiente adecuado para el normal desarrollo de las actividades dentro del Datacenter.
- Garantizar bajo consumo eléctrico.
- Monitorear automáticamente el control de calor, enfriamiento, humidificación², deshumidificación³ y filtrado de partículas.
- La central automatizada de control y monitoreo, tiene que ser probada e instalada por el fabricante, que integre los componentes mecánicos y eléctricos constituyendo un sistema de soporte que controla y monitorea todas las variables importantes del sistema. Además se tendrá en cuenta la calibración de los sensores de humedad y temperatura, con la opción de desactivación de alarmas y sistemas de operación.
- El sistema deberá contar con la capacidad de enviar alarmas, correos electrónicos mediante interfaz POP3 o alertas SNMP o bien utilizar la tecnología celular para notificar al personal responsable.
- Ante cualquier alarma que se presente, el sistema de aire acondicionado redundante debe incluir las interfaces de comunicaciones necesarias, que permitan la comunicación automática entre las unidades, de forma que se puedan programar ciclos alternados de operación o asistencia automática en la

¹ Un servidor Blade es un tipo de computadora para los Datacenter.

²Proceso en el que se aumenta el vapor de agua contenido en el aire.

³Proceso mediante el cual se disminuye la humedad de una masa de aire con la finalidad de aumentar su capacidad evaporativa.

eventualidad de un aumento en la temperatura del centro de cómputo.

- La instalación de pantallas de visualización, que permitan la presentación de las variables más importantes del sistema, tendrán una ubicación estratégica dentro del edificio.
- El sistema debe estar construido con la mejor tecnología disponible, acogiéndose a todos los estándares disponibles. El funcionamiento del sistema deberá ser de 7x24X365, ya que ésta es la disponibilidad de operación del Datacenter.
- El sistema debe estar probado en la fábrica antes de ser enviado. Dichas pruebas deben incluir:
 - ✓ Pruebas completas de pérdidas de presión y fugas.
 - ✓ Prueba “Hi-Pot”⁴.
 - ✓ Pruebas de calibración del sistema.
 - ✓ El sistema debe venir acompañado con un completo reporte de pruebas para verificar los procedimientos de fábrica.

Chequeo y registros del sistema

Se debe chequear el funcionamiento de los siguientes componentes del sistema de aire acondicionado

- Forzadores de aire.
- Compresores.
- Válvula solenoide de línea de líquido.
- Resistencias.
- Humidificador.

El sistema debe ser capaz de llevar un historial de alarmas, de modo que la central será la encargada de guardar los últimos eventos registrados

⁴ Prueba de alto potencial, estas pruebas son aplicadas al aislamiento de los distintos equipos eléctricos con el fin de evaluar la condición de aislamiento.

mediante la activación de alarmas. Estos eventos quedarán registrados con el día, hora y minutos en el cual ocurrió.

- Temperatura de control alta.
- Temperatura de control baja.
- Humedad de control alta.
- Humedad de control baja.
- Alta presión en el filtro diferencial.
- Falla en el sensor del retorno.
- Alta temperatura de suministro.
- Baja temperatura de suministro.
- Flujo de aire bajo o nulo.
- Falla en el sensor de suministro.
- Falla en el regulador de agua.
- Alta presión interna.
- Baja presión de succión.
- Falla en el humidificador.
- Detección de agua internamente.
- Detección de fuego.
- Detección de humo.
- Falla en las bombas.

Además se registrará los tiempos de operación de cada uno de los siguientes componentes:

- Compresores.
- Humidificador.
- Deshumidificador.
- Forzadores de aire.

Los equipos del sistema de aire acondicionado redundante deberán realizar balanceo de operación y permitir alternar su funcionamiento mediante programación de maniobras ON/OFF.

La capacidad deberá ser suficiente para soportar la demanda actual y un crecimiento en racks y servidores adicionales del 50% de la capacidad instalada en el Datacenter.

Diseño del sistemas de UPS (sistema de energía ininterrumpible)

En los países desarrollados se podría asegurar que las redes públicas de distribución de energía tienen un buen nivel de confiabilidad, aunque, está la posibilidad de que se produzcan un tiempo de inactividad sin importar el motivo que fuese (contingencia), y estos fallos no programados ocasionan problemas en el normal funcionamiento del negocio; es así que nace la necesidad de incorporar un sistema que sea tolerante a fallas en lo que respecta a energía, ya que estamos hablando de un sistema **UPS (sistema de energía ininterrumpible)**, éste se ubica entre la red pública de distribución y sus cargas de misión crítica.

La configuración de diseño del sistema UPS que se elegirá está en función de la disponibilidad de los equipamientos que deseo dar cobertura de energía, las variables que intervienen en la disponibilidad de un sistema, entre ellas la confiabilidad de los componentes, los cronogramas de mantenimiento, los errores humanos, y por último el tiempo de recuperación. De este modo, la configuración elegida podrá mitigar algunos fallos mencionados anteriormente.

Entre los sistemas UPS más conocidos en el mercado no hay una solución específica que se adapte a nuestros requerimientos, sino que debemos ser capaces de diseñar nuestra solución a medida que pase el tiempo, teniendo presente el grado de disponibilidad de nuestra carga crítica, el **Core Business**, el costo asociado, el retorno de la inversión (**ROI**), por nombrar los más importantes. Entre los sistemas más comunes se hallan:

- Paralelo redundante.
- Redundante aislado.
- Redundante distribuido.
- Hottie.
- Hotsynch.
- De buses paralelos múltiples.

- Sistemas más sistema.
- Sistemas catcher.

Estos nombres pueden tener significados diferentes dependiendo de la interpretación del diseñador, por ello, hoy en día el mercado posee cinco configuraciones de mayor utilización, Estas cinco son:

1. De capacidad.
2. Redundante aislada.
3. Paralela redundante.
4. Redundante distribuida.
5. Sistemas más sistema.

La criticidad de carga es el punto donde se debe analizar la mejor configuración para mi sistema UPS, con este parámetro se obtendrá beneficios y limitaciones sin duda, de modo que es menester hacer un buen análisis con fortalezas y debilidades de cada sistema y las necesidades de Core Business.

Disponibilidad

La disponibilidad es el porcentaje estimado de tiempo en que la energía eléctrica está presente y funcionando adecuadamente para abastecer la carga crítica, definición que es sostenida por los administradores de la siguiente manera, el procesamiento de datos exige cada vez mayor disponibilidad.

Niveles

Las tareas de mantenimiento a intervalos regulares es un proceso que todos los sistemas tanto de alimentación ininterrumpida como de distribución eléctrica deben ser realizados. La disponibilidad de la configuración del sistema está en función al nivel de inmunidad a las fallas y a la capacidad inherente de admitir la realización de tareas de mantenimiento y pruebas de rutina mientras se sigue operando la carga crítica. El **Uptime** define una serie de niveles (**TIERS**) de operaciones de un Datacenter en varios puntos importantes en la operación, uno de los puntos es el del sistema UPS que brinda los lineamientos necesarios para su elección.

¿Qué significa N?

La nomenclatura que incluye la letra **N** ejemplifica la necesidad de un equipo de carga crítica.

Habitualmente en el mercado se utilizan nomenclaturas **N**, **N+1**, **2N**, **2(N+1)** para designar las distintas configuraciones de redundancia de los sistemas UPS, cabe aclarar, que no todos los sistemas **N+1** o **2N** son iguales. A continuación se pueden observar las diferencias entre cada una de ellas:

1. **N - Configuración de capacidad:** Designa a las instalaciones con un solo sistema de UPS o varios juntos proporcionan capacidad equivalente a la carga total crítica del Datacenter. Está configuración es la más típica y no proporciona redundancia de ningún tipo. **Tier 1 - Según TIA-942.**
2. **N+1 - Redundancia aislada:** Está configuración posee dos (2) UPS capaces de soportar toda la carga crítica, pero únicamente una está operativa y la restante ingresa en operación por alguna falla de la primera. Tiene la ventaja de no necesitar sincronización y la desventaja de ser ineficiente por tener una UPS sin carga y la dependencia de dos bypass estáticos STS de las dos UPS.
3. **N+1 - Redundancia en paralelo:** Esta configuración posee dos (2) UPS capaces de soportar toda la carga por completo del Datacenter. Ésta es una de las configuraciones más habituales, y requiere que los sistemas estén sincronizados y que sean del mismo fabricante. No es tolerante a fallos, aunque se puede mitigar según la implementación a optar. **Tier 2, 3, 4 - Según TIA-942.**
4. **2N - Redundancia sistema + sistema:** El diseño puede equivaler a dos sistemas de capacidad N alimentado simultáneamente a las PDU, es decir, dos parejas de UPS + generador, y tiene varias implementaciones posibles con la ventaja de eliminar varios puntos de fallos, con su consecuente inversión. **Tier 4 - Según TIA-942.**
5. **2(N+1) - Doble redundancia en paralelo:** Esta solución corresponde a dos configuraciones de redundancia en paralelo alimentadas simultáneamente a la carga crítica del Datacenter y requiere cuadruplicar la potencia eléctrica necesaria ya que cada uno de los sistemas UPS tiene que ser capaz de proteger la carga crítica. Exige

dos generadores capaces de soportar independientemente toda la carga de la instalación. Todo el sistema es tolerante a fallos. **Tier 4 - Según TIA-942**, siempre y cuando se utilicen dos distribuidores diferentes de energía.

Históricamente, ha sido necesario proyectar los requisitos de potencia para la carga crítica pensando en las instalaciones futuras, es decir, haciendo una proyección de 10 a 15 años. Está claro que proyectar este tipo de carga resulta sin sentido por el avance de la tecnología, dado que en la década de los 90s se desarrollo en concepto de **Vatios/Área cuadrada** para proveer un marco para el análisis y la comparación de infraestructuras y esta medida no tuvo éxito por no comprenderse este concepto, por ello, se comenzó a utilizar el de **Vatios/Rack** para referirse a la capacidad del sistema, puesto que este parámetro es más confiable, ya que la cantidad de racks en un lugar determinado es muy fácil de contar.

Sistemas de configuraciones UPS más utilizadas en el mercado

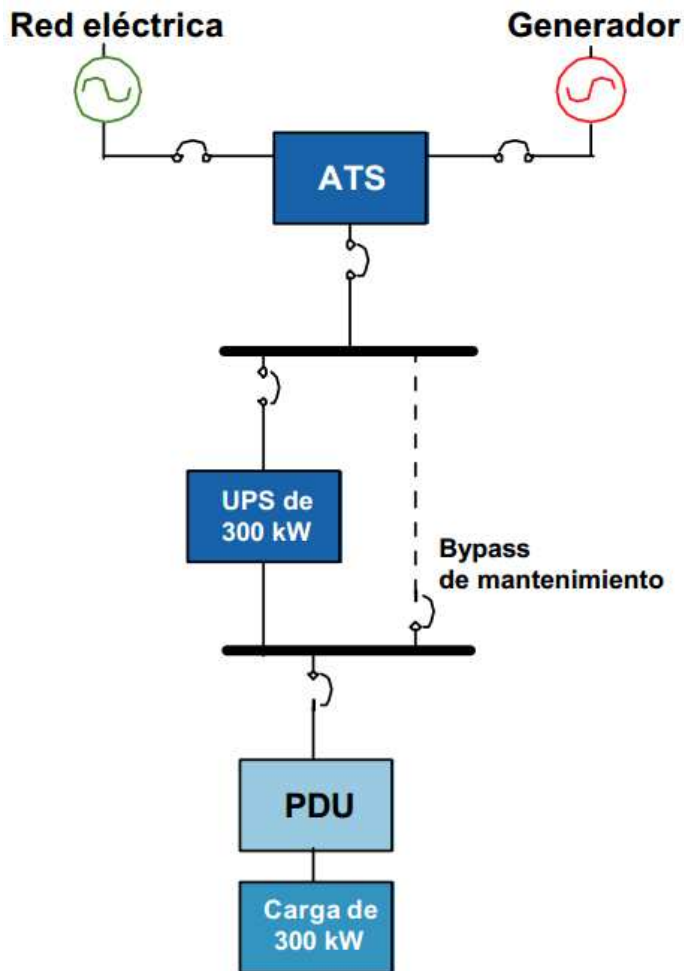
Sistemas de capacidad o sistema N

Un sistema N es un sistema compuesto por un único módulo de UPS, o un conjunto de módulos en paralelo cuya capacidad es igual a la protección de la carga crítica, y esta configuración es la más común en la industria. Por ejemplo una sala de cómputos de 1000 metros cuadrados con una capacidad de diseño proyectada de 500KW es una configuración N ya sea que tenga un solo sistema UPS de 500 KW o dos de 250 KW conectadas en paralelo por un bus común. Estos se consideran configuraciones N, aunque los diseños de los módulos UPS son diferentes. Los sistemas UPS pequeños, que superan la capacidad de 20KW aproximadamente, tienen interruptores de bypass estático que permiten que la carga se transfiera en forma segura a la red eléctrica si el modulo UPS tiene problemas internos. El fabricante selecciona los puntos en los cuales la carga de la UPS se transfiere al bypass estático para proveer la máxima protección para la carga crítica, mientras que al mismo tiempo protege el propio módulo. Un ejemplo de esto sería en módulos trifásicos es común tener regímenes de sobrecargas, de modo que un módulo puede soporta hasta el 125% de la carga nominal por 15 minutos, superado ese porcentaje, el módulo comenzará una rutina de medición del

tiempo por la que un clock interno iniciará una cuenta regresiva de 5 minutos, y cuando dicho tiempo expire si la carga no volvió a los niveles normales, el módulo transferirá la carga en forma segura la **bypass estático**. Existen muchos casos en los que se activa el bypass y se especifica en cada módulo de UPS particular.

Una forma de mejorar el sistema de configuración N es dotarlo de la capacidad de bypass de mantenimiento o externo, porque un bypass externo permite que todo el sistema de UPS (módulos y bypass estático) se apague de manera segura para tareas de mantenimiento cuando es requerido. Dentro del panel que alimenta la UPS se encuentra el bypass de mantenimiento y se conecta al panel de salida, éste es un circuito que normalmente se encuentra abierto y que solo se puede cerrar cuando el módulo UPS está en bypass estático, por consiguiente, deben tomarse ciertas medidas de seguridad en la etapa de diseño para evitar el cierre del bypass de mantenimiento cuando la UPS no está en bypass estático. El bypass de mantenimiento es un importante componente del sistema, bien implementado, permite que el módulo UPS se repare en forma segura sin que sea necesario desconectar la carga.

Gráfica: Un sistema UPS común de un solo módulo.



Ventajas

- Configuración del hardware sencilla y rentable.
- Se utiliza toda su potencia.
- La disponibilidad es superior a la red eléctrica.
- Tiene capacidad de expansión, si crecen los requisitos de potencia. Pueden instalarse varios módulos en paralelo si se respeta su potencia nominal.

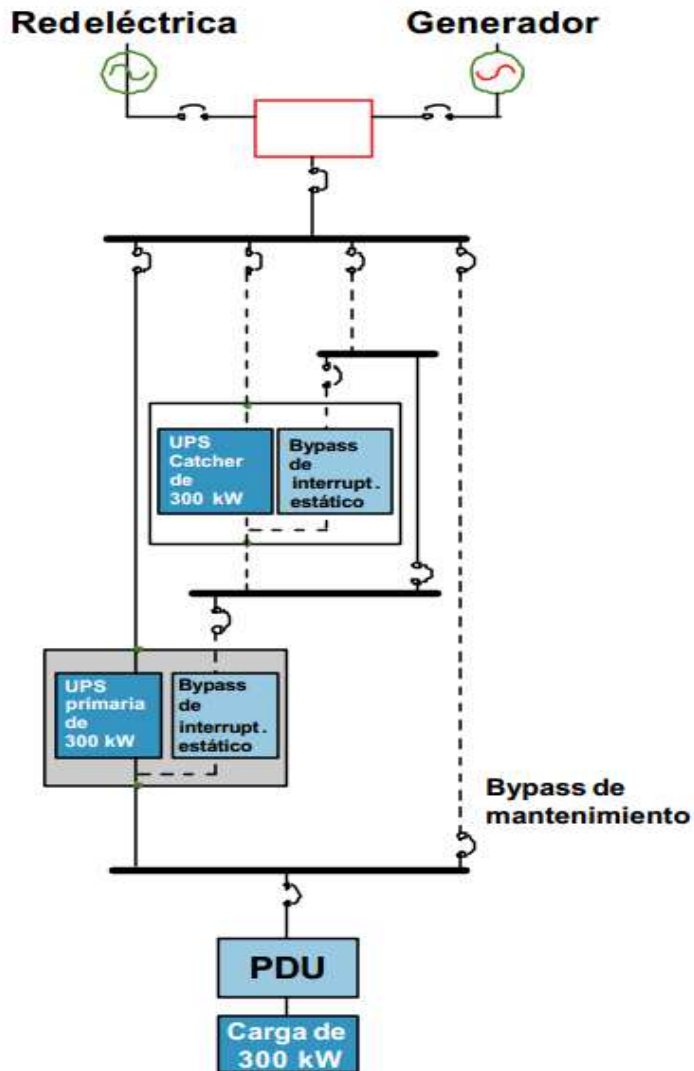
Desventajas

- La disponibilidad es limitada cuando ocurre una falla en un módulo UPS, en cuyo caso la carga se transfiere al bypass, lo que expone a la carga crítica a una fuente de energía no protegida.
- Durante el mantenimiento de la UPS, las baterías o los equipos aguas abajo, se exponen a una carga de una fuente no protegida, y el tiempo es un factor a tener en cuenta.
- La falta de redundancia limita la protección de la carga contra las fallas de la UPS.
- Existen varios puntos de fallas únicos, lo que significa que el sistema solo tiene la confiabilidad de su punto más débil.

Sistema de Redundante aislado

A este sistema se lo llama técnicamente como N+1, sin embargo es distinto a una configuración paralela redundante a la que también se la denomina N+1. Este sistema no necesita que los módulos sean de la misma capacidad y no requiere de un bus paralelo. En esta configuración existe un módulo principal o primario que alimenta la carga. La UPS secundaria o de aislación alimenta el bypass estático. Esta arquitectura requiere que tenga el módulo principal separado para el circuito de bypass estático. Este es el método por el que se logra un nivel de redundancia en una configuración que anteriormente no era redundante sin tener que reemplazar la UPS existente en su totalidad. En el caso de normal operación del sistema, el módulo UPS primario soportará la carga crítica total, y el módulo de aislación no tendrá ninguna carga conectada. Ante un evento por el cual la carga del/los módulos primarios se transfiera al bypass estático, el módulo de aislación aceptará la carga total del módulo primario instantáneamente. Por ende, el módulo de aislación debe elegirse cuidadosamente para garantizar que sea capaz de aceptar la carga rápidamente. De no ser así, podría transferir la carga al bypass estático y así vulnerar la protección adicional que provee esta configuración.

Gráfica: configuración de UPS redundante aislada.



Ventajas

- Heterogeneidad de los componentes en marcas y modelos.
- Brinda tolerancia a fallas.
- No necesita sincronización.

Desventajas

- El sistema depende de la operación adecuada del bypass estático del módulo primario para recibir la potencia del módulo de reserva.
- Se requiere que los bypass estáticos en ambos módulos UPS funcionen correctamente para abastecer una corriente tal que exceda la capacidad del inversor.
- El módulo UPS secundario debe ser capaz de controlar un incremento de la carga repentino cuando el módulo primario transfiera la carga al bypass. (Por lo general , la UPS secundaria funciona por un largo periodo de tiempo con 0 % de carga, no todos los módulos UPS pueden realizar esta tarea, lo que hace que la selección del módulo de bypass sea clave).
- El tablero de conmutación y los controles asociados son complejos y costosos.
- Los costos operativos son más elevados, ya que la UPS secundaria tiene una carga de 0%, que consume energía solo para seguir funcionando.
- Un sistema de dos módulos (uno primario y otro secundario) requiere por lo menos un disyuntor adicional que permita elegir entre la red eléctrica y el UPS secundario como fuente de Bypass. Incrementa más el riesgo de errores humanos por el complejo sistema con un bus de carga común.
- Dos o más módulos primarios necesitan un circuito especial para posibilitar la selección del módulo de reserva a la red eléctrica como fuente del bypass (interruptor estático de transferencia).
- Existe un único bus de carga por sistema, que es un solo punto de falla único.

Sistemas paralelo redundante o sistema N+1

La arquitectura paralela redundante permite que el sistema tolere la falla de un módulo UPS único sin que se deba transferir la carga crítica al sistema de distribución eléctrico. Proteger la carga crítica de las variaciones y cortes del suministro eléctrico de la red es responsabilidad del sistema UPS. El proceso de pasar a un bypass estático o a un bypass de mantenimiento tiene que ser

una práctica de menor frecuencia. La configuración paralela redundante está conformada por varios módulos UPS de la misma capacidad conectados a un mismo bus de salida común. El sistema tiene redundancia N+1 si la capacidad excedente de potencia es por lo menos igual a la capacidad de un módulo del sistema, el sistema tendrá redundancia N+2. Los sistemas paralelos redundantes requieren módulos UPS del mismo fabricante y la misma capacidad, el fabricante también provee el tablero para conexiones en paralelo para el sistema. El tablero posee la inteligencia suficiente para realizar la comunicación necesaria de los módulos UPS individuales, con el fin de generar una tensión de salida que esté completamente sincronizada. El bus paralelo puede tener monitoreo para visualizar las cargas del sistema, ya que necesita mostrar cuántos módulos tiene conectados y cuántos módulos se necesitan para mantener la redundancia del sistema. Los módulos UPS comparten la carga equitativamente cuando el funcionamiento es normal, y cuando uno de los módulos sale de servicio por un motivo determinado, además se necesita que los módulos UPS restantes acepten inmediatamente la carga del módulo UPS que falló. Esta propiedad permite que cualquier módulo pueda extraerse del bus y repararse sin que la carga crítica deba conectarse directamente a la red eléctrica.

En una configuración de sistema N+1, existe la posibilidad de incrementar la capacidad de las UPS a medida que crece la carga crítica. Para ello, los controles de capacidad deben ser lo suficientemente inteligentes para lograr que cuando el porcentaje de capacidad alcance cierto nivel, y el sistema debe poner en operación automáticamente el nuevo módulo equilibrando cargas. Cuanto mayor es la capacidad en potencia requerida por un sistema UPS, mayor es el tamaño y peso del mismo. Por lo general en un Datacenter la sala que alberga estos dispositivos está dimensionada para un cierto crecimiento, tanto de potencia como de espacio físico asignado, por ello, es menester planificar de forma sostenida el crecimiento de estos sistemas.

La eficiencia del sistema puede ser un factor importante a la hora de diseñar un sistema UPS redundante. Por lo general, los módulos UPS con una carga ligera son menos eficientes que los módulos con una carga cercana a su capacidad. La siguiente tabla 1 muestra la carga operativa típica para un

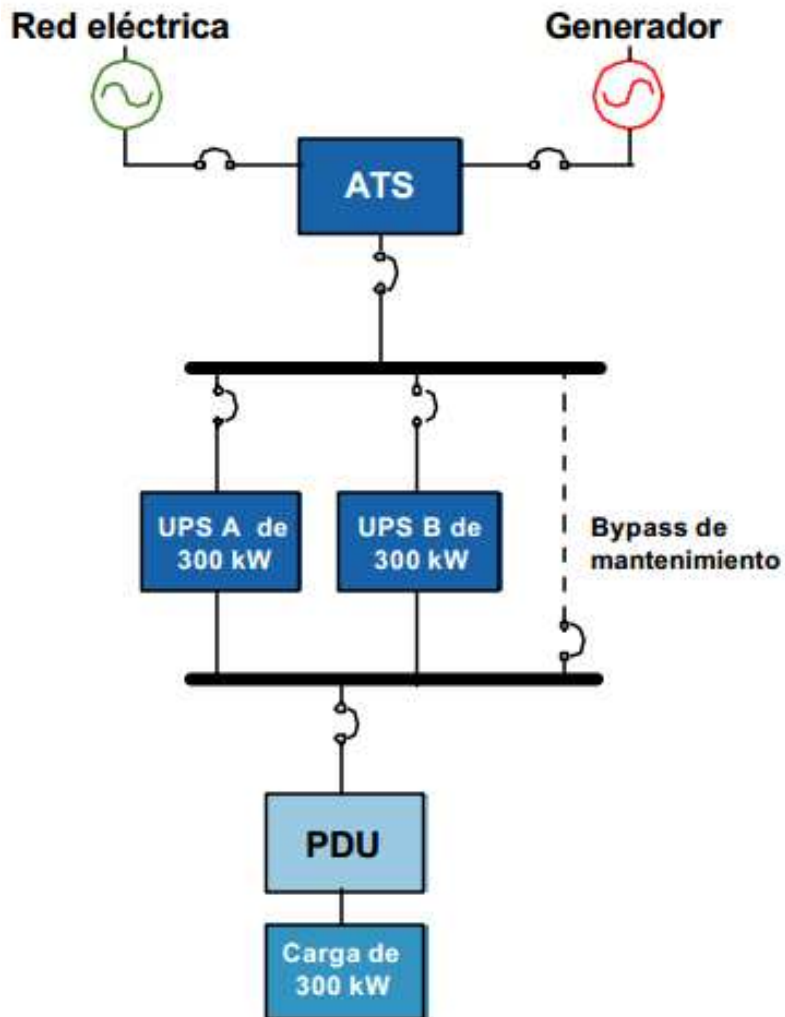
sistema utilizando diversos tamaños de UPS que alimentan una carga de 240 KW en todos los casos.

Tabla 1:

Módulos UPS en paralelo	Carga crítica	Capacidad total del sistema UPS	Porcentaje de carga por módulo UPS
2 x 240 kW	240 kW	480 kW	50%
3 x 120 kW	240 kW	360 kW	66%
4 x 80 kW	240 kW	320 kW	75%
5 x 60 kW	240 kW	300 kW	80%

Mientras que la siguiente gráfica muestra la típica configuración paralela redundante de dos módulos, y esta solución muestra que estos sistemas proveen protecciones contra las fallas de un solo módulo UPS, aunque sigue existiendo un punto único de falla que es el bus paralelo. Por lo tanto, se debe contemplar el diseño de un circuito de bypass de mantenimiento para permitir el cierre del bus paralelo.

Gráfica: Configuración de UPS paralela redundante N+1.



Ventajas

- Posee un nivel de disponibilidad muy alto, por la capacidad extra que se le puede asignar al sistema (módulos en paralelo).
- Las probabilidades de fallas son menores en comparación con las configuraciones redundantes aisladas, ya que esta configuración tiene menos lógicas de control, y los módulos están On-line constantemente (no hay cargas escalonadas).
- Tiene la propiedad de expandir la potencia en función de la carga crítica rápidamente.

- La arquitectura del sistema es flexible en instalación y mantenimiento.

Desventajas

- Todos los módulos deben ser iguales, fabricantes, modelos, régimen de trabajo y configuración.
- Siguen teniendo problemas aguas arriba y aguas abajo del sistema UPS.
- Los niveles de eficiencia operativa son más bajos, ya que ninguna unidad trabaja al 100%.
- Existe un bus carga por sistema que es el único punto de falla.
- Los equipos de la mayoría de los fabricantes necesitan tableros inteligentes externos para compartir la carga equitativamente entre los módulos UPS, además se tiene que tener en cuenta los tableros de bypass de mantenimiento. Por lo tanto, el sistema se torna más complejo y el costo aumenta en mayor medida.

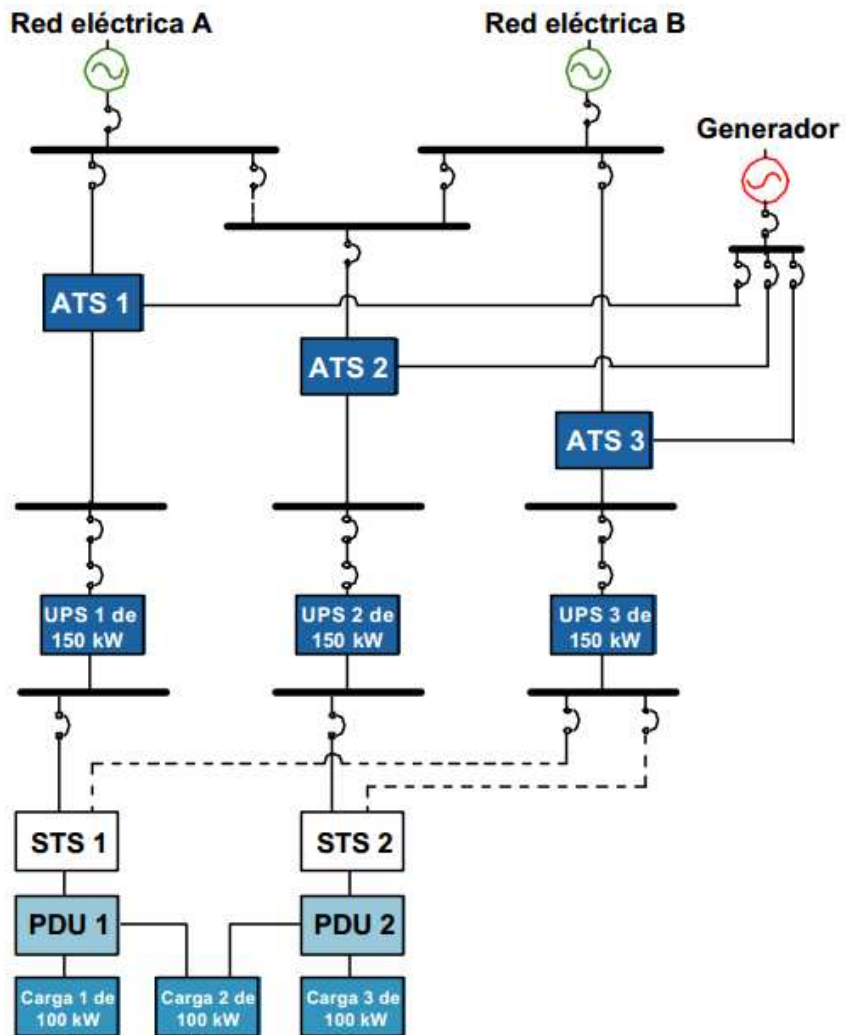
Sistema redundante distribuido

Las configuraciones redundantes distribuidas son utilizadas actualmente en nuestros mercados, y este diseño utiliza tres o más módulos UPS con circuitos de E/S independiente. Por ejemplo, los buses de salidas se conectan a la carga crítica por medio de diversas unidades PDU. Desde la entrada de la red de distribución eléctrica hasta el sistema UPS, las configuraciones redundantes distribuidas de sistema a sistema son muy similares. Minimizan los puntos de fallas y proveen capacidad de mantenimiento concurrente. La diferencia principal es la cantidad de módulos UPS que se necesitan para proveer caminos de energía redundante para la carga crítica y la organización de la distribución desde la UPS hasta la carga crítica, a medida que crece el requisito de carga N, la cantidad de módulos UPS disminuye con el consecuente ahorro de dinero.

La gráfica siguiente muestra una carga de 300KW con dos conceptos de diseño redundante diferentes. Se utilizan tres módulos UPS en una arquitectura redundante distribuida que también se denomina sistema Capcher, y en esta configuración el módulo 3 se conecta a la entrada secundaria de cada STS (Interruptor de transferencia estático), y toma la

carga ante la falla de cualquiera de los módulos UPS primarios, y además posee carga alguna.

Gráfica: Configuración de un sistema UPS redundante distribuida.



Los sistemas redundantes distribuidos se eligen generalmente para instalaciones grandes y complejas donde se requiere mantenimiento concurrente y muchas de las cargas son de cable simple. Esta configuración también genera ahorros con respecto a una configuración 2N. Los factores que motivan el uso de configuraciones redundantes, son:

Mantenimiento concurrente: La función principal de esta operación es cerrar completamente cualquier componente eléctrico o subconjunto para su mantenimiento o prueba de rutina.

Puntos de fallas únicos: Un sistema de configuración N se compone esencialmente de una serie de puntos de falla únicos, y la eliminación de estos puntos es la clave de la redundancia.

STS (Interrupor estático de transferencia): El STS tiene por cometido conmutar entre dos entradas de energía y brindar una salida, es decir, cuando falla una alimentación del UPS primario, el dispositivo transfiere la carga al circuito de alimentación UPS secundario.

La debilidad de este sistema parte del uso de interruptores estáticos para realizar la transferencia, y al ser dispositivos complejos presentan fallas inesperadas, y ésta puede propagarse aguas arriba y dejar fuera de línea off-line todo el sistema UPS.

Sincronización de fuentes diversas: Cuando se utilizan dispositivos STS en un Datacenter, es importante que los circuitos de alimentación de los dos sistemas de UPS estén sincronizados, porque es posible que los módulos UPS se desfasen, especialmente cuando el suministro proviene de baterías. Una solución para evitar una transferencia desfasada es instalar una unidad de sincronización entre los dos sistemas de UPS, lo que permite que las salidas de corriente alterna (**CA**) se sincronicen.

Ventajas

- Permite el mantenimiento concurrente de todos los componentes si todas las cargas son de cable doble alimentación.
- Ahorro de costos en comparación con una arquitectura 2(N+1) debido a la menor cantidad de módulos UPS.
- Posee líneas de energía separadas para realizar alimentación doble.

Desventajas

- Es una solución relativamente costosa en comparación con las configuraciones anteriores, debido al uso generalizado de tableros de

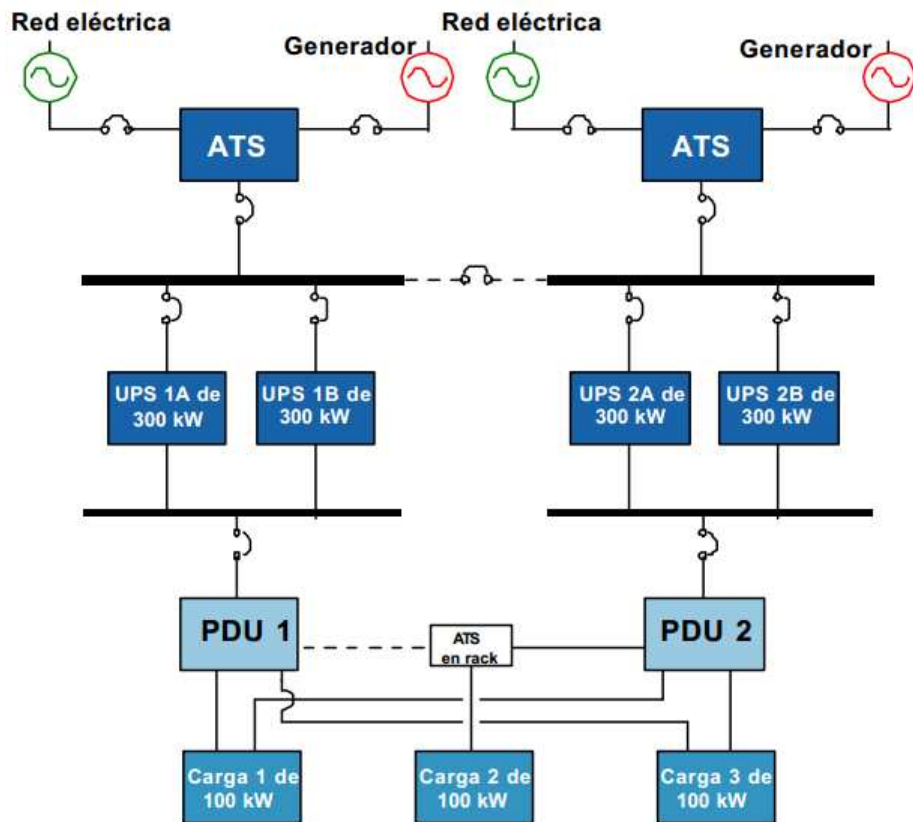
conmutación. El costo es una función del nivel de redundancia que necesitamos para nuestra carga crítica.

- Los puntos de fallas están en los STS.
- Las instalaciones de estos sistemas lleva un alto grado de complejidad como su administración.

Sistema de redundancia con sistema más sistema

Estos sistemas sirven para eliminar todos los puntos de fallas en las configuraciones que se mostraron anteriormente. Este es el diseño más confiable y el más costoso de la industria. La elección de este sistema depende de la visión que tenga el proyectista de hasta dónde quiere preservar o salvaguardar la carga crítica que maneja el Datacenter, es decir, ponderar en tener operativo un 100% del tiempo todas las instalaciones que dan soporte a la carga crítica (core business) y esto no tiene precio. El negocio no puede permitirse estar fuera de servicio por contingencias, y el costo de mantener **Off-line** todos los servicios es más alto que el costo de los sistemas redundantes, por lo que la inactividad de un Datacenter con esta envergadura es inaceptable. Muchos Datacenter eligen esta configuración para proteger su negocio.

Gráfica: Configuración de UPS 2(N+1).



En este ejemplo se muestra que las cargas críticas son de 300KW, por lo tanto, el diseño requiere que se utilicen cuatro módulos de UPS de 300KW, y dos buses paralelos separados para conectar dos módulos a cada uno.

Ventajas

- Los dos caminos de energía hacen que no exista ningún punto de falla único, tienen una alta tolerancia a las fallas.
- La configuración ofrece redundancia completa desde la entrada de la red de distribución eléctrica hasta las cargas críticas.
- En estos diseños 2(N+1), sigue existiendo redundancia en el sistema UPS, incluso durante el mantenimiento concurrente.

Desventajas

- Alto costo de inversión, debido a la gran cantidad de componentes del sistema UPS.
- La eficiencia del sistema UPS disminuye debido al funcionamiento habitual con una carga menor a la completa.

Conclusión:

La infraestructura energética es la clave para la operación exitosa de los equipos de un Datacenter. Existen diversas arquitecturas disponibles en el mercado en lo que respecta a sistemas de alimentación ininterrumpible (UPS) cada uno con sus ventajas y limitaciones. El secreto de su elección, dependerá de varios factores a tener en cuenta. Como ser la tolerancia a los riesgos (contingencias), la disponibilidad de la información, el dimensionamiento de los tipos de cargas (simples o dobles), el costo asociado por la parada del Datacenter (off-line) del negocio, el presupuesto asociado que estaría dispuesto a erogar para la implantación del sistema, y por último, el costo/beneficio asociado; todos estos son los factores a tener en cuenta en la elección correcta del sistema UPS.

Estructuras de racks y montajes de equipos de IT

En la actualidad se tienen racks para servidores de diferentes marcas, modelos, tamaños, y tecnologías por lo que es necesario unificarlos para aprovechar mejor el espacio, y así darle un mejor manejo al control de temperaturas y humedades, y conducir el enfriamiento donde se requiera para así economizar energía. Los racks del centro de cómputo deberán cumplir la Norma EIA-310D, dotar de puertas traseras dividida, puertas delanteras debidamente perforadas para el alojamiento de los dispositivos electrónicos, de forma que permitan garantizar el flujo del aire acondicionado, dentro de los racks del centro de cómputo. Se deberá suministrar e instalar sistemas de gabinetes estandarizados para montar los servidores y equipos activos existentes que permitan la administración organizada de las máquinas. El Datacenter deberá poseer en correcto funcionamiento consolas extraíbles para rack de servidor, que incluyan como mínimo entre otros los siguientes aspectos: Monitor plano LCD de 17", teclado, mouse, accesorios varios.

Sistema de conexión a tierra para equipos de cómputo, comunicaciones y/o telecomunicaciones

El propósito del sistema de conexión a tierra es crear una vía de baja impedancia a tierra física para descargas eléctricas y voltajes transitorios, relámpagos, energía defectuosa, activación de circuitos (motores que se encienden y se apagan), descargas electroestáticas que son causas comunes de estas descargas y voltajes transitorios. Un sistema efectivo de conexión a tierra minimiza los efectos perjudiciales de estas descargas. De modo que se debe adquirir e instalar un sistema de protección a tierra según las normas, las cuales deberán proteger todos los sistemas existentes y el sistema redundante como son bandejas porta cables metálicas, todos los gabinetes eléctricos de cableado y servidores, los sistemas de aire acondicionado, sistemas electrógenos y conductos metálicos que se instalen, etc.

Además se tiene que efectuar los cálculos necesarios para el dimensionamiento del sistema de conexión a tierra física para el centro de cómputo de acuerdo a las especificaciones técnicas y normativas vigentes. El sistema de conexión a tierra física para el Datacenter, deberá diseñarse e implementarse de acuerdo a las siguientes normas:

El estándar TIA-942 define métodos prácticos para asegurar la continuidad eléctrica a lo largo de los materiales de racks y la apropiada conexión a tierra física de racks y equipos montados en racks. El estándar J-STD-607-A-2002, Commercial Building Grounding Earthing and Bonding Requirements for Telecommunications J-STD-607-A-2002, requisitos de conexión y unión a tierra física en edificios comerciales para telecomunicaciones. Este estándar se enfoca en la conexión a tierra física para telecomunicaciones y define un sistema que inicia en la instalación de la entrada principal de conexión a tierra física para telecomunicaciones (el TMGB) y termina en los busbars de conexión a tierra física para telecomunicaciones (TGBs) ubicados en los cuartos de telecomunicaciones.

La **IEEE** provee mayores detalles sobre cómo diseñar la estructura de conexión a tierra para un cuarto de computadoras, a través de una red común de unión a tierra (CBN). La CBN es el conjunto de elementos metálicos que

están interconectados, de manera intencional o casual, para proveer las principales uniones y conexiones a tierra dentro de un edificio de telecomunicaciones. Estos componentes incluyen acero estructural o varillas de refuerzo, plomería metálica, racks para cables, y conductores de uniones a tierra. La CBN está conectada al sistema exterior de electrodos de tierra física. Esto es lo que se conoce como malla de masa metálica.

Lo anteriormente señalado es un punto clave en el diseño del proyecto de las instalaciones y vale resaltar su importancia en la protección de las personas, equipos, instalaciones y la eficiencia operativa. Para mantener el ritmo de los demandantes negocios actuales, los Datacenter deben conseguir niveles de productividad y disponibilidad sin precedentes, razón por la cual los administradores están poniendo cada vez mayor atención en los problemas que se presentan en sus instalaciones e infraestructuras, incluyendo el sistema de conexión a tierra para redes. La adecuada conexión a tierra en un Datacenter es definida por el estándar de Infraestructura de telecomunicaciones para Datacenter **EIA/TIA-942**, y va más allá de los requerimientos del National Electrical Code (**NEC**), para protección de equipos y mejora de la confiabilidad del sistema. La TIA-942 ha adoptado la definición “grados” proporcionada por el Uptime Institute, en la que grado I es el nivel más bajo y permite solamente 28.8 horas de tiempos caídos de información generada en sitio por año. En contraste, el grado IV usado en mercados como el financiero y el de salud, que cuentan con productividad y disponibilidad crítica, tiene accesibilidad de 99.995%, lo que requiere que el Datacenter sea diseñado para experimentar sólo 0.4 horas de tiempo caído anualmente, es decir, menos de 5 segundos por día. Los dos objetivos del sistema de conexión a tierra son igualar potenciales eléctricos y crear una ruta a tierra de baja resistencia. Para lograr estos objetivos, existen cinco principios básicos:

1. El sistema de conexión a tierra debe ser intencional y contar con una cuidadosa planeación, en la que se deberán utilizar únicamente componentes de alta calidad y profesionales capacitados para hacer las conexiones.
2. El sistema de conexión a tierra deberá ser verificable visualmente y medible. Un sistema como éste puede ser inspeccionado por degradación

y es accesible para realizar movimientos, adiciones y cambios, asegurando una confiabilidad y posibilidad de expandir la capacidad del sistema a largo plazo. Desde el diseño se debe tener siempre presente la posibilidad de realizar una re-ingeniería.

3. El sistema de conexión a tierra deberá ser dimensionado adecuadamente. El uso inapropiado de líneas directivas puede reducir la disponibilidad de la red y causar caídas prematuras del equipo que contribuyen a incrementar costos de operación.
4. El sistema de conexión a tierra deberá desviar las corrientes dañinas fuera del equipo. Durante una descarga de corriente, los racks en cadena se energizan de más provocando daños en el equipo.
5. Todos los componentes metálicos en el Datacenter deberán ser unidos al sistema de conexión a tierra para minimizar el flujo de corriente. La corriente fluye cuando hay una diferencia potencial entre componentes. Si la corriente fluye a través de una pieza del equipo, algún daño puede ocurrir, por esto, equipos como racks, gabinetes y bandejas para cableado deben estar unidos al sistema de conexión a tierra.

Gráfica: Sistema de puesta a tierra de un sala.



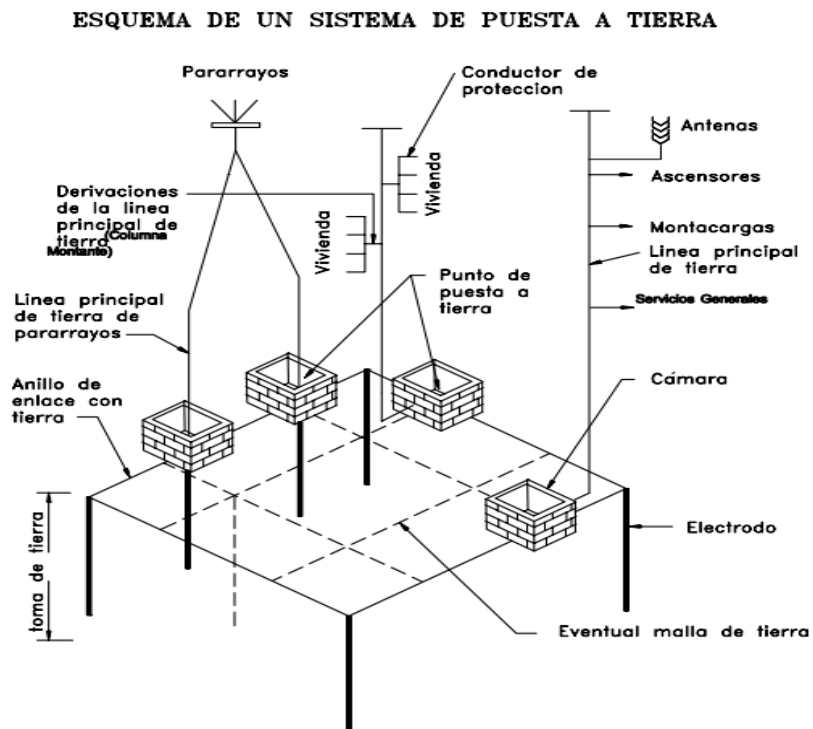
Razones para la instalación de un sistema de puesta a tierra

- Impedancia suficientemente baja.
- Seguridad dentro de la sala y el edificio contenedor.
- limitar el voltaje dentro de los límites razonables.

Para finalizar, una cuestión importante es generar continuidad eléctrica a lo largo de los racks y gabinetes. En el Datacenter, la continuidad en racks y gabinetes es importante para asegurar la protección de descargas electrostáticas y para la apropiada conexión a tierra de interruptores y sistemas de protección eléctrica. Los racks estándar y normalizados poseen una acometida específica para la masa metálica.

Un inconveniente común en los equipos de datos, es la pérdida de sincronismo por una malla de referencia a la malla de masa metálica y real de la puesta a tierra, una sin la otra no permiten un correcto funcionamiento de los equipos.

Gráfica: Esquema de un sistema de puesta a tierra.



Sistemas de monitoreo ambiental y físico del Datacenter

Con el fin de generar un esquema homogéneo de monitoreo de los servidores, equipamiento ambiental, etc., ubicados en el Datacenter, se deberá suministrar, instalar y poner en funcionamiento los distintos sistemas que convivirán. El siguiente es un breve resumen de los puntos a abordar:

- Sistema Ambiental: Suministro, instalación y configuración de la unidad principal de administración ambiental junto con los sensores requeridos de acuerdo a las especificaciones técnicas definidas para éste ítem.
- Sistema Eléctrico: Conexión eléctrica para el suministro de potencia de la unidad principal.
- Interconexión Lógica: Conexión general de todos los sistemas.
- Ejecución de pruebas: Simulacros y pruebas del sistema en su totalidad.

Sistema de detección y extinción de incendios

El Datacenter debe poseer un sistema de detección y extinción de incendio, en todos los cuartos involucrados en el funcionamiento del mismo. El sistema de detección y extinción de incendios deberá cubrir los riesgos de incendio y conflagración mediante un sistema electrónico de detección, alarma y extinción automática compatible con las normas vigentes. El sistema de detección de incendios deberá detectar conatos⁵ de incendio y conflagraciones, mostrando oportunamente a los operadores para apoyar los planes de extinción y evacuación.

Se requiere un sistema de detección y extinción de incendios a base de Argón, o Ecaro 25⁶ u otro agente de iguales o superiores características, con gas reglamentado por la norma **NFPA (National Fire Protection Association)** 2001, listado **UL (Underwriters Laboratories)** y aprobado **FM (Factory Mutual)**. Se debe garantizar que el agente extintor utilizado para el

⁵ Acción o suceso que se inicia pero no continúa

⁶ El agente limpio (clean agent) ECARO 25 es un compuesto químico conformado por pentafluoretano, especialmente diseñado para áreas críticas, no produce efectos dañinos en equipos, personas ni medio ambiente, además no requiere de interrupción de la operación de equipos en caso de descarga.

sistema de detección y extinción de incendios, cumpla con las siguientes características, entre otras:

- Que corresponda al grupo de agentes limpios.
- Que sea un agente no tóxico.
- Que permita protección a los bienes.
- Que brinde protección a las personas, permitiéndole respirar en una atmósfera reducida de oxígeno cuando el agente es descargado.
- Que no dañe el medio ambiente y la capa de ozono (ecológico).

El sistema de detección deberá contar con un panel de control, y con conexión física a detectores de humo, los cuales deberán estar localizados sobre el techo y bajo el piso falso del Datacenter. Este poseerá documentado los cálculos hidráulicos del sistema de detección y extinción de incendios, de acuerdo a la norma **NFPA 2001** (National Fire Protection Association) por medio de un software especializado y desarrollado por los fabricantes de los equipos de detección y extinción de incendios.

La solución propuesta debe ser diseñada e instalada de acuerdo con las normas y códigos existentes, NFPA (National Fire Protection Association), UL (Underwriters Laboratories) y FM (Factory Mutual), entre otros. De acuerdo con los resultados del estudio de los cálculos hidráulicos, se deberá ofrecer las cantidades mínimas necesarias de los siguientes componentes que garanticen la efectividad del sistema para la detección y extinción de incendios:

- Cilindros para almacenamiento del agente argón o ecaro 25 u otro agente de iguales o superiores características, con válvula de descarga.
- Agente extintor (argón o ecaro 25, igual o superior).
- Mangueras de descarga.
- Actuador eléctrico.
- Actuador manual.
- Interruptor de presión.
- Supervisor de baja presión.
- Boquilla de descarga.

- Avisos de alarma sobre el agente extintor.
- Tablero de control.
- Detectores de humo y temperatura.
- Cornetas con luz.
- Módulos de monitoreo y control.
- Planos de todos los sistemas implementados.
- Manuales entrenamiento y operación.
- Plan de evacuación.
- Comité de crisis.
- Plan de restauración (Director técnico de crisis).

Se deberá garantizar que los sistemas (Argón o Ecaro 25, u otro agente de iguales o superiores características), actúen por concentración en volumen, en los sitios a proteger, por lo tanto la estanqueidad de dichos sitios debe ser suministrada y garantizada en la solución propuesta. Se debe permitir la evacuación antes de actuar. El equipo debe tener una parte de detección y una de actuación, de tal manera que se disponga de detectores que eviten totalmente falsas alarmas, tal como se exige en los estándares técnicos para este tipo de instalaciones de alta seguridad.

El Datacenter debe especificar a través de políticas de seguridad el modo de operación del sistema, detallando como mínimo la forma de garantizar la continuidad en el servicio, en el caso de falla en el suministro de corriente (Plan de contingencia). El sistema de detección debe ser de tecnología de punta tipo direccionable e inteligente, el cual recibe las señales de los detectores de humo o temperatura ubicados en los diferentes sitios. El tablero al recibir la señal de un detector, procesa la señal y da una alarma por medio de la corneta con luz de alarma. Después de verificar la señal por medio del accionamiento de otro detector, da una señal eléctrica al solenoide del actuador eléctrico de los cilindros del agente extintor, para iniciar la inundación total con el agente en el recinto protegido, sobre y bajo el piso falso y extinguir el fuego en un tiempo no mayor a sesenta (60) segundos. Paralelamente da la señal de apagar el aire acondicionado, la válvula solenoide puede ser accionada manualmente mediante la operación de la estación manual ubicada en la salida de las áreas protegidas.

El sistema debe operar de acuerdo a los siguientes parámetros:

- Inundación total del volumen protegido, con una concentración del 7% según la norma **NFPA**.
- Detección por medio de zona cruzada con detectores en cada zona, garantizando cobertura a cada área interna del Datacenter.
- Descargas con baterías de cilindros comunes en cada uno de los sitios involucrados en la solución.
- Garantizar el hermetismo de las áreas a proteger en el Datacenter.

Teniendo en cuenta el estudio de los cálculos hidráulicos, las áreas internas del Datacenter deberán estar protegidas con bancos de cilindros independientes de **Argón** o **Ecaro 25**, u otro agente de iguales o superiores características, los cuales serán ubicados en los sitios de común acuerdo. En caso de ser necesario, también deben poder ser accionados mecánicamente (en el sitio) mediante la operación del actuador manual integrado al actuador eléctrico del cilindro, para garantizar que el sistema de cada área pueda ser operado de 3 formas diferentes a saber:

- Automáticamente (por medio de detectores).
- Eléctricamente (por medio de la estación manual).
- Manualmente (por medio del actuador manual).

Luego de ser descargado el agente extintor, debe ser conducido al área afectada mediante una red de tuberías de acero y aplicado mediante boquillas de inundación total. La solución del sistema de detección y extinción de incendios propuesta debe conectarse al sistema de respaldo ininterrumpido de potencia. Además el Datacenter debe ser dotado de extintores manuales, aunque posea otros sistemas contra incendio instalado, en la siguiente tabla se detalla la clasificación de incendios y sus respectivos extintores.

Gráfica: Sistema de extinción de incendios.



Gráfica: Tabla de clasificación de extintores.

TIPOS DE MATAFUEGOS							
	A Agua	AB Agua + Espuma Química	ABC Polvo Químico Seco	BC Dióxido de carbono (CO ₂)	ABC Halotron 1	D Polvo Químico D	K Potasio
 Sólidos	SI	SI	SI	NO	SI	NO	NO
 Líquidos	NO	SI	SI	SI	SI	NO	NO
 Eléctricos	NO	NO	SI	SI	SI	NO	NO
 Metales	NO	NO	NO	NO	NO	SI	NO
 Grasas	NO	NO	NO	NO	NO	NO	SI

Detectores de incendios

A los detectores podemos clasificarlos en dos tipos: de humo (iónico o fotoeléctrico) y de calor. Los detectores de humo iónicos detectan productos visibles o invisibles de combustión utilizando la ionización de gases por partículas Alpha emitidas por una pequeña cantidad de americio, el humo ionizado reduce la resistencia eléctrica del circuito que pasa a ser conductor Ideal para fuego con llamas. Los sensores fotoeléctricos utilizan una fuente de luz direccionada de tal forma que el rayo luminoso no llegue a la foto celda cuando las partículas de humo entran en el detector. Este tipo de detector es ideal para fuegos lentos sin llamas, locales con movimiento de aire. Los detectores deben ser instalados en las entradas y retorno de aire acondicionado, en el techo falso y piso falso.

Sistema eléctrico

Teniendo en cuenta el proyecto se requiere de la implementación de sistemas eléctricos con circuitos principales, circuitos secundarios tanto de corriente normal como regulada con su debida protección e igualmente sistemas de iluminación y control en los diferentes puntos de entrada al Datacenter y acceso principal.

Instalación de tableros de distribución eléctrica redundantes requeridos

Se requiere instalar tableros de distribución eléctrica para la instalación del sistema de cómputo, líneas de carga de rack de una cantidad determinada de potencia (**Kw**), y demás sistema que forman parte del sistema eléctrico general del Datacenter.

Sistema de iluminación automatizado

Se requiere la instalación de un sistema de iluminación para todos los pasillos de equipos y en las áreas aledañas para la iluminación de acuerdo a los requerimientos del Datacenter de 500 luxmen a un metro de altura, de igual forma estos sistemas deben estar controlados automáticamente para que se enciendan solamente las áreas donde haya movimientos de personas. El sistema de iluminación contempla el sistema de emergencia en salas críticas, en caso de cortes de energía no programados.

Adecuaciones físicas

Consiste en el manejo adecuado de todas las áreas intervenidas a las cuales se les debe realizar mejoras de estructura y acabados acorde con las normas en el caso de una construcción edilicia ya existente. En caso contrario de tratarse de una nueva estructura y de haber definido previamente el tipo de Datacenter que necesitamos, definición del Tier, realizaremos de ser necesario el nuevo proyecto edilicio acorde a las normas que nos regimos.

Las áreas en mención son:

- Pisos y techos falsos.
- Paredes del centro de cómputo.
- Centro de operaciones (NOC).
- Cuartos de sistemas UPS.
- Áreas de sub-estaciones eléctricas.
- Cuarto de entrada de servicios, los pasillos, las oficinas y otras.
- Sala de refrigeración.
- Sala de generación.
- Sala baterías (opcional).

Distribución física propuesta del Datacenter

1. Sistemas de aire acondicionado.
2. Sistema de aire acondicionado (enfriamiento de filas).
3. Sistemas de **UPS** y distribución de potencia regulada.
4. Suministro y puesta en funcionamiento de racks y hardware para el montaje de equipos de **IT**.
5. Sistema de puesta a tierra para equipos de cómputo y comunicaciones.
6. Sistema de monitoreo ambiental y físico.
7. Sistema de gestión centralizada para la infraestructura.
8. Sistema de detección y extinción de incendios.
9. Sistema de seguridad y control de acceso.

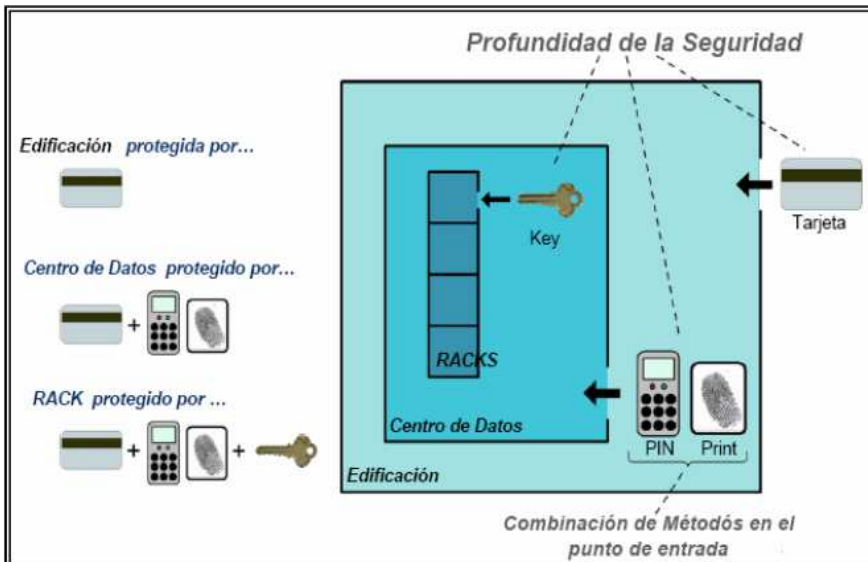
10. Sistema de cableado estructurado.
11. Suministro y puesta en funcionamiento de un sistema eléctrico.
12. Adecuaciones Físicas.
 - Paredes.
 - Cuarto de operadores.
 - Cuarto de entrada de servicios.
 - Puertas de seguridad.
 - Piso falso.
 - Adecuación del techo.
 - Iluminación principal y de emergencia.
14. Alimentación auxiliar (Red Normal).

Sistema de seguridad y control de acceso

El Datacenter deberá contemplar lectoras de huella dactilar y/o iris en cada puerta de acceso. El sistema de identificación biométrico de huella dactilar o iris debe garantizar que los datos leídos sean de carácter único en cada ser humano, lo que garantizará solamente el acceso al personal autorizado. Es requerido que el Datacenter posea en funcionamiento cámaras para el control visual, con el propósito de dar cobertura a las puertas de acceso y demás áreas del centro de cómputo, las cuales deberán ser instaladas en los sitios de común acceso.

El sistema de seguridad y control de acceso, debe conectarse al sistema de respaldo ininterrumpido de potencia. El sistema de seguridad y control de acceso deberá permitir la desactivación total de todas las puertas del centro de cómputo, en el supuesto caso de que el sistema de detección y extinción de incendios se active al recibir las señales de los detectores de humo o temperatura. El sistema de seguridad y control de acceso deberá permitir la desactivación total de todas las puertas del centro de cómputo, mediante la activación de un botón anti pánico de forma manual, el cual será ubicado en el sitio que se defina para tal fin, de común acuerdo.

Gráfica: Distintos tipos de control acceso aplicados a un Datacenter.



CAPÍTULO 4- Cableado

Sistema de cableado estructurado

En el Datacenter se requiere la instalación de bandejas porta cables para llevar las acometidas y realizar la distribución de cableado lógico (Datos) y energía a los gabinetes de distribución principales, a los gabinetes secundarios, a los gabinetes de comunicación de datos y a los gabinetes de servidores, ya que en estas bandejas se instalarán todos los cables, y se deberá destinar una para las acometidas eléctricas normal y regulada, y otra para el cableado de fibras ópticas, cableado UTP troncal, cables multipares, cables coaxiales principales, etc., mientras que en los cuartos del sistema UPS, de entradas de servicio y el cuarto de backbone, debe hacerse llegar las bandejas antes mencionadas en los tamaños requeridos para la distribución de cableados eléctricos y lógicos. Estas deberán ser debidamente instaladas y pintadas de acuerdo a las normas eléctricas vigentes. En estas bandejas se instalarán todos los cables, una bandeja para las acometidas eléctricas normal y regulada y otra bandeja para el cableado lógico tales, cableado UTP, cable multipares, cables coaxiales, etc.

La fibra es extremadamente delicada y por ser un centro de datos con equipos activos y servidores de misión crítica requiere de conductos especiales para fibra, por lo que se deberá instalar bandejas de fibras ópticas entre los gabinetes distribuidores de cableado, los gabinetes de cableado de fibra y los gabinetes de servidores y/o switch que lo requieran. Estas bandejas deberán instalarse debidamente de acuerdo a las normas para conductos y fibras, y es obligatorio utilizar toda la gama de accesorios disponibles tales como soportes, fijadores, curvas, codos de los tamaños adecuados a la bandeja a instalar y que cumplan con las normas. En estas bandejas se instalarán todos los cables de fibra óptica únicamente.

En el pasado había dos especificaciones principales de terminación de cableado: Los cables de datos y por otro lado, los cables de voz. En la actualidad, los sistemas de Cableado Estructurado (**CE**), soportan una gran cantidad de servicios y aplicaciones (voz, datos, video, texto, imágenes), tales como:

- Teléfonos, conmutadores.
- TV, Audio estéreo, DVD, VCR.
- Computadoras.
- Módems, máquinas de fax.
- Receptores de satélite.
- Sistemas de seguridad.
- Sistemas de automatización.
- Control de luces.
- Enrutadores, switches, access points, etc.

En 1985, muchas compañías de la industria de las telecomunicaciones estaban desconcertadas por la falta de estándares de cableado, entonces la EIA (Electronics Industries Associations) comenzó a desarrollar un estándar para este propósito. El primer borrador (draft) del estándar no fue liberado sino hasta julio de 1991, y se le asignó el nombre de EIA/TIA-568. En 1994, el estándar fue renombrado a EIA/TIA-568A, el existente estándar de AT&T 258A fue incluido y referenciado como EIA/TIA-568B. Estos estándares de facto se hicieron populares y ampliamente usados, después fueron adoptados por organismos internacionales como el ISO/IEC11801:1995.

En un NOC de un Datacenter, miles de cables pueden ingresar a la instalación y salir de ésta. El cableado estructurado crea un sistema de cableado organizado que los instaladores, administradores de red y cualquier otro técnico que trabaje con cables puede comprender fácilmente. La administración de cables cumple varios propósitos. Primero, presenta un sistema prolijo y organizado, que ayuda a determinar problemas de cableado. Segundo, la optimización del cableado protege a los cables del daño físico y de las interferencias EMI⁷, lo que reduce en gran medida la cantidad de problemas experimentados.

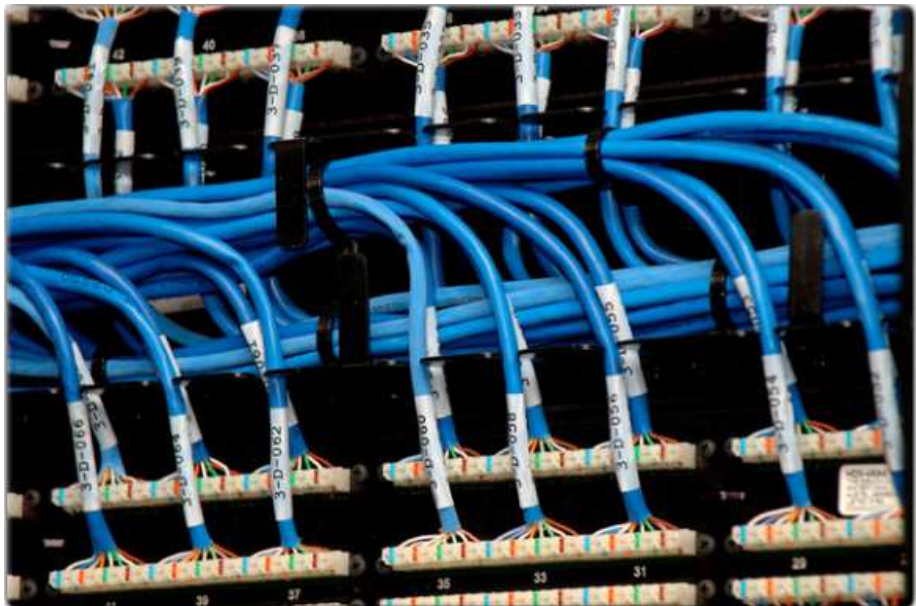
Para brindar asistencia en el proceso de resolución de problemas:

- Todos los cables deben estar etiquetados en ambos extremos, mediante convención estándar que indique origen y destino.
- Todos los tendidos de cableado deben ser documentados en el diagrama de topología de la red física.
- Todos los tendidos de cableado, tanto de cobre como de fibra, deben probarse de extremo a extremo mediante el envío de una señal a través del cable y la medición de la pérdida.

Los estándares de cableado especifican una distancia máxima para todos los tipos de cable y todas las tecnologías de red. Por ejemplo, el **IEEE** especifica que para una Fast Ethernet sobre cable de par trenzado no blindado (**UTP** unshielded twisted pair), el tendido del cableado desde el switch hasta el host no puede superar los 100 metros (aproximadamente 328 pies). Si la longitud del cableado es mayor que el largo recomendado pueden ocurrir problemas con las comunicaciones de datos, especialmente si las terminaciones de los extremos del cable no están totalmente terminadas. La documentación del plan y de las pruebas de cables es fundamental para el funcionamiento de la red.

⁷ Perturbación en un circuito electrónico causada por una fuente eléctrica externa.

Gráfica: Identificación del cableado.



El sistema de cableado estructurado (**SCE**) es una serie de estándares definidos por la EIA/TIA que definen como diseñar, construir y administrar un sistema de cableado que es estructurado, es decir, que el sistema está diseñado en bloques que tienen características de desempeño muy específicas. Un **SCE** se refiere a todo el cableado y componentes instalados en una red basados en un orden lógico y organizado.

Tipos de organizaciones de estándares de cableado

Hay muchas organizaciones involucradas en el cableado estructurado en el mundo. En Estados Unidos es la ANSI, TIA e EIA, Internacionalmente es la ISO (International Standards Organization). El propósito de las organizaciones de estándares es formular un conjunto de reglas comunes para todos en la industria; en el caso del cableado estructurado para propósitos comerciales el propósito es proveer un conjunto estándar de reglas que permitan el soporte de múltiples marcas o fabricantes. Existen varias referencias en **SCE** alrededor del mundo, tales como:

- EIA/TIA-568A/B El primer estándar de cableado estructurado publicado en EUA por la EIA/TIA en 1991.
- ISO/IEC11801 Versión internacional del estándar EIA/TIA-568.
- CENELEC EN 50173 Estándar de cableado estructurado británico.
- CSA T529 Estándar de cableado estructurado Canadiense.

El estándar de cableado estructurado EIA/TIA-568 fue diseñado para:

- Un sistema de cableado genérico de telecomunicaciones para edificios comerciales.
- Definir un tipo de medio, topología, terminaciones y puntos de conexión y administración.
- Soportar ambiente de múltiples vendedores y productos.
- La habilidad para planear e instalar cableado de telecomunicaciones para edificios comerciales sin previo conocimiento de los productos que se utilizaran en el cableado.

Los 6 subsistemas del cableado estructurado

1. Entrada al edificio

La entrada de servicios del edificio es el punto en el cual el cableado externo hace interfaz con el cableado backbone dentro del edificio. Este punto consiste en la entrada de los servicios de telecomunicaciones al edificio (acometidas), incluyendo el punto de entrada a través de la pared y hasta el cuarto o espacio de entrada. Los requerimientos de la interface de red están definidos en el estándar EIA/TIA-569A.

2. Cuarto de equipos

El cuarto de equipos es un espacio centralizado dentro del edificio donde se albergan los equipos de red (ruteadores, switches, mux, PBXs, video, etc.), los aspectos de diseño del cuarto de equipos están especificados en el estándar EIA/TIA-569A.

3. Cableado de backbone

El cableado de backbone permite la interconexión entre los gabinetes de telecomunicaciones, cuartos de telecomunicaciones y los servicios de la entrada, además tiene:

- Conexión vertical entre pisos (cables puentes).
- Cables entre un cuarto de equipos y cables de entrada a los servicios del edificio (distribuidores).
- Cables entre edificios (enlaces).

Gráfica: Tipos de cables requeridos para backbone.

Tipo De Cable	Distancias Máximas Backbone
100 ohm UTP (24 o 22 AWG)	800 metros (Voz)
150 ohm STP	90 metros (Datos)
Fibra Multimodo 62.5/125 μm	2,000 metros
fibra Monomodo 8.3/125 μm	3,000 metros

4. Gabinete o rack de telecomunicaciones

El rack de telecomunicaciones es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Es el primer punto de conexión físico entre el proveedor de servicio y el Datacenter.

5. Cableado horizontal

El sistema de cableado horizontal se extiende desde el área de trabajo de telecomunicaciones al rack de telecomunicaciones y consiste en lo siguiente:

- Cableado horizontal.
- Interconexión.
- Enchufe de telecomunicaciones.
- Terminaciones del cable.

A continuación, tres tipos de medios son reconocidos para el cableado horizontal, cada uno debe de tener una extensión máxima de 90 metros:

- Cable UTP 100-ohm, 4-pares, (24 AWG).
- Cable 150-ohm STP, 2-pares.
- Fibra óptica 62.5/125- μ m.

6. Área de trabajo

Los componentes del área de trabajo se extienden desde la terminal de conexionado a los dispositivos o estaciones de trabajo.

Los componentes del área de trabajo son los siguientes:

- Dispositivos: Computadoras, terminales, teléfonos.
- Cables de patcheo: Cables modulares, cables adaptadores/conversores, jumpers de fibra.
- Adaptadores: deberán ser externos al enchufe de telecomunicaciones, en general, se instalarán en el equipo terminal.

Gráfico: Terminales de pared para telecomunicaciones.



Gráfico: Racks o gabinetes de telecomunicaciones.

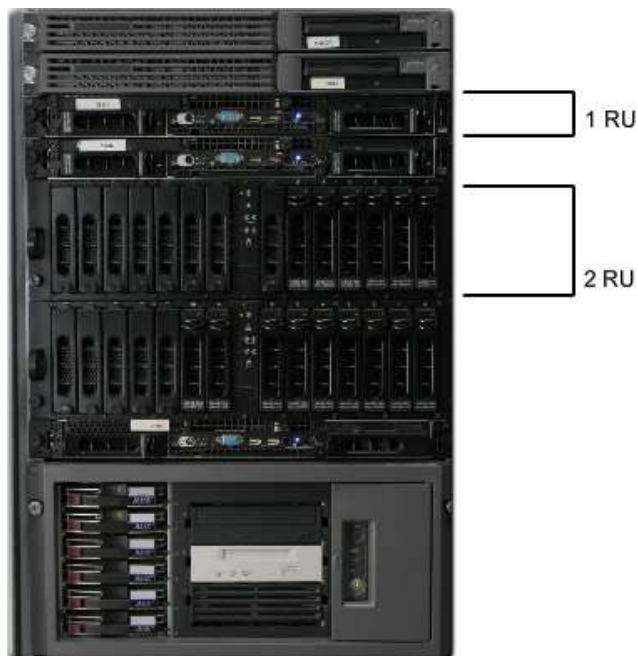


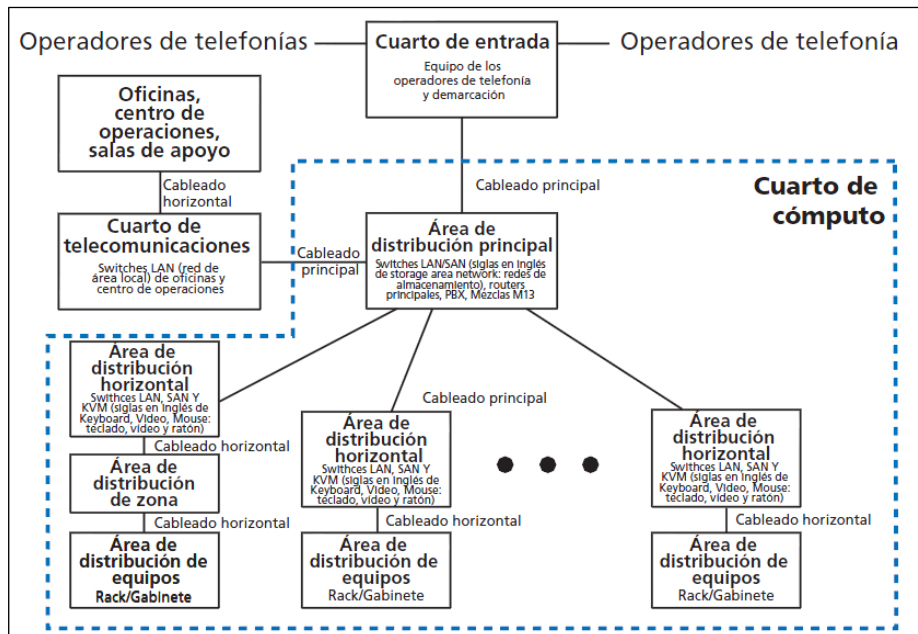
Gráfico: Paneles de patcheo (patch panel).



Topología física del Datacenter

El sistema de cableado de un Datacenter es una estructura que debe soportar múltiples productos de conectividad, por ello se deben seguir los estándares definidos que correspondan.

Gráfica: Datacenter que cumple con el estándar TIA-942.



Elementos del cableado estructurado del Datacenter TIA-942

- Salas de computadores.
- Salas de telecomunicaciones.
- Área de distribución principal.
- Área de distribución horizontal.
- Cableado de backbone.
- Cableado horizontal.

Beneficios del sistema de cableado

- Basado en un estándar.
- Soporta velocidades y anchos de banda elevados.
- Infraestructura física integral.

- Mayor vida útil del cableado.
- Continuidad del negocio, eficiencia operativa.
- Escalabilidad.

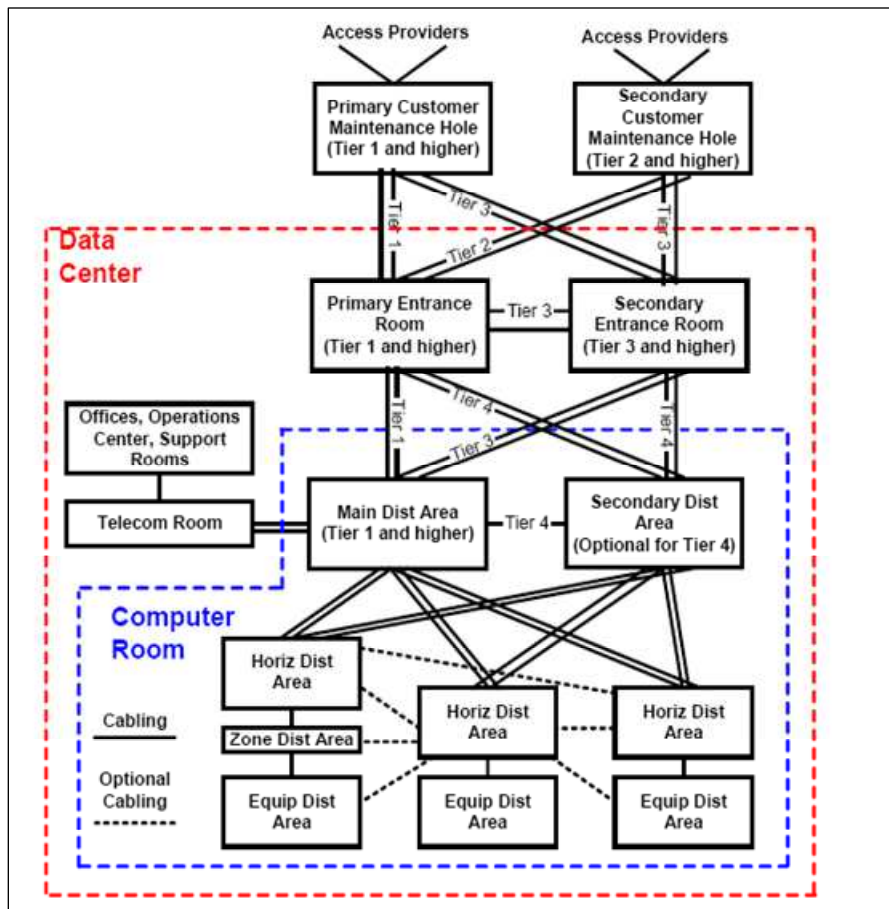
Consideraciones de diseño

- Aparte de redundancias en sistemas eléctricos y mecánicos, deben de haber redundancias en cableado estructurado de acuerdo a nivel (Tier) deseado:
 - ✓ Proveedores de servicios redundantes.
 - ✓ Acometidas redundantes.
 - ✓ Rutas de canalizaciones redundantes.
 - ✓ Cableado vertical redundante.
 - ✓ Cableado horizontal redundante.
- Flexibilidad respecto a los servicios soportados.
- Sistema de cableado relacionado con la capacidad del canal.
- Respetar las especificaciones y recomendaciones de los fabricantes de los equipos.
- Plantear el diseño de acuerdo a los lineamientos de EIA/TIA-942.
- Los materiales deben de ser listados (**UL** o **ETL**) para garantizar niveles de calidad.

Detalles del sistema de transmisión de datos

El crecimiento de un Datacenter es rápido y significativo. Las grandes empresas crecen el 50% anual en datos, por lo tanto las redes de cables se vuelven más complejas y dispares debiendo transportar no sólo datos, sino también voz, imágenes y señales de control, ante esto surge una urgente necesidad de integración y de contar no solo con un sistema de cableado genérico sino que éste debe ser redundante o tolerante a fallas como se muestra en la figura.

Gráfica: Topología redundante según estándar EIA/TIA-942.



El estándar ISO 11801:2002 ofrece lineamientos para la implementación de un sistema de cableado tolerante a fallas capaz de adaptarse a diferentes aplicaciones para que las futuras modificaciones sean fáciles de realizar adicionalmente. Además, como se muestra en la figura anterior, este estándar debe estar acompañado del estándar **EIA/TIA-568-B** que establece el criterio técnico para la configuración del sistema de cableado. Los requerimientos generales para la implementación son:

Distribuidor de campus (CD): Las instalaciones de la entrada del edificio proporcionan el punto en el que las interfaces de cableado salen y se interconecta con el cableado del backbone. Los requisitos físicos de la interfaz de la red se definen en el estándar de **EIA/TIA-569-B**. Para Europa

refiera a **EN50174-1** y a **EIA/TIA-568-B** para las especificaciones de los E.E.U.U..

Distribuidor de edificio (BD) / equipment room facility (ER): Los aspectos del diseño del cuarto de BD/ER se especifican en el estándar de **EIA/TIA-569-B** y del **EN 50174-1**. Este sitio contiene servidores y switches de telecomunicaciones, y sirve para interconectar el cableado distribuidor del campus con el cableado del distribuidor del edificio.

Cableado del backbone: El propósito del cableado del backbone 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.

Distribución de piso (FD) / telecommunications room (TR): El cuarto FD/TR es el área dentro del edificio que alberga el sistema de cableado de telecomunicaciones. Incluye las terminaciones y/o conexiones cruzadas horizontales y el sistema de cableado del backbone, sirve para efectuar la interconexión entre el cableado horizontal y el cableado vertical.

Cableado vertical: Es el conjunto de cables que se utilizan para efectuar la interconexión entre el distribuidor de edificio y los distribuidores de planta.

Cableado horizontal: El cableado horizontal incorpora el sistema de cableado que se extiende desde el área de trabajo de telecomunicaciones, hasta el cuarto de telecomunicaciones, éste debe estar implementado en topología estrella, que consiste de dos elementos básicos:

Cable horizontal y hardware de conexión: (También llamado cableado horizontal), proporcionan los medios para transportar señales de telecomunicaciones entre el área de trabajo y el cuarto de telecomunicaciones. Estos componentes son los contenidos de las rutas y espacios horizontales.

Rutas y espacios horizontales: (También llamado "Sistemas de Distribución Horizontal") Las rutas y espacios horizontales son utilizados para distribuir y soportar cable horizontal y conectar hardware entre la salida del área de trabajo y el cuarto de telecomunicaciones. Estas rutas y espacios son los "Contenedores" del cableado horizontal.

El cableado horizontal incluye:

- Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo. En inglés: work área outlets (**WAO**).
- Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
- Paneles de empate (Patch) y cables de empate utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

Punto de transición: Este punto sirve para adaptar distintos tipos de cable horizontal en aquellas instalaciones en las que sea necesario el tendido de distintos soportes físicos.

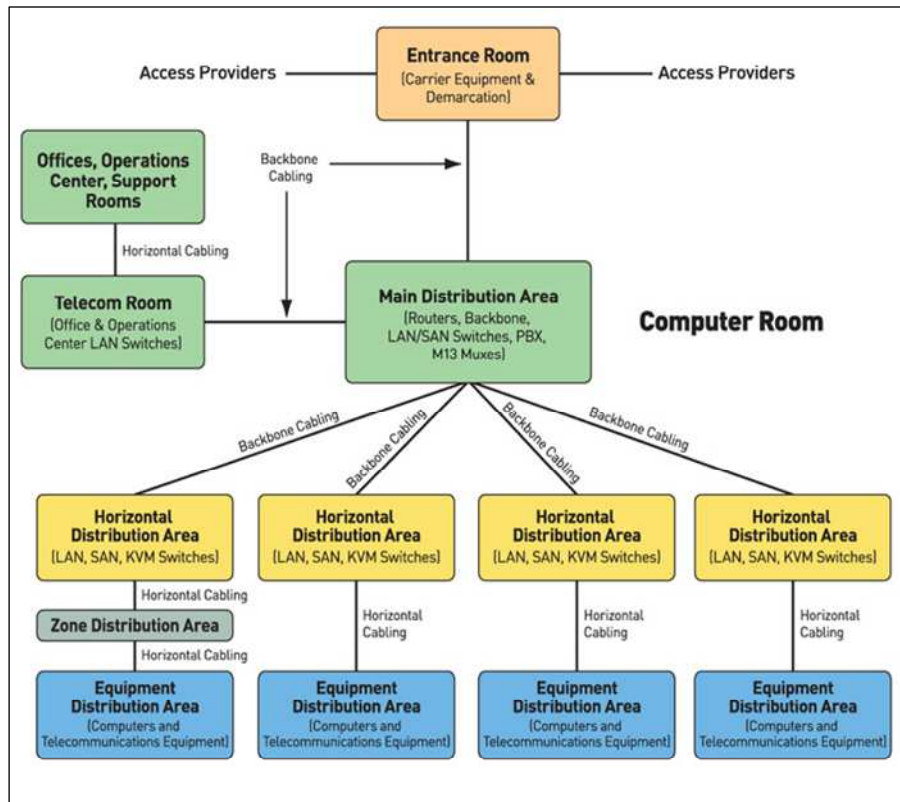
Toma de usuario o roseta: Dispositivo fijo de conexión, que sirve para interconectar la terminación del cable horizontal con el equipo del usuario (PC, terminal de datos, terminal telefónico, etc.).

Topología básica del Datacenter - componentes EIA/TIA-568-B

- Habitación de entrada, Analogía: "Instalación de entrada".
- El área de distribución principal (MDA), Analogía: "Habitación de equipo".
- El área de distribución horizontal (HDA), Analogía: "Habitación de telecomunicaciones".

- Dividir en zonas el área de distribución (ZDA), Analogía: "Punto de consolidación".
- El área de distribución de equipo (EDA), Analogía: "La área de trabajo".

Gráfico: Componentes de la topología.



CAPÍTULO 5 - Cooling

Enfriamiento (Cooling)

El enfriamiento o cooling es una parte muy importante hoy en día en un Datacenter, y el enfriamiento es un gran reto para los ingenieros que no sólo consiste en enfriar solamente, sino en retirar el aire caliente de las zonas de trabajo y evacuar la potencia disipada por los equipos, asegurando un flujo de aire que mantenga a los mismos dentro del rango de trabajo estipulado por el fabricante.

- Ley N° 1 de la termodinámica, la energía puede ser cambiada de una forma a otra pero ésta no puede ser creada o destruida.

Gráfica: Requerimiento del Datacenter EIA/TIA-942.

PARÁMETROS DE OPERACIÓN	
Temperatura	20 a 25 grados centígrados 68 a 70° F
Humedad	40 % a 55 %
Máximo punto de condensación	21 grados Centígrados 69.8° F
Máxima	5 grados por hora 41° F por hora

- Las mediciones se deben realizar cuando todo el equipamiento este en funcionamiento.
- Se realizan a 1.5 metros sobre el piso y cada 3 o 6 metros sobre la línea del pasillo frío o en cualquier punto de toma de aire.

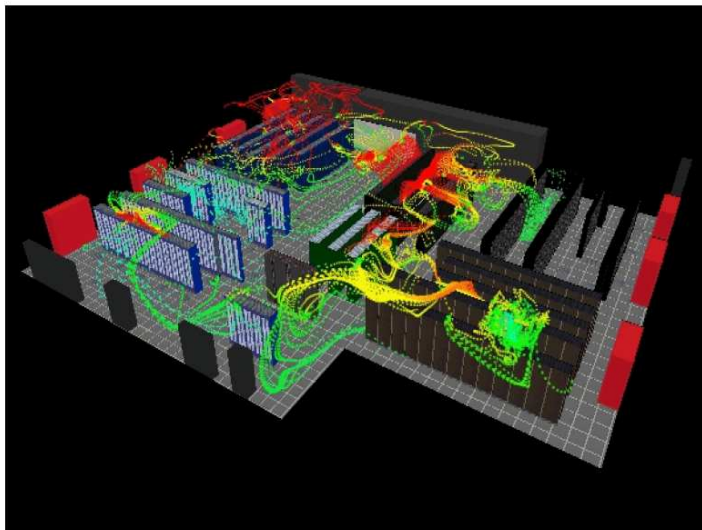
- Diferencial de presión positivo respecto a las áreas colindantes.
- Asegurar el sistema de enfriamiento de la sala.

Consideraciones

- Energía entrada = calor de salida.
- 1 Ton = 12,000 BTU⁸/Hr.
- 1 Ton = 3.5 Kw.
- 1 Kw. = 3413 BTU/Hr.
- El calor solo fluye en una dirección, de lo caliente a lo frío (concepto de gradiente).

Es importante definir el consumo de energía dentro del Datacenter para calcular la demanda de calor que se debe retirar del ambiente y la forma como se hará será la parte de la estrategia más importante del diseño.

Gráfica: Simulación del efecto de calor dentro de una sala de computo.



⁸ BTU La cantidad de calor requerido para elevar la temperatura de una libra de agua en un grado Fahrenheit.

El exceso de calor produce

- Acorta la vida útil de la electrónica, (esto es el core del negocio, en este caso puede llevar a la muerte ante de lo planeado al no alcanzar las rentas proyectadas).
- Reducción velocidad de procesamiento.
- Parada de aplicaciones.
- Averías prematuras.

Conociendo el circuito de refrigeración del servidor mejoramos la explotación de las salas **IT**.

Gráfico: Simulación de una corriente de aire caliente-frío de un conjunto de racks.

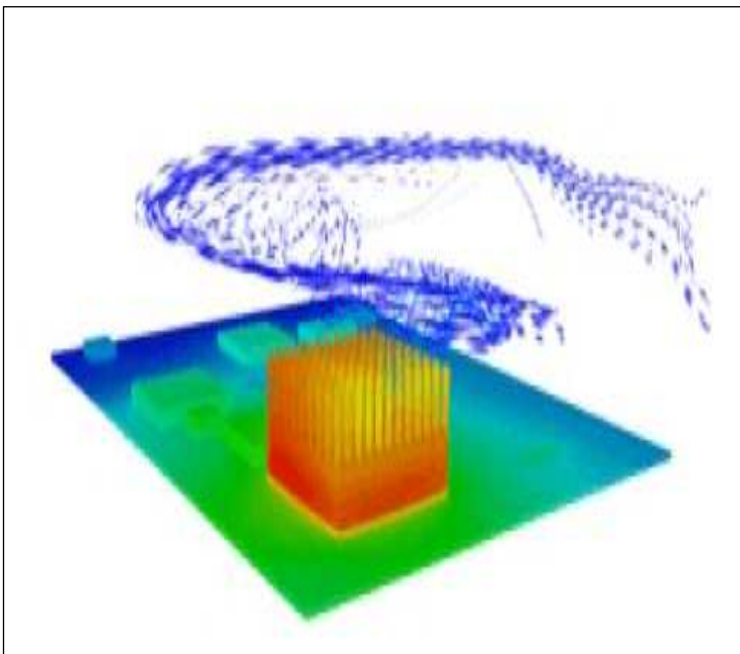
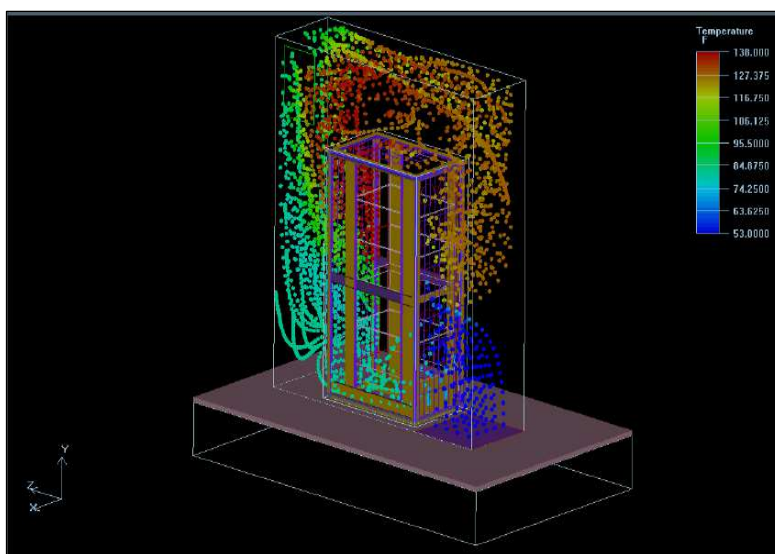
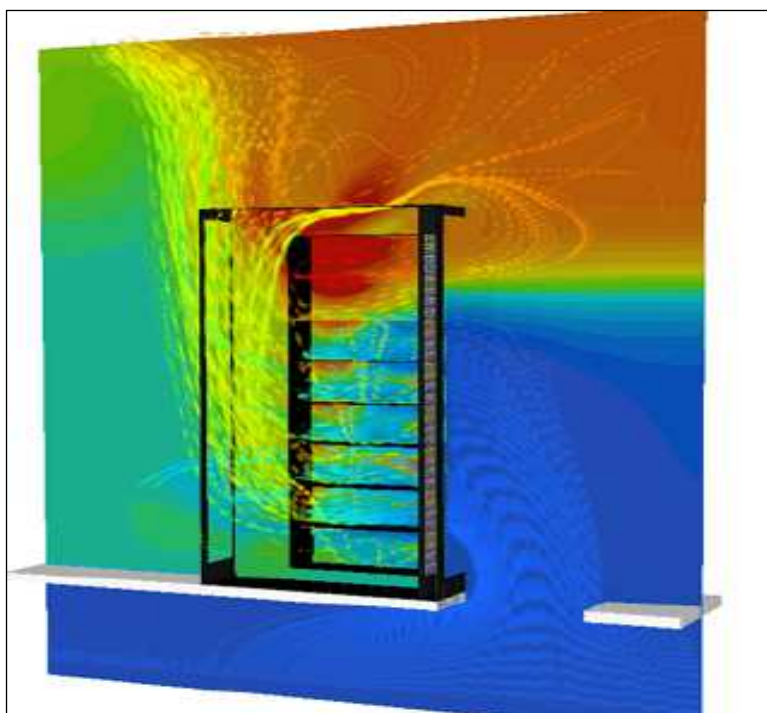


Gráfico: Simulación de una corriente de aire caliente-frío de un de rack en particular.



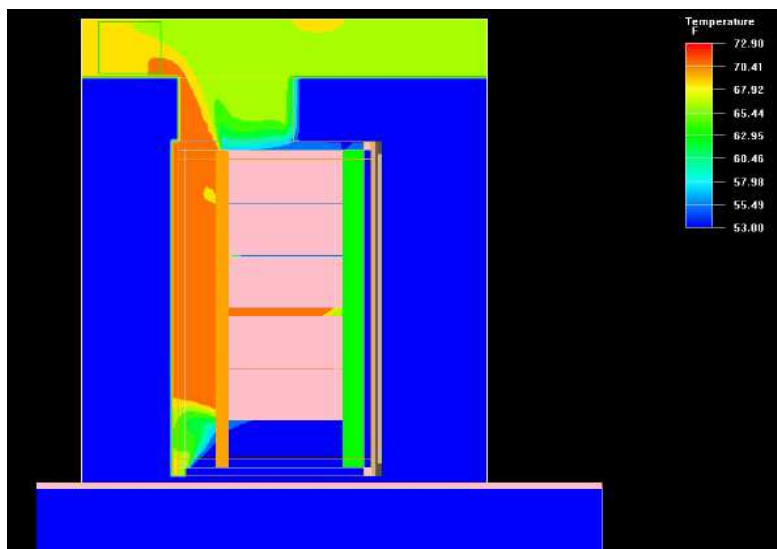


Gráfico: El armario o rack.



La ventilación

Para una ventilación adecuada se puede:

- Forzar el flujo de aire mediante ventiladores.
- Utilizar el flujo natural de aire en pasillos calientes y fríos mediante perforaciones en las puertas frontales y traseras.
- Combinación de ambos.

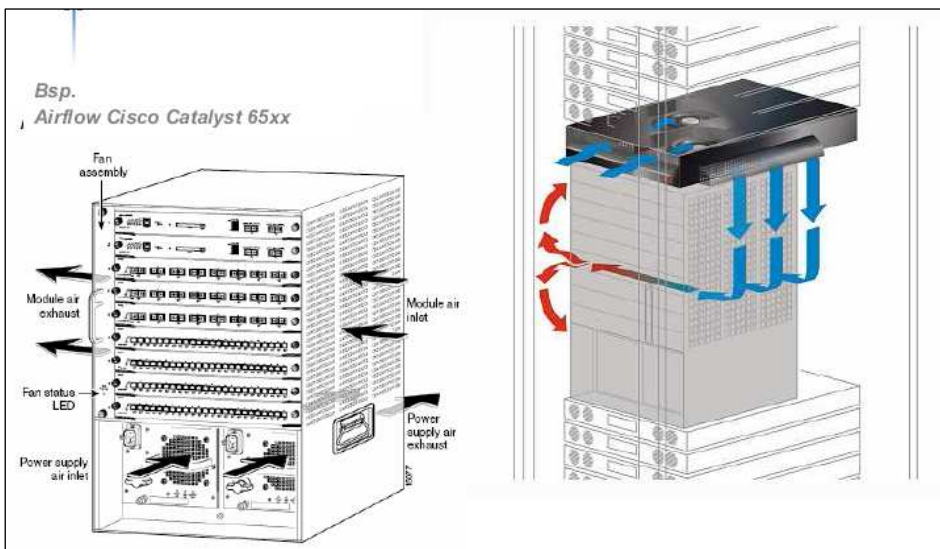
Para cargas moderadas de calor

- Perforaciones que provean un mínimo de 50 % de espacio abierto.
- Forzar el flujo de aire mediante ventiladores en combinación con perforaciones y espacio suficiente entre el equipo y las puertas, uso de deflectores en los racks, pero principalmente respetar las normas de instalación.

Para cargas altas de calor

- Sistemas de enfriamiento en combinación con perforaciones.
- Si se instalan ventiladores no deben contraponer el concepto de pasillos fríos y calientes.
- Para alta disponibilidad se requiere que los ventiladores estén en circuitos independientes de **PDUS** o **UPS**.

Gráfico: El flujo de aire en un rack.



Para racks con más de 2.5 Kw de potencia.

- Es vital extraer el aire caliente del interior del armario.
- En función de la temperatura, Montar ventiladores de velocidad regulada,.
- Evitar que el aire caliente se mezcle con la de sala.

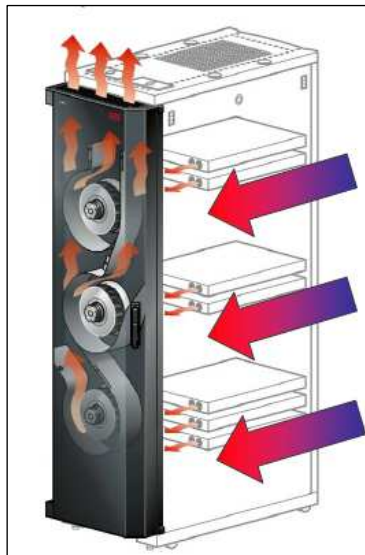
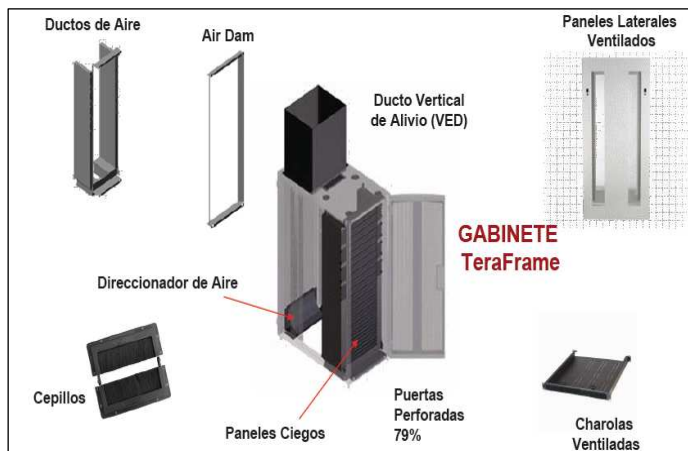


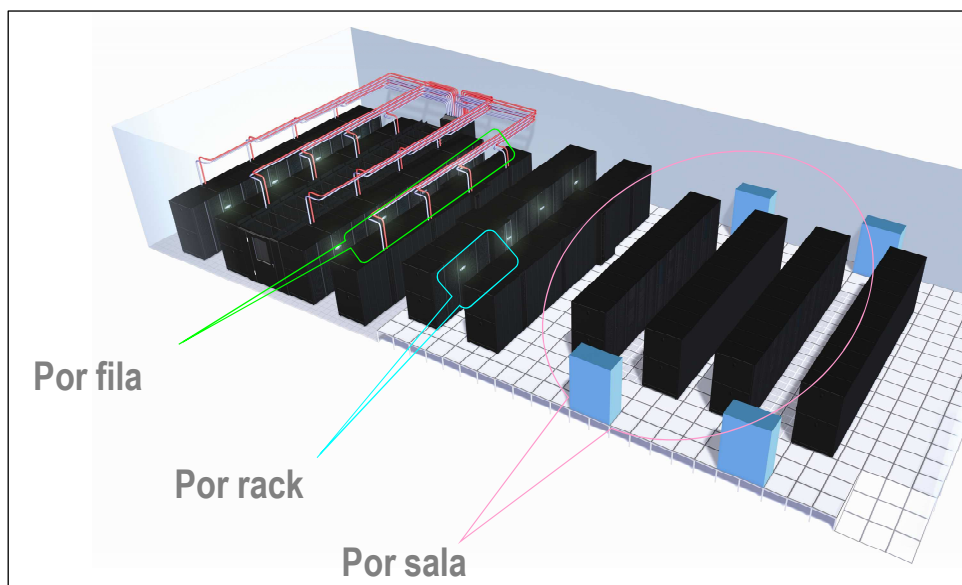
Gráfico: Enfriamiento dentro del rack.



Gráfica: Aire acondicionado INROW/RC.



Gráfica: Arquitecturas mezcladas de enfriamiento.

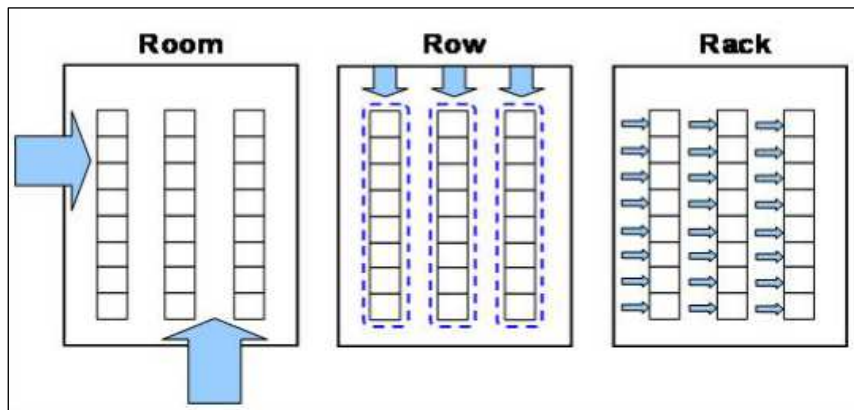


Arquitecturas de enfriamiento

Soluciones de enfriamiento para cada ambiente:

1. Rack: Enfriamiento dedicado y distribución de aire para gabinetes simples o puntos calientes.
2. Filas: Enfriamiento eficiente para cargas de **TI** en racks desde baja hasta alta densidad.
3. Salas: Enfriamiento flexible para cargas en racks - no racks con las más bajas densidades.

Gráfica: Esquema de enfriamiento.



Pasillos calientes, pasillos fríos

Gabinetes:

- Gabinetes frente a frente (pasillos fríos).
- Patrón alternado.

En la actualidad la mayoría de los equipos, tienen la toma como la expulsión de aire por el frente. El concepto es el ahorro de espacio al permitir construir filas de racks, espalda contra espalda, lo que obliga a los diseñadores de los

sistemas de refrigeración a plantearse soluciones innovadoras en este campo.

Cableado:

- Cables de distribución de energía en pasillos fríos.
- Cableado de telecomunicaciones en pasillos calientes.

Gráfico: Debemos separar pasillos calientes de los fríos.

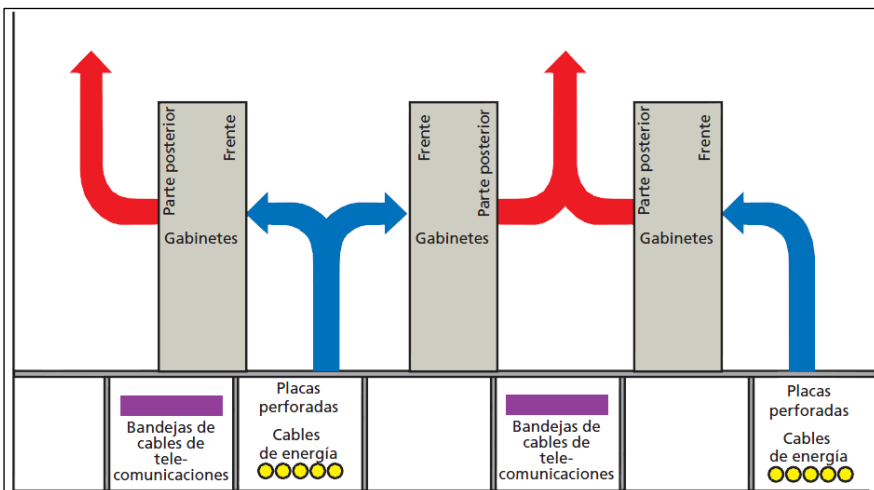
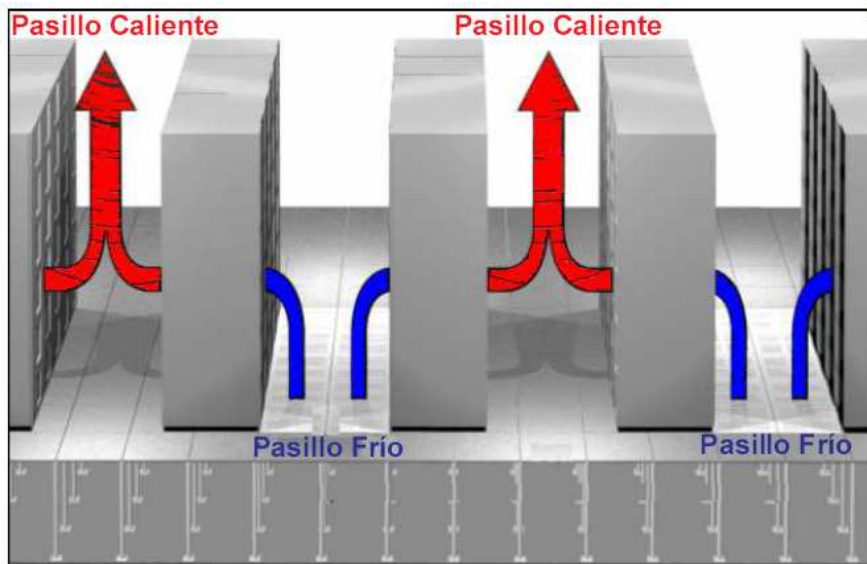


Gráfico: Enfriamiento (40-50 KW pasillo caliente central, tipo sala).

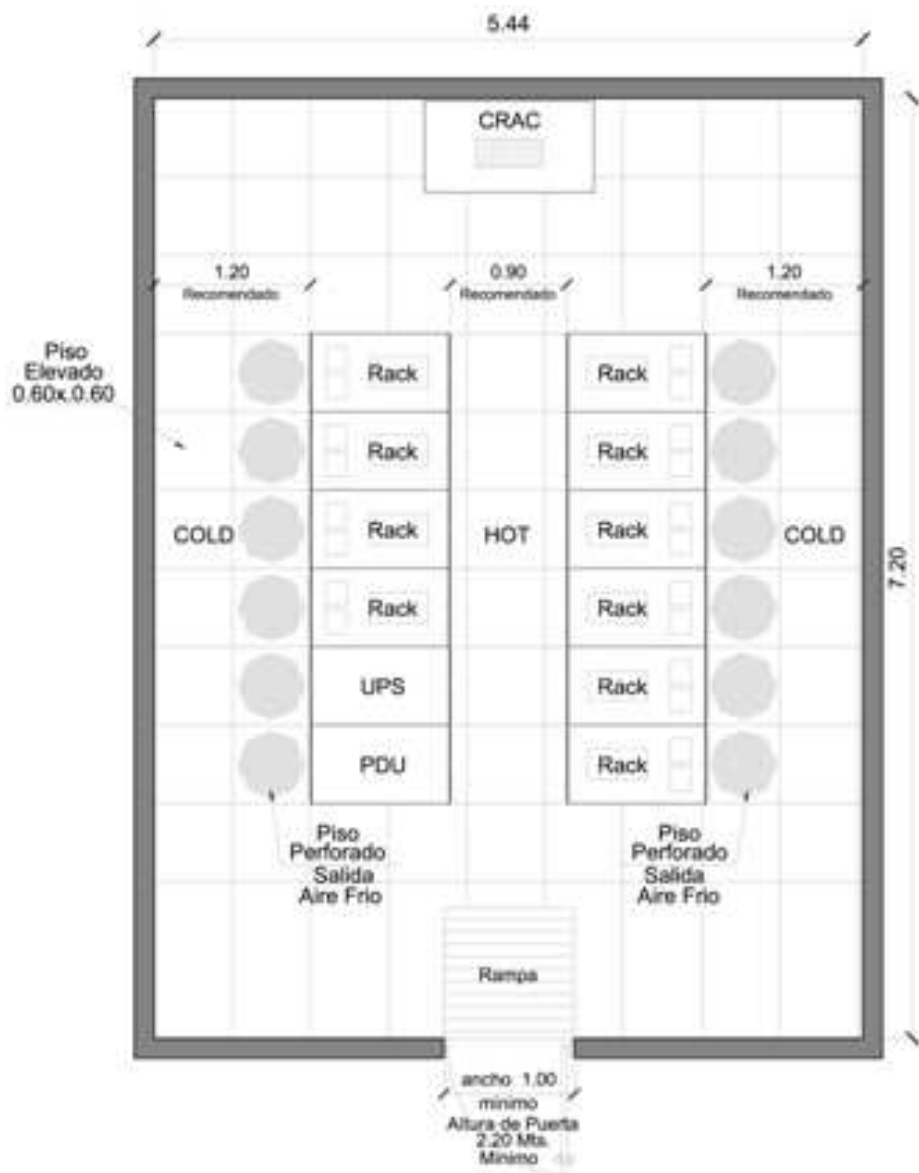


Gráfico: Enfriamiento (40-50 KW pasillo frío central, tipo sala).

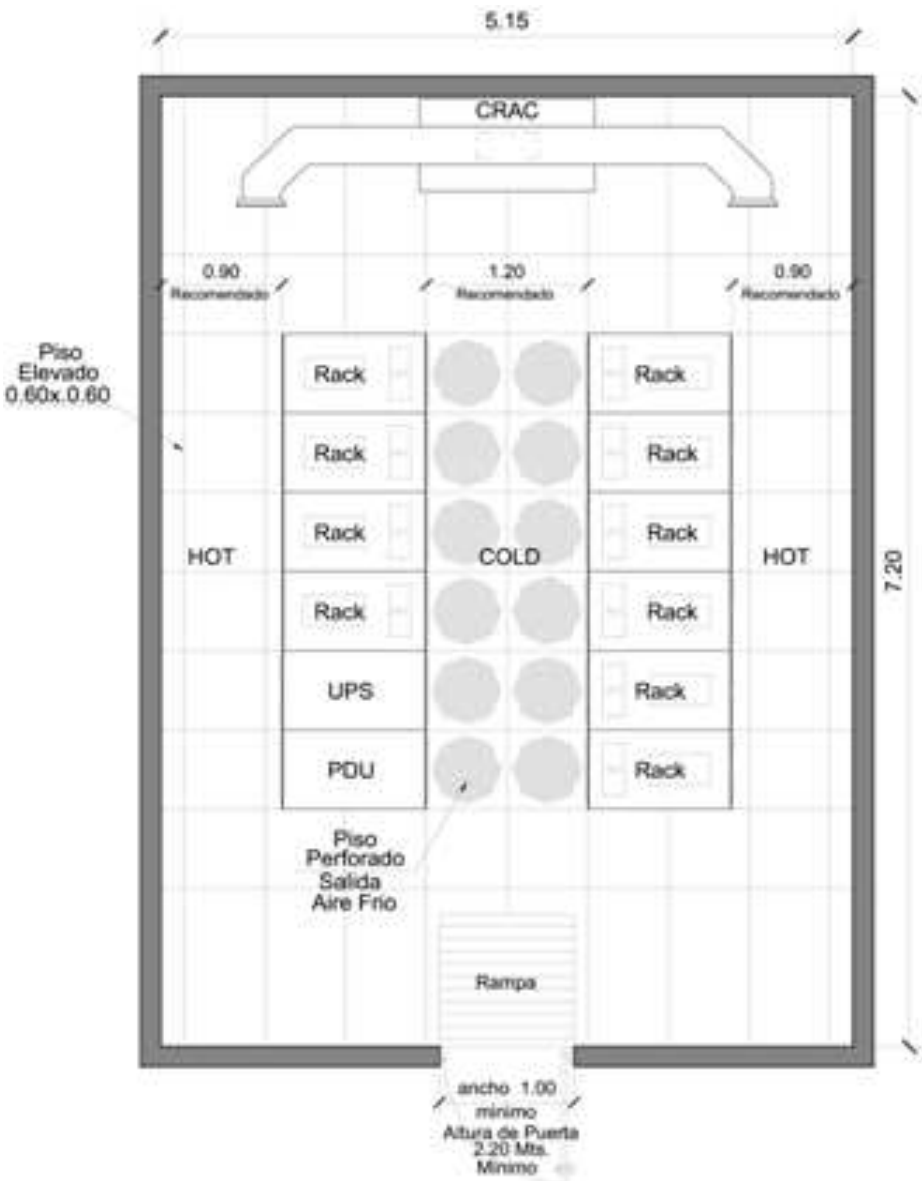


Gráfico: Enfriamiento por fila (in-row).

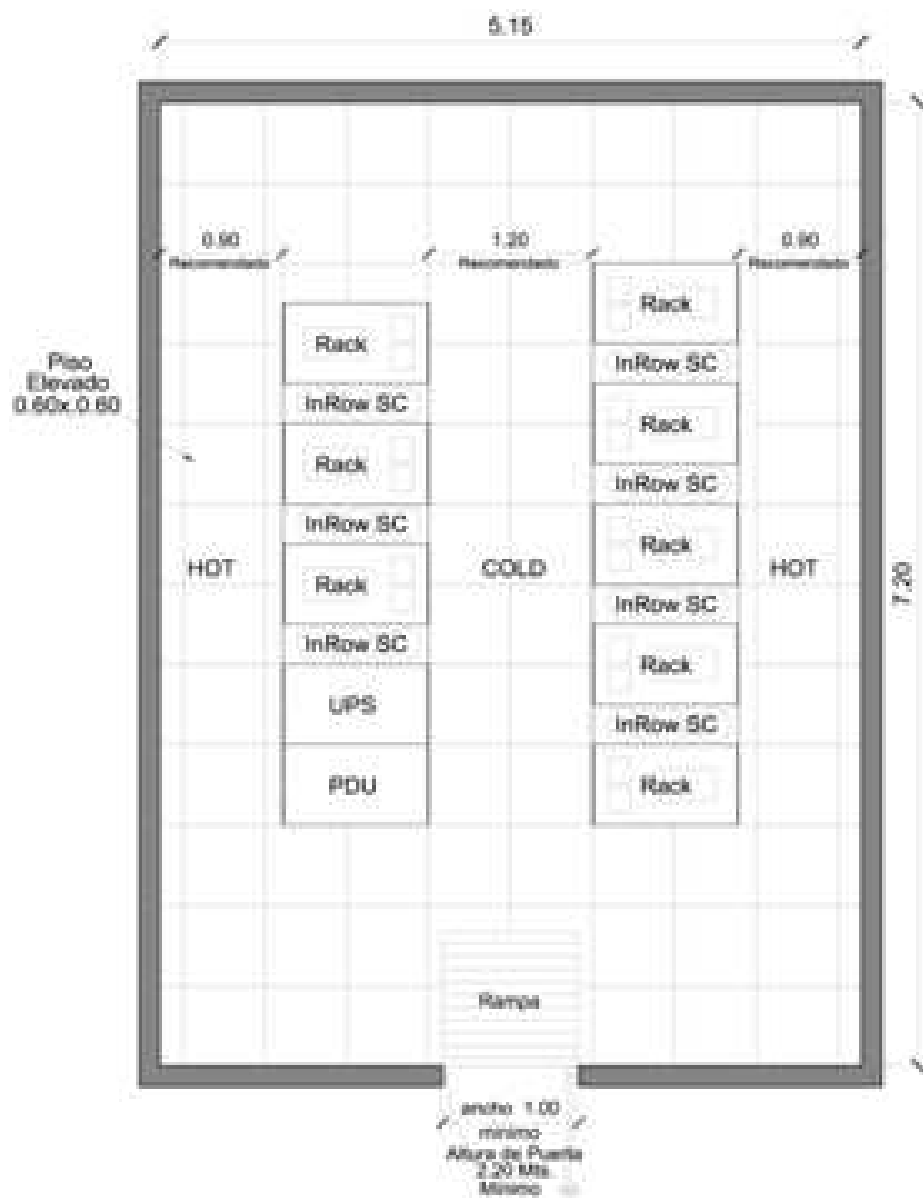
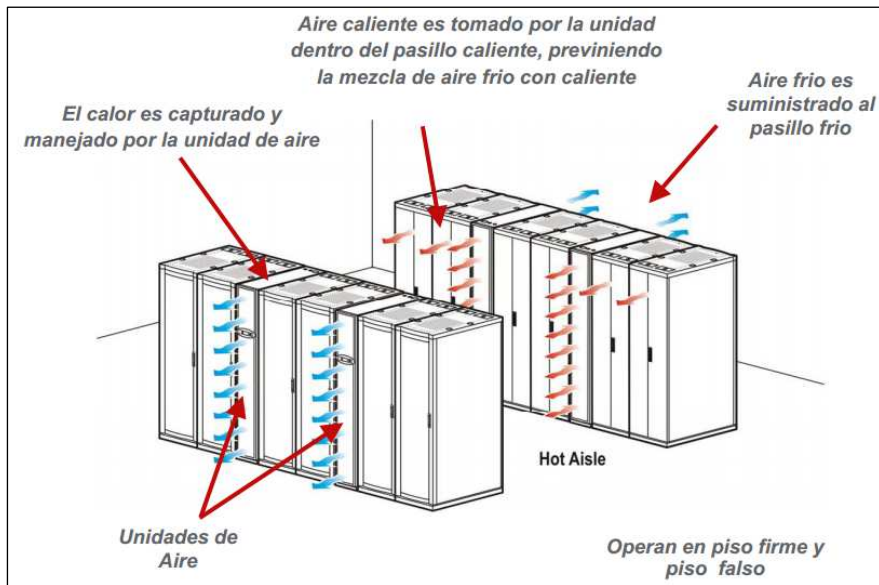
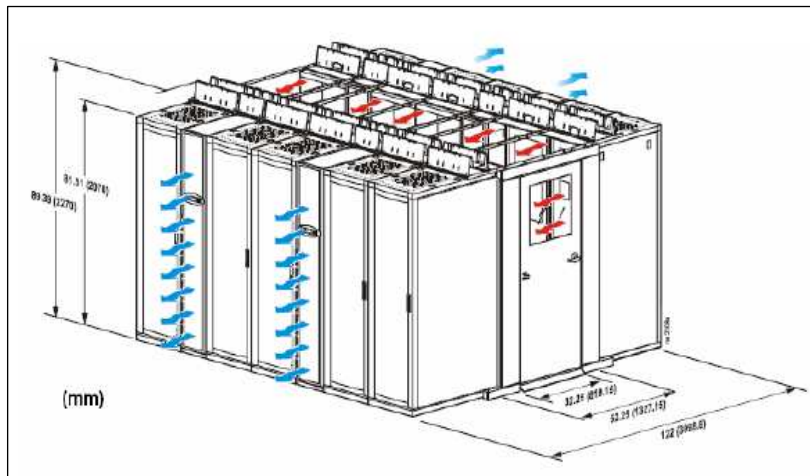


Gráfico: Detalle del aire acondicionado circulando por pasillos abiertos.



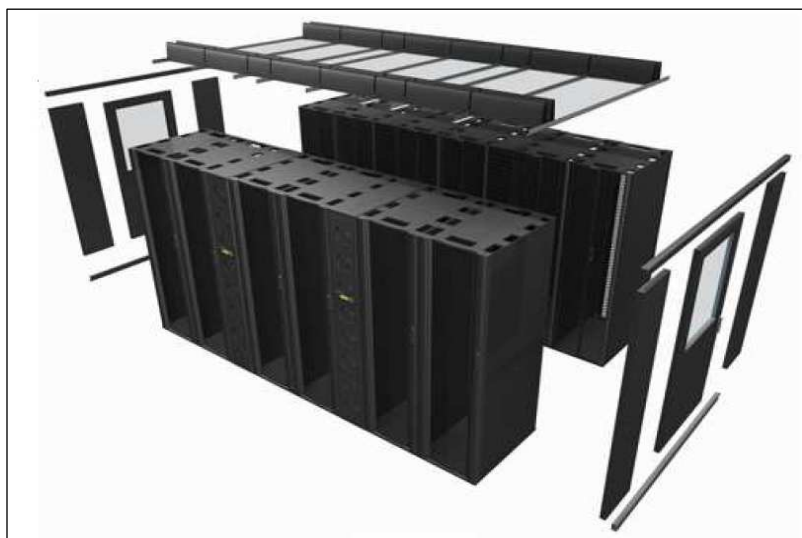
1. Refrigeradora hasta 17kw por unidad de aire.
2. Permite ampliaciones.
3. No necesita conductos de aire.
4. No se precisa de falso suelo.
5. Ahorro considerable de espacio.

Gráfico: Aire acondicionado en pasillos cerrados.



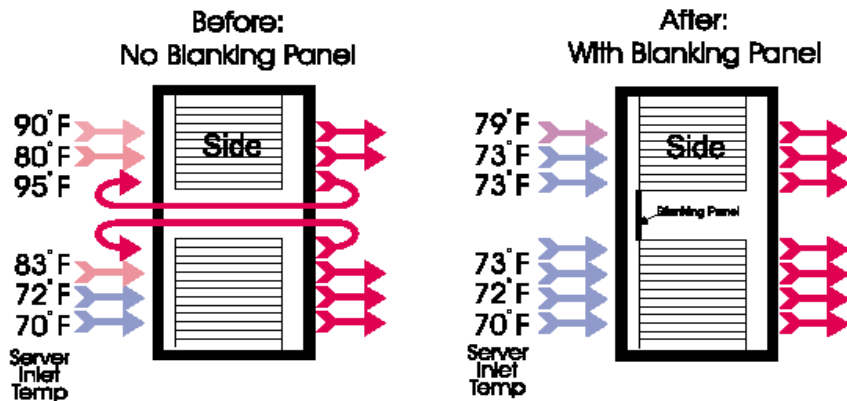
1. Refrigeradora hasta 30kw por unidad de aire.
2. Permite ampliaciones.
3. No necesita conductos de aire.
4. No se precisa de falso suelo.
5. Ahorro considerable de espacio.

Gráfico: Vista 3D de la sala de rack.



Factores que afectan la distribución del aire

La falta de aberturas o paneles de obturación alrededor de los lados de los rieles de los racks permite que el aire caliente extraído re circule hacia la parte delantera del rack. Gráficamente.



CAPÍTULO 6 - Adecuación Física

Piso Falso

La placa base de las áreas comprendidas para la instalación del piso falso (área de centro de cómputo) deberá ser preparada adecuadamente, con el fin de eliminar escombros, partículas, polvo e impurezas, entre otros. También se deberá dar un acabado final y aplicar pintura epóxica (tres (3) manos finales) sobre la placa para evitar el desprendimiento de partículas al área que contendrá el nuevo piso falso, e instalar un piso falso en toda el área del Datacenter, teniendo en cuenta las normas y recomendaciones que aplican para la implementación de centros de cómputo, tal como la norma ANSI/TIA-942, entre otras. Y por último, los paneles deberán estar fabricados en aluminio fundido o acero embutido en frío, de mínimo: 600 mm x 600 mm, con espesor de 6 mm, y vigas estructurales de 32 mm, en el contorno y en la parte inferior del panel.

Recubrimiento MICARTA

Cada panel debe estar cubierto por una lámina de MICARTA de 1/16" de espesor. La protección de la lámina MICARTA, deberá instalarse en el borde del panel una cinta plástica que cumple la doble función de embellecer el piso y sellar las salidas de aire. TOLERANCIA: + o - 1.3 mm. De este modo se garantizará que el piso no tenga partes metálicas expuestas, cumpliendo así con los estándares a nivel mundial.

Se deberá garantizar que la parte inferior o base, sea elaborada en tubo de acero de 1" de diámetro y de la longitud necesaria para conseguir la altura requerida del piso falso, e instalar Stringers (4 terminaciones entre cada pedestal galvanizado y cincado), que soporte una carga mínima de 200 kg con el fin que sirvan de ensamble a las cabezas de los pedestales, soporte de la estructura, y para mantener una continuidad eléctrica. Cuatro soportes se conectarán al sistema de malla de alta frecuencia, en cable, a fin de garantizar la descarga de electricidad estática.

Hay que garantizar que la cruceta posea guías para alinear y soportar perfectamente los paneles y con esta construcción producir la descarga electrostática del piso hacia el sistema de tierra, e igualmente que garantizar que los pedestales posean una capacidad de carga mínima de 5.000 Kg. y su altura no podrá ser inferior a 27cm.

Gráfica: Piso técnico.



Gráfica: Detalle del piso técnico.



Perforaciones del piso para la circulación del aire acondicionado

Se deberá garantizar que las perforaciones para el paso del aire acondicionado a través de los paneles del piso falso que así se requieran, sean realizadas directamente de fábrica, de acuerdo con los estándares internacionales para paneles perforados. Las perforaciones serán de 5/16" de diámetro y estarán uniformemente distribuidas en cada panel.

Techo Falso

Adecuar un techo falso es sin duda un tema a discutir. El mismo deberá contemplar todos los materiales requeridos para su instalación, deberá ser anti flama, el área del techo se pintara con pinturas según las normas vigentes, se debe demarcar las vigas con el fin de identificarlas para permitir la instalación de bandejas porta cables.

Gráfica: Techo falso.



Perforaciones para cables

Se deberá hacer perforaciones de 10 cm. x 15 cm. para el paso de cables, en los paneles que sea necesario. Estas perforaciones deberán tener en sus aristas protección de caucho de iguales características a las del piso, con el fin de evitar que los cables puedan ser cortados por los bordes de los paneles. Para el sello de la perforación se debe instalar un accesorio de escobillas, para evitar pérdidas de aire acondicionado.

Iluminación principal y de emergencia

El Datacenter deberá tener instaladas lámparas fluorescentes con rejilla, celdas semi-especular, celda parabólica, balasto electrónico, incrustadas en el cielorraso, garantizando como mínimo la luminosidad ideal y suficiente para todo el edificio, con un sistema de movimiento con sensor de multi-Tecnología infrarrojo y ultrasónico para la activación de las luces.

Además, instalar lámparas de emergencia, con respaldo de baterías de 90 minutos. La conexión de cada lámpara será por medio de toma eléctrica para facilitar el mantenimiento de la instalación. El cableado debe ser en circuitos trifilares con código de colores Amarillo – Fase, Blanco – Neutro y Verde – Tierra, calibre No.12 AWG.

Y también realizar la conexión de las lámparas de emergencia al sistema UPS, de tal manera que se activen cuando se interrumpa el suministro de energía eléctrica a través de una transferencia automática conectada al sistema de potencia ininterrumpida.

Red eléctrica regulada

Se requieren Tableros de Distribución de Potencia (**PDU**) para que soporten la red eléctrica regulada del centro de cómputo con el fin de establecer un sistema redundante. Garantizar el suministro e instalación de todos los materiales o equipos requeridos y efectuar las actividades necesarias que permitan el normal y efectivo funcionamiento de la solución a implementar, de conformidad con las normas técnicas establecidas para tal fin. Los Tableros de Distribución de Potencia (PDU), deberán tener alimentación de corriente eléctrica tanto del sistema UPS Central. De esta forma se garantiza el suministro eléctrico continuo al centro de cómputo, sin interrupción de los servicios informáticos.

Los Tableros de Distribución de Potencia (PDU) tienen que ser de lámina de acero cold rolled calibre 14, previamente tratada con químico limpiador y desoxidante, doble capa de pintura anticorrosivo y doble capa de pintura de aplicación electrostática horneable. Y contar con un analizador de redes digital con monitoreo remoto, de marca reconocida en el mercado, debe proveer al menos lecturas de voltajes y corrientes de línea y de fase, factor

de potencia, THD⁹ de voltaje y corriente, energía, potencia aparente, potencia activa, potencia reactiva. Adicionalmente permitir la comunicación de la información medida a través de un puerto de comunicaciones con protocolo reconocido.

Todas las perforaciones que tengan los tableros de Distribución de Potencia (PDU), tienen que estar debidamente protegidas y aisladas para evitar cortes en los cables. Los circuitos se deben entregar adecuadamente marcados con su respectivo número de circuito. Cada sistema (racks, servidores, comunicaciones, detección y extinción de incendios, seguridad y control de acceso, lámparas de emergencia y demás) deberá recibir la corriente regulada en forma independiente (UPS central actual y UPS a adquirir en este proceso), de manera que garantice la continuidad de los servicios en caso de contingencia.

Se suministrará, instalará y dejará en perfecto funcionamiento los elementos y equipos necesarios, que permitan que todas las conexiones eléctricas reguladas de los servidores y demás equipos instalados en cada rack queden debidamente conectados de manera redundante al sistema de corriente regulada, garantizando redundancia en la fuente. El sistema de detección y extinción de incendios deberá contar con el respectivo circuito dedicado de energía regulada.

El sistema de seguridad y control de acceso tiene que contar con el respectivo circuito dedicado de energía regulada. Es necesario contemplar en la solución a implementar una holgura o crecimiento del 50% de la capacidad instalada. Las tomas eléctricas a instalar deberán tener polo a tierra aislado. Y de igual manera garantizar una toma corriente doble para cada punto de voz y datos, y que la medición de voltaje para todas las tomas de corriente eléctrica regulada instalada, no supere los 0.5 voltios entre neutro y tierra.

⁹ % Distorsión Armónica

CAPÍTULO 7 - Políticas

Definición de la política general

Se entiende por política a las reglas generales de comportamiento definidas para la interacción entre los usuarios y los activos informáticos. Las políticas son independientes de los ambientes propios de la entidad y representan la base de un modelo de seguridad.

Política

La política se aplicará a todo el personal vinculado laboralmente con el Datacenter, contratistas y terceros que tengan acceso a los recursos de información de la organización.

Introducción

La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen al personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, o sea en general a los activos asociados al mantenimiento y procesamiento de la información. Como por ejemplo los activos de hardware y los activos de software.

Áreas de procesamiento de la información:

- Centros de procesamiento normales o de emergencia.
- Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación.
- Áreas donde se encuentren concentrados dispositivos de información.
- Áreas donde se almacenen y guarden elementos de respaldo datos (cd, discos duros, cintas, estaciones sun, etc.).

Definiciones

- **Activos de información:** Corresponde a elementos tales como bases de datos, Documentación, manuales de usuarios, planes de continuidad, etc.
- **Activos de software:** Son elementos tales como aplicaciones de software, herramientas de desarrollo y utilidades adicionales.
- **Activos físicos:** Se consideran activos físicos elementos tales como computadores, laptops, módems, impresoras, maquinas de fax, equipos de comunicaciones, Pbx, cintas, discos, UPS, muebles, etc.

Objetivo de la política

Prevenir el acceso físico no autorizado, además de evitar daños o robo a los activos de la organización e interrupciones a las actividades del negocio.

Un enunciado de la política es: "Toda área o equipo informático, debe cumplir con todas las políticas funcionales y procedimientos de seguridad física, con el fin de evitar el acceso a personas no autorizadas, daño e interferencia a los recursos e infraestructura de la información".

Elementos adicionales a la política general

Aspectos de la seguridad física a ser considerados en la definición de las políticas funcionales:

- Equipos de control del medio ambiente.
- Almacenamiento de cintas de respaldo.
- Seguridad de las oficinas, salones.
- Reglas sobre el trabajo en áreas seguras.
- Cableado, **UPS**, impresoras y módems.
- Seguridad de los equipos.

- Control de los sistemas de potencia.
- Múltiples sistemas de alimentación.
- Sistemas de control de potencia.

Políticas relacionadas

1. Política de control de acceso.
2. Política de continuidad del negocio.

Roles y responsabilidades

Los roles y responsabilidades de la administración general del Datacenter tienen que garantizar la continuidad del negocio en caso de un evento que afecte la operación normal de Datacenter.

Violaciones a las políticas de seguridad

Las violaciones a las políticas de seguridad física, pueden resultar en acciones de tipo disciplinario, que pueden incluir:

- Acciones de tipo disciplinario según los lineamientos establecidos por el código sustantivo del trabajo, el reglamento interno de trabajo, el código de comportamiento empresarial, las cláusulas especiales que se establezcan con los empleados en sus contratos laborales y/o todo aquello que según las leyes definan como acciones disciplinarias patronales.
- Reprimenda formal.
- Suspensión o acceso restringido a las áreas de procesamiento de la información.
- Reembolso por algún daño causado.
- Suspensión sin pago de salario.

- Terminación del contrato de trabajo o relación comercial (basados en las disposiciones emitidas por las leyes en materia laboral).
- Demanda civil o penal.

Revisión de la política

Esta política debe ser modificada si existieran cambios en la infraestructura física del Datacenter, y de no haberlos realizar su revisión anualmente.

Aspectos específicos sobre la política de seguridad física

Seguridad en el perímetro físico

El sitio escogido para colocar los sistemas de información, equipos de computo y comunicaciones, debe estar protegido por barreras y controles físicos, para evitar intrusión física, inundaciones, y otro tipo de amenazas que afecten su normal operación.

Recomendaciones y controles adicionales

El tamaño del área será determinado por la cantidad de hardware necesario para el procesamiento y almacenamiento de la información. Los requerimientos de tipo ambiental tienen que ser especificados por los diferentes fabricantes de los equipos. Las medidas de seguridad ha tomar dependerán directamente del valor de los activos de información, su nivel de confidencialidad, y los valores requeridos de disponibilidad. Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- El perímetro de seguridad debe ser claramente definido.
- El sitio donde es ubiquen los recursos informáticos debe ser físicamente sólido, y protegido de accesos no autorizados factores naturales, usando mecanismos de control, barreras físicas, alarmas, etc.

- Debe existir un área de recepción que solo permita la entrada de personal autorizado.
- Todas las salidas de emergencia en el perímetro de seguridad deben tener alarmas sonoras y cierre automático.

Control de acceso físico a áreas seguras

Todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas. Se recomienda además tener separados físicamente la operación de terceros con las propias, en caso de existir actividades de terceros en el Datacenter establecer controles por la persona responsable.

Como recomendaciones y controles Adicionales debido al posible robo, vandalismo y uso no autorizado de los sistemas de información, considerar restringir el acceso de personas a las áreas consideradas seguras, según lo definido.

Todo sistema de control de acceso tiene que considerar diferentes categorías de personal:

1. Operadores y usuarios que trabajan regularmente en las áreas seguras.
2. Personal de soporte que requiera acceso periódico.
3. Otros, que requieran acceder muy rara vez.

Aspectos de la seguridad de la información a ser considerados cuando se implementa la política de seguridad física son:

- Personal no autorizado puede llegar a tener acceso a las áreas restringidas, causando posibles fallas al sistema, por lo tanto visitantes o terceras personas que ingresen a un área definida como segura, deberán poseer una identificación a la vista que claramente

los identifique como tal y estas identificaciones serán intransferibles. Se debe además hacer una revisión periódica de identificadores de acceso, una formal realizada con auditoria, al menos una vez al año, y las diferentes divisiones internamente realizarlas cada tres meses. O no deberán existir señales, ni indicaciones de ningún tipo sobre la ubicación de los centros de procesamiento en la organización. O en caso de pérdidas de llaves, tiene que haber procedimientos que garanticen que las mismas no podrán ser utilizadas por extraños. Equipos como fax, fotocopadoras, impresoras deben estar en áreas definidas por el Datacenter como seguras, esto se aplica también para equipos de comunicaciones como switches, enrutadores, firewalls, ids, etc.

- Las puertas y ventanas deben estar cerradas, en caso de ser el primer piso se deben considerar controles adicionales.

Uso de maquinas fax/módems

La información sensitiva o confidencial solo puede ser enviada vía Fax o Módems cuando no existan otros medios que garanticen una mejor seguridad, ambos el dueño y el receptor deben autorizar la transmisión de antemano.

Esta política considera las amenazas asociadas con el uso de maquinas de fax. El riesgo proviene principalmente de la relativa inseguridad del medio, dado que la información confidencial puede ser revelada a personas no autorizadas.

Usos de impresoras

La información clasificada como altamente confidencial no debe ser nunca enviada a una impresora de la red, sin que exista una persona autorizada para cuidarla durante y después de la impresión.

La variedad de la información que se envía a las impresoras puede alternar entre información pública e información confidencial, dado que información confidencial puede ser revelada a personas no autorizadas.

Presencia de extraños en las instalaciones

Todos los empleados deben estar vigilantes ante la presencia de personas extrañas sin identificación visible dentro de las instalaciones del Datacenter y en ese caso reportar inmediatamente a seguridad. Entre los controles adicionales tenemos:

- Todos los visitantes o extraños deben ser acompañados durante su estadía en el Datacenter, debido a la existencia de información confidencial o hurto.
- Equipos como videograbadoras, cámaras fotográficas, no tienen que ser permitidos su uso dentro de las instalaciones del Datacenter, a menos que exista una autorización formal por el oficial de seguridad o personal de seguridad del Datacenter.

Áreas de carga y descarga

La carga y descarga de materiales en el Datacenter requerirá de un primer control (inspección rigurosa por seguridad) en recepción y, luego de su respectiva autorización para ingresar, se entregará en el sitio respectivo. También debe ser cuidadosamente controlado su ingreso, y aislado de los centros de procesamiento de información.

Los siguientes controles deben ser considerados:

- Todo elemento que ingrese al Datacenter debe ser inspeccionado por la compañía de seguridad rigurosamente con el fin de identificar material peligroso y que coincida con su respectiva autorización de ingreso.
- Las áreas de descarga deben estar debidamente identificadas para evitar el acceso a las instalaciones por parte de terceros.
- Los materiales que tengan que entrar al Datacenter deben ser inspeccionados debidamente en la zona de descarga, para evitar la entrada de elementos peligrosos a las áreas internas.
- El material entrante o saliente debe ser registrado, con el fin de mantener el listado de inventario actualizado.

Seguridad de los equipos

En lo referente a la ubicación de computadores y hardware en general, es necesario tener especial cuidado contra fallas del sistema de control del medio ambiente, y otras amenazas que puedan afectar el normal funcionamiento del sistema.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas:

- Fallas en el control de la temperatura o humedad pueden afectar la operación del negocio, así que, se debe tener un estricto monitoreo sobre estas variables.
- Se deben adoptar o mantener al día controles para minimizar el riesgo potencial de robo.
- Todos los visitantes o terceras personas que ingresen a las instalaciones del Datacenter deberán poseer una identificación a la vista que claramente los identifique como tal.
- En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses (¿cuánto tiempo se recomienda?) y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control del manual de seguridad física.
- Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipos eléctricos, papel o químicos especiales o explosivos.
- En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo contacto de incendio. O inundación o falta de suministro.
- Las salas de procesamiento de la información deberán estar ubicadas en pisos a una altura superior al nivel de la calle a fin de evitar inundaciones.

- Las cañerías de desagüe de dichas salas y ubicadas en el piso deberán poseer válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre-flujos o interferencia eléctrica y/o radiación electromagnética.
- El cableado de la red debe ser protegido de interferencias, por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimento.
- El uso de elementos adicionales de protección (contra polvo o radiación) para los equipos informáticos debe ser considerado en ambientes de tipo industrial.
- Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico. Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes de los equipos, entre los controles adicionales.
- El correcto uso del sistema **UPS** garantizará el suficiente tiempo para realizar las funciones de respaldo en servidores y aplicaciones.
- El sistema de generación debe ser regularmente probado de acuerdo a las recomendaciones del fabricante, o por lo menos una vez al año o tener interruptores eléctricos adicionales localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia. Las luces de emergencia deben funcionar en caso de fallas eléctricas.

Instalación y mantenimiento del cableado

El cableado de la red debe ser instalado y mantenido por ingenieros calificados con el fin de garantizar su integridad. Y conectores de pared no utilizados deben ser sellados y su estado formalmente notificado.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Un daño malicioso a la red puede causar un grave disturbio en los sistemas de procesamiento y comunicaciones.
- Una incursión ilegal puede comprometer la seguridad de los datos, usuarios y contraseñas.
- El cableado de la red debe ser protegido de interceptación o daño, por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de acuerdo a las normas técnicas de los de comunicaciones.
- Para el caso de conexiones muy críticas (transporte de mucha información o aplicaciones especiales) se debe considerar el uso de fibra óptica.
- Considerar el uso de enlaces redundantes.

Mantenimiento de los equipos

Los mantenimientos programados sobre los equipos deberán seguir las recomendaciones del fabricante y ser realizados únicamente por personal autorizado, considerando el hecho que si se tuviera que enviar fuera de las instalaciones, y tener en cuenta la información sensible y los requerimientos de las pólizas de aseguramiento.

Equipos fuera de las instalaciones

El uso de equipos de procesamiento de la información o software, fuera de las instalaciones del Datacenter, debe ser autorizado por el jefe o director del área donde el empleado dependa. Esto aplica para computadores personales, agendas electrónicas, teléfonos móviles, PDAs, etc.

Las siguientes recomendaciones deben ser consideradas:

- No dejar los equipos desatendidos en zonas públicas. Los computadores personales deben evitar su exposición y ser llevados como equipaje de mano.
- Las especificaciones del fabricante deben ser consideradas.
- El trabajo remoto debe estar sujeto a controles especiales, considerando las normas y políticas de seguridad vigentes.
- Se debe considerar el uso de seguros contra robo, pérdida etc.

Destrucción de equipos y re-uso

Los equipos de almacenamiento de información deben ser destruidos físicamente de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no quede información remanente, evitando además el uso de comandos de borrado usados en su operación normal.

Políticas de escritorios y pantallas limpias

El Datacenter tiene que adoptar una política de escritorios limpios para papeles, y medios de información, junto con una política de pantalla limpia, con el fin de reducir los riesgos por pérdida, daño a la información durante o fuera de las horas de trabajo.

Los siguientes controles deben ser considerados:

- Cuando sea apropiado, papeles y medios de información deben estar asegurados en armarios especiales, especialmente en horas fuera de las normales de trabajo.
- Información confidencial y crítica para la organización debe ser asegurada preferiblemente en armarios resistentes a: Golpes de impacto, fuego e inundación. Los computadores personales no se deben dejar dentro de la sesión, se recomienda el uso de llaves físicas, contraseñas, y otro tipo de controles cuando no estén en uso.
- Puntos de envío y recepción del correo, maquinas de fax, deben ser protegidos de acceso no autorizado.
- Las fotocopadoras deben estar protegidas de uso no autorizado.

CAPÍTULO 8 - SAN/NAS/DAS

Introducción al storage área network (SAN)

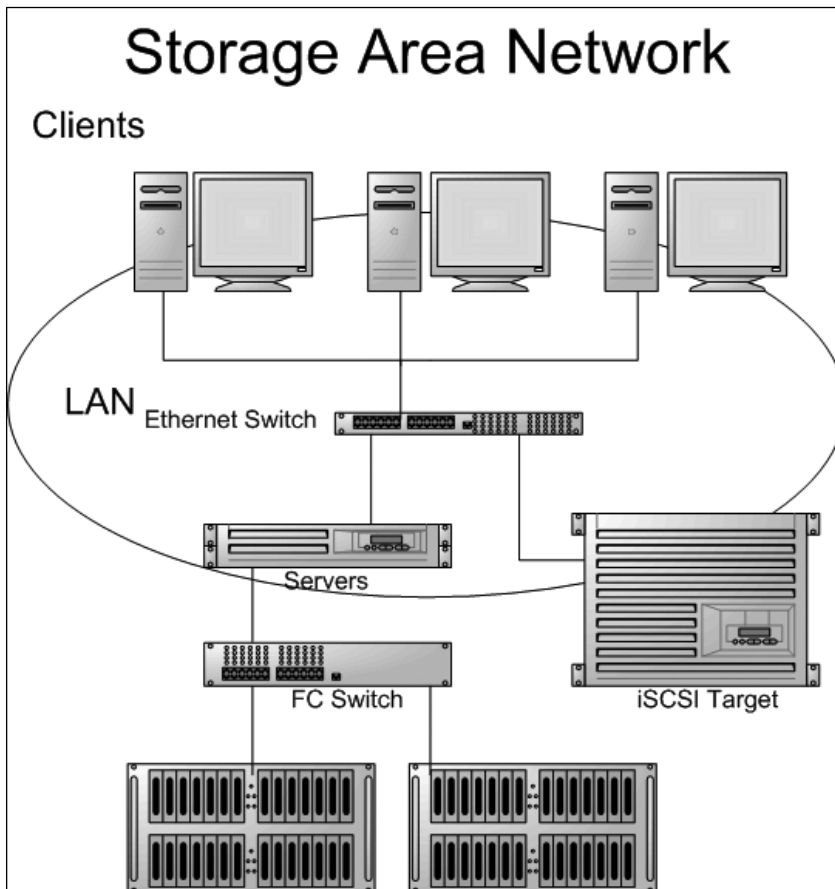
Una **SAN** (Storage Área Network) aplica un modelo de red a los ambientes de almacenamiento en los Datacenter. Las SANs operan detrás de los servidores para proveer una ruta común entre los servidores y los dispositivos de almacenamiento. A diferencia de las soluciones **DAS** (Directly Attached Storage) basadas en servidores y de los **NAS** (Network Attached Storage) orientadas a archivos, los SANs proveen un acceso a nivel de bloque o de archivo a los datos que son compartidos entre los recursos computacionales y personales. La tecnología SAN predominante se implementa en una configuración Fibre Channel (FC). A partir del crecimiento de los SANs y la denominación global del Protocolo Internet (**IP**), el almacenamiento por medio de redes IP para transportar tráfico de almacenamiento se encuentra al frente del desarrollo técnico. Las redes IP proveen niveles crecientes de manejabilidad, interoperabilidad y costo-beneficio. Se pueden observar beneficios inmediatos en la consolidación de almacenamiento, virtualización, espejos, respaldo, y administración, gracias a la convergencia del almacenamiento con las redes existentes IP (LANs/MANs/WANs),. La convergencia también provee incrementos en capacidad, flexibilidad, expansibilidad y escalabilidad.

Las dos principales normas que utilizan el protocolo **IP** son **FCIP** (Fibre Channel over IP), también conocido como iFCP en forma híbrida, e **iSCSI** (IP Small Computer System Interface). Ambas transportan comandos tanto Fibre Channel como SCSI incorporados dentro de un datagrama IP. Ambas fueron desarrolladas por la IETF (*Internet Engineering Task Force*). La diferencia entre las dos es que SCSI puede trabajar con los dispositivos existentes Ethernet, mientras que FCIP o iFCP, alternativamente definidos como Tunelaje Fibre Channel, pueden solamente trabajar con componentes Fibre Channel.

El Tunelaje es el encapsulamiento de comandos Fibre Channel dentro de un paquete IP para su transmisión en una red IP. Actualmente, 10Gigabit

ethernet está ganando rápidamente popularidad para los backbones de los centros de datos corporativos.

Gráfica: Topología SAN.



Evolución de las tecnologías de almacenamiento

Con el advenimiento de Internet, intranets corporativos, e-mail, e-commerce, business-to-business (B2B), ERP (Enterprise Resource Planning), Customer Resource Management (CRM), data warehousing, CAD/CAM, rich media streaming, convergencia voz/video/datos, y muchas otras aplicaciones de tiempo real, la demanda de mayor capacidad de almacenamiento en las empresas ha aumentado en enorme medida. Los datos por sí mismos son tan importantes para la operación exitosa de los negocios como su personal y sus sistemas. Y la necesidad de proteger este recurso estratégico ha

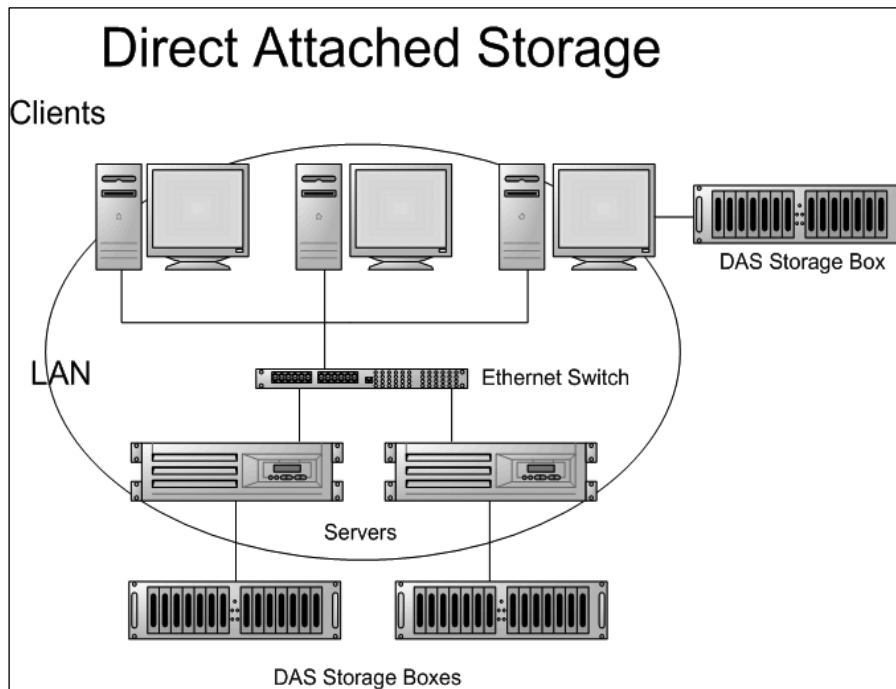
excedido enormemente las capacidades de una cinta de respaldo, no pudiendo satisfacer todas las necesidades requeridas. Además, el creciente almacenamiento de datos da como resultado la implementación de bibliotecas de cintas, e incluso con ellas existen problemas inherentes con las cintas que no pueden ser solucionados aumentando o reemplazando las capacidades de almacenamiento.

Las tecnologías de redes de almacenamiento se han desarrollado en las siguientes tres principales configuraciones:

- **Direct attached storage (DAS).**
- **Network attached storage (NAS).**
- **Storage área network (SAN).**

DAS es el método tradicional de anexar localmente dispositivos de almacenamiento a los servidores por medio de una ruta de comunicación directa entre el servidor y los dispositivos de almacenamiento. Tal como se muestra en la siguiente figura 1, la conectividad entre el servidor y los dispositivos de almacenamiento se encuentran en rutas dedicadas separadas de la conectividad a la red. El acceso se proporciona por medio de un controlador inteligente. El almacenamiento sólo puede ser accedido a través del servidor directamente conectado. Este método se desarrolló primordialmente para satisfacer demandas pequeñas en los puertos de unidades de los sistemas host de computadoras. Por lo que, cuando un servidor necesita más espacio de unidades, una unidad nueva de almacenamiento es anexada, permitiendo a un servidor ser espejo de otro. Esta funcionalidad también puede conseguirse por medio de servidores directamente anexados a las interfaces del servidor.

Figura 1:



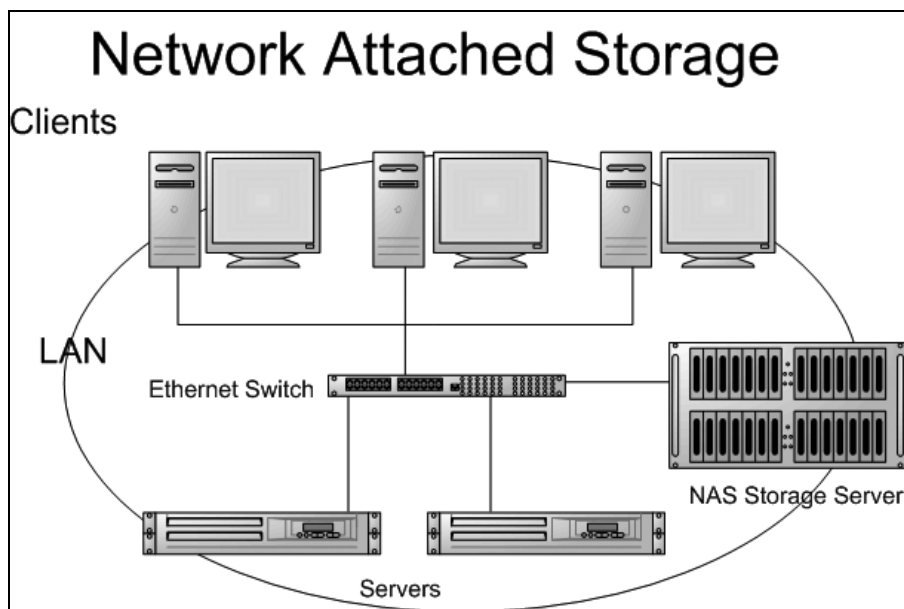
Nota: Las implementaciones 10G 6 se basan en una capacidad de canal teórica de cableado no blindado categoría 6/clase E. La transmisión de 10Gb/s sobre UTP se encuentra en evaluación por el grupo de estudio 10G-BASE-T y puede estar limitada en longitud y requerir alguna mitigación, dependiendo de las capacidades de los equipos electrónicos.

Network attached storage (NAS)

NAS es una arquitectura de almacenamiento con acceso a un nivel de archivo con elementos de almacenamiento conectados directamente a una LAN. Este provee acceso a archivos a un sistema de computadoras heterogéneo. A diferencia de otros sistemas de almacenamiento, a este se accede directamente por medio de la red (véase la Figura 2). Una capa adicional es agregada para cubrir los archivos almacenados compartidos. Este sistema generalmente utiliza **NFS** (Network File System) o **CIFS** (Common Internet File System) las cuales son aplicaciones IP. Una computadora separada usualmente actúa como "archivador", el cual es

básicamente un controlador de acceso de tráfico y seguridad para el almacenamiento. La ventaja de este método es que varios servidores pueden compartir almacenamiento en una unidad separada. A diferencia de **DAS**, cada servidor no necesita su propio almacenamiento separado lo cuál permite una utilización más eficiente de la capacidad de almacenamiento disponible. El servidor puede soportar diferentes plataformas siempre y cuando usen el protocolo **IP**.

Figura 2:



SAN a bajo nivel

Al igual que **DAS**, un **SAN** puede conectarse detrás de los servidores. Los SANs proveen un acceso a nivel de bloque para compartir almacenamiento de datos. Cuando se habla sobre acceso a nivel de bloque se refiere a los bloques específicos de datos en un dispositivo de almacenamiento, a diferencia del acceso a nivel de archivo el cual que refiere al acceso a nivel de archivo. Un archivo puede contener varios bloques.

Los SANs proveen alta disponibilidad y una continuidad de negocio robusta para ambientes de datos críticos, y generalmente poseen una arquitectura **Switched Fabric** que usa Fibre Channel (FC) como conectividad. Si damos

un vistazo a la Figura 3, el término *Switched Fabric* se refiere a cada unidad de almacenamiento conectado a cada servidor por medio de varios Switches lo cual provee redundancia dentro de las rutas a las unidades de almacenamiento. Esto provee rutas adicionales para comunicaciones y elimina al switch como punto único de falla. Ethernet posee muchas ventajas similares a Fibre Channel para el soporte de SANs. Y algunas de éstas incluyen alta velocidad, soporte a la topología *Switched Fabric*, interoperabilidad expandida, y un conjunto grande de herramientas de administración.

SAN sobre IP

IP fue desarrollado como un estándar abierto con interoperabilidad completa de componentes. Las dos nuevas tecnologías IP de redes de almacenamiento son FC sobre IP (FCIP o iFCP una forma híbrida) y SCSI sobre IP (**iSCSI**). FCIP soporta comunicaciones Fibre Channel a través de una red IP estándar por medio de Fibre Channel Tunneling o tunneling de almacenamiento y posee el beneficio de utilizar almacenamiento en ubicaciones que pueden exceder los límites de la conexión directa hasta casi 10 Km. Si se utiliza fibra como medio de transporte, dentro del Datacenter, Fibre Channel tradicional puede correr sobre cable coaxial o par trenzado, pero a distancias significativamente más cortas. IFCP la forma híbrida transporta comandos iSCSI sobre Fibre Channel.

Mientras que iSCSI mapea los comandos SCSI, datos y estado sobre redes Ethernet. Esta última tiene la ventaja de operar sobre redes dispersas geográficamente sin que requieran estar conectadas al tejido Fibre Channel ya que se utiliza la conectividad Ethernet existente. La incorporación del estándar IP dentro de estos sistemas de almacenamiento ofrece beneficios en el desempeño a través de la velocidad, como ser mayor disponibilidad, tolerancia de fallas y escalabilidad. Estas soluciones implementadas apropiadamente, pueden casi garantizar un 100% de disponibilidad de datos. Los protocolos de administración basados en IP proveen también a los administradores de redes de un conjunto de herramientas, avisos y disparadores que eran propietarios en previas generaciones de tecnología de almacenamiento. Se ven también enormemente mejoradas las soluciones de

encriptación y seguridad. Con **10G** ganando popularidad y la disponibilidad de nuevos enlaces WAN más rápidos, estas soluciones pueden ofrecer almacenamiento real *Bajo Demanda*.

- **Fibre Channel Sobre IP (FCIP).**
- **Fibre Channel (FC) Tradicional.**

FC tradicional es una tecnología de interconexión SAN basada en normas dentro y entre los Datacenter limitados geográficamente. Es una interfaz serial abierta de alta velocidad para interconectar servidores a dispositivos de almacenamiento (discos, “bibliotecas” de cintas o CD jukeboxes) o a otros servidores. FC tiene grandes capacidades de direccionamiento. De manera similar a SCSI, cada dispositivo recibe un número en el canal. Actualmente, ésta es la interfaz de redes de almacenamiento dominante. Fibre Channel puede estar totalmente interconectado proporcionando una excelente redundancia.

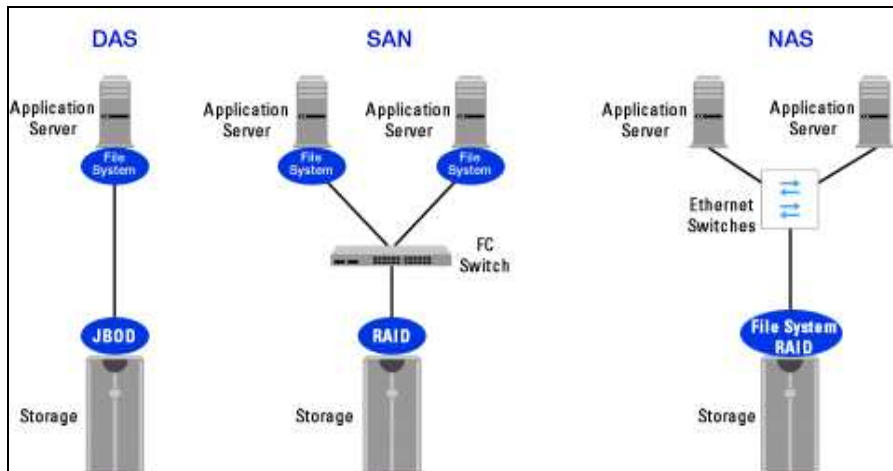
FC puede operar en las siguientes velocidades: 133Mb/s, 266Mb/s, 530Mb/s, 1Gb/s, 2GB/s, con 1Gb/s y 2Gb/s como las elecciones predominantes. Las distancias de transmisión varían con la velocidad y el medio. Nuevos Switches 10G Fibre Channel están siendo actualmente vendidos. Acorde a la norma *IEEE 802.3ae*, cuando se usan cables de fibra óptica monomodo, la distancia soportada es 10 kilómetros, y hasta 300 m cuando se utiliza la nueva fibra multimodo de 50 micras. La fibra optimizada para láser es una consideración importante en la selección de fibra para transmisiones 10Gb/s.

Topología FCIP

Con el fin de superar los límites de distancia de FC tradicional, el protocolo de tunneling de Fibre Channel sobre IP (FCIP) fue desarrollado. FCIP soporta comunicaciones FC a través de una red estándar IP, permitiendo la interconexión de SANs FC, los cuales pueden estar dispersos en toda la empresa, sin importar su geografía. Para la replicación entre los sistemas de almacenamiento sobre una WAN, FCIP provee un mecanismo para interconectar islas de SANs FC sobre la infraestructura IP (LANs/MANs/WANs) para formar un simple Red SAN FC unificado. A

continuación, en la Figura 3, se muestra una configuración básica de Fibre Channel IP.

Figura 3:



Elementos y componentes típicos de una red de almacenamiento

El hardware Fibre Channel interconecta los dispositivos de almacenamiento con los servidores y forma el Fibre Channel Red a través de las siguientes conexiones:

- Dispositivos interconectados: switches directores.
- Dispositivos traductores: adaptadores host bus (hbas instalados en el servidor), adaptadores, puentes, enrutadores, y gateways.
- Dispositivos de almacenamiento: disk arrays no raid o raid (redundant array of independent disks), bibliotecas de cintas.
- Servidores: el servidor es el iniciador en un san fibre channel y provee la interfaz a la red ip.
- Medios de capa física: cables coaxiales, de par trenzado y/o de fibra óptica.

Los Switches SAN FC se clasifican dentro del tejido ya sea como switches o directores. Una red switch contiene una cantidad de puertos, mientras que un

director es un switch con un conteo de puertos elevados (generalmente superior a los 64 puertos). Switches Fibre Channel pueden estar enlazados en red para formar redes de almacenamiento mayores. Un HBA es más complejo que una tarjeta tradicional Ethernet. Ésta conecta la red Fibre Channel a la red IP. Se puede usar un puente para conectar SCSI tradicional o dispositivos de almacenamiento ESCON (Enterprise System Connection) a la red Fibre Channel. Al combinar las ventajas de SCSI y de la tecnología de redes, iFCP, el sucesor híbrido de FCIP, permite a los dispositivos FC comunicarse en la red por medio de comandos iSCSI y Switches tradicionales Ethernet.

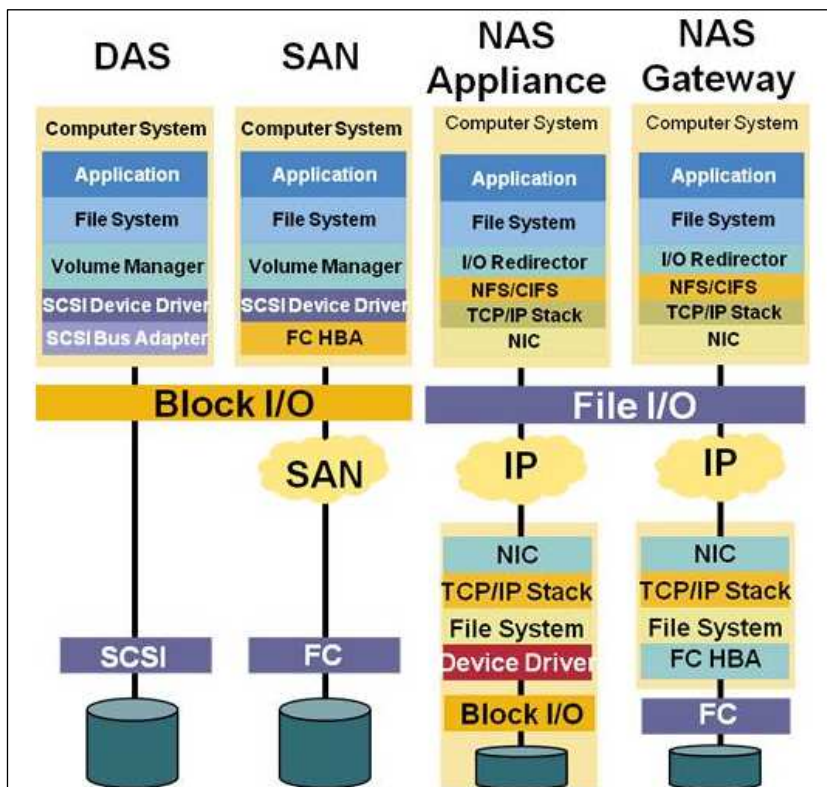
- **Small Computer Systems Interface (SCSI) sobre IP (iSCSI).**

El protocolo iSCSI, el almacenamiento y las redes IP: iSCSI usa dispositivos Ethernet existentes y el protocolo IP para transportar y manejar datos almacenados en un SAN SCSI. Esto nos da una solución de almacenamiento simple, de alta velocidad, bajo costo y larga distancia. Un problema de los dispositivos SCSI conectados directamente era el límite de distancia, y al usar componentes de redes existentes y explotar ventajas de las redes IP tales como administración de red y otras herramientas para LANs, MANs y WANs, iSCSI se está expandiendo en el mercado de almacenamiento y extendiendo la conectividad SAN sin límites de distancia.

Generalmente, para implementar una red de almacenamiento iSCSI en un Datacenter, la conectividad se proporciona por medio de un iSCSI Host Bus Adapters (**HBAs**) o NIC de almacenamiento que conecta los recursos de almacenamiento al Ethernet existente por medio de Switches IP Ethernet o Switches IP de almacenamiento y routers. Los routers y Switches IP especificados para almacenamiento tienen una combinación de interfaces iSCSI y otras interfaces de almacenamiento tales como SCSI o Fibre Channel, estos proporcionan conectividad multi-protocolo no disponible en Switches convencionales IP y Ethernet. Al conectarse a SANs FC, se necesita un Switch o router IP de almacenamiento para convertir el protocolo FC a iSCSI. Los routers and Switches IP de almacenamiento extienden el alcance del SAN FC y unen los SANs FC a los SANs iSCSI. Por ejemplo, un switch de almacenamiento IP permite a los usuarios realizar FC-to-FC

Switching, FC-to-iSCSI Switching, o FC-to- Ethernet Switching además de Ethernet-to-Ethernet Switching.

Gráfica: Arquitecturas DAS, NAS y SAN.



Redes de almacenamiento de arquitecturas mezcladas

La flexibilidad y el bajo costo son los factores conductores más importantes para la implementación de un modelo iSCSI especialmente para almacenamiento a larga distancia. Además, ya que las velocidades Ethernet se están continuamente incrementando, se cree que 10 Giga bit Ethernet based iSCSI será ampliamente utilizado para SANs en los actuales Datacenter. Se han desarrollado un gran número de dispositivos e incluso iFCP para soportar la gran base instalada de soluciones tradicionales de almacenamiento FC. Con el fin de proteger la actual inversión de las organizaciones en tecnología de almacenamiento, las instalaciones SAN

probablemente evolucionarán de ser una simple red de almacenamiento específico a ser una mezcla de productos Fibre Channel y SCSI.

Además, se espera una convergencia o integración de NAS y SANs así como también se espera que surjan Switches Fibre Channel y Ethernet multilingües (combinación). La red integrada SAN y NAS será escalable, al igual que soportará múltiples protocolos e interfaces. Esta integración permitirá a los usuarios optimizar sus SANs Fibre Channel tradicionales al proporcionarle conexiones confiables en largas distancias usando electrónicos existentes, por medio de la convergencia entre protocolos Fibre Channel e iSCSI.

Evolución de las normas para (SAN)

Las normas FC se desarrollaron por los subcomités técnicos **NCITS:T11** del **NCITS** (*National Committee for Information Technology Standards*). Las normas originales FC fueron aprobadas por ANSI X.3230 en 1994. La primera norma SCSI fue ratificada por ANSI en 1986. Desde entonces, ha habido varias enmiendas que reflejan los cambios en la industria.

El IETF (*Internet Engineering Task Force*) se está expandiendo en estas normas a través de mejoras en el protocolo IP para la interfaz existente y las anteriores normas operacionales. En Febrero del 2003, la especificación iSCSI fue oficialmente aprobada como "norma propuesta" por IETF. Adicionalmente, la SNIA (*Storage Networking Industry Association*), la FCIA (*Fibre Channel Industry Association*), y otros grupos de la industria se encuentran trabajando en la implementación y desarrollo de las normas SAN. El Datacenter es el núcleo de la infraestructura crítica de una organización. Además de los componentes SANs, NASs, un Datacenter típico incluye una gran variedad de componentes y conectividad. Para satisfacer la evolución de los Centros de Datos, el grupo TIA TR-42.1.1 está trabajando en la norma "Telecommunications Infrastructure Standard for Data Centers" a ser publicada como ANSI/TIA/EIA-942. Esta norma cubrirá el diseño de sistemas de cableado, canalizaciones y espacios.

Las consideraciones de cableado y los factores de diseño para SANs son prevalecientes en los Datacenter, pero también incluyen video, voz, y otras

aplicaciones convergentes. Una cimentación de red robusta es esencial. En un ambiente de Datacenter los requisitos básicos para el sistema de cableado son:

- Sistemas abiertos basados en normas.
- Alto desempeño, alto ancho de banda y calidad.
- Soporte para 10Gb Ethernet.
- Soporte para varios tipos de arquitecturas de almacenamiento y protocolos.
- Soporte para demandas de ancho de banda acumulativas para aplicaciones convergentes.
- Alta confiabilidad.
- Alta Redundancia.

Para cumplir con todos estos requisitos, la primera elección es 10Gb Ethernet. Esta es una infraestructura robusta para las comunicaciones empresariales en un Datacenter y está totalmente alineado con el draft TIA de la norma de Datacenter. Con el fin de mejorar la confiabilidad de la infraestructura de comunicaciones, la redundancia es la consideración principal de diseño en un Datacenter. Esta redundancia puede obtenerse al proveer servicios físicamente separados, áreas y canalizaciones cross-conectadas, o por medio de dispositivos electrónicos redundantes en topologías de red.

Conclusión:

Las redes de áreas de almacenamiento son tan solo un componente de las aplicaciones convergentes que utilizan las redes actuales. Los beneficios de estos sistemas no sólo son numerosos, sino completamente esenciales para un negocio, al proporcionar el ancho de banda necesario para todas los servicios que brinda el Datacenter.

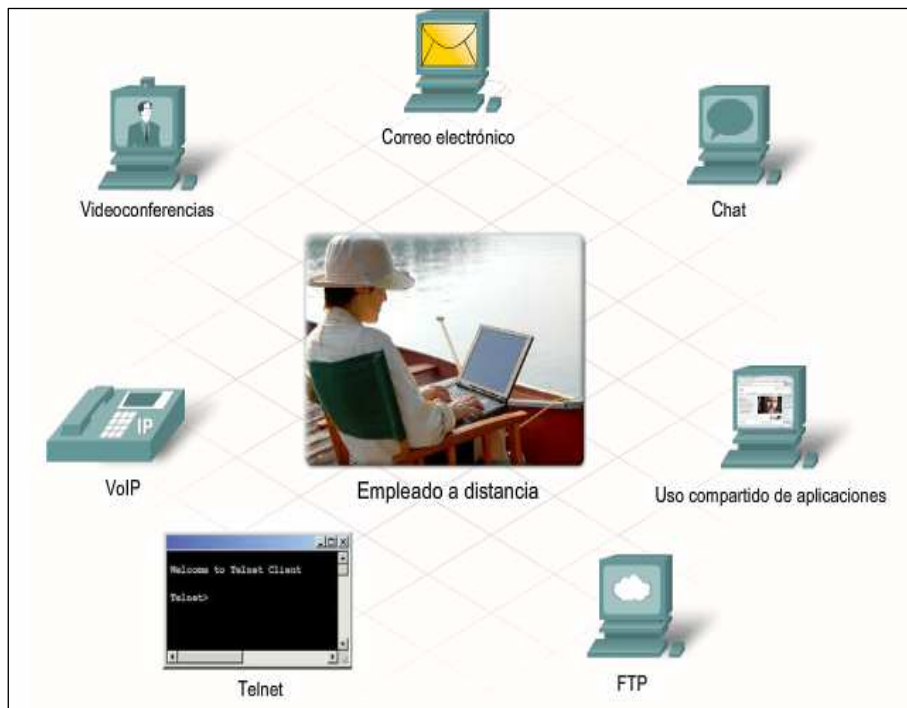
CAPÍTULO 9 - Servicios

Servicios que un brinda Datacenter

Introducción:

- Soporte de aplicaciones críticas.
- Soporte de base de datos.
- Necesidad de control centralizado.
- Soporte de diversos requisitos comerciales.
- Soportes a otros Datacenter.

Gráfica: Aplicaciones que brinda un Datacenter.



Un Datacenter debe admitir el intercambio de diversos tipos de tráfico de red, entre ellos archivos de datos, correo electrónico, telefonía IP y aplicaciones de video entre otras. Para optimizar el ancho de banda de un Datacenter, éste debe estar organizado de manera que el tráfico permanezca localizado y

no se propague a partes innecesarias de la red. El uso del modelo de diseño jerárquico de tres capas ayuda a organizar la red. Este modelo jerárquico es aplicable según las necesidades de nuestro diseño del Datacenter, el mismo sirve como base para nuestra futura implementación.

Este modelo divide las funcionalidades de la red en tres capas definidas:

- Capa de núcleo.
- Capa de distribución.
- Capa de acceso.

Cada capa está diseñada para cumplir funciones específicas.

- La capa de acceso proporciona conectividad a los usuarios.
- La capa de distribución se utiliza para enviar el tráfico de una red local a otra.
- La capa núcleo representa una capa Backbone de alta velocidad entre redes finales dispersas.

Descripción de capas

La capa de núcleo

- Proporciona una capa de Backbone de alta velocidad con conexiones redundantes (de respaldo).
- Transporta grandes cantidades de datos entre múltiples redes finales.
- Incluye switches y routers muy eficaces de alta velocidad.

La capa de distribución

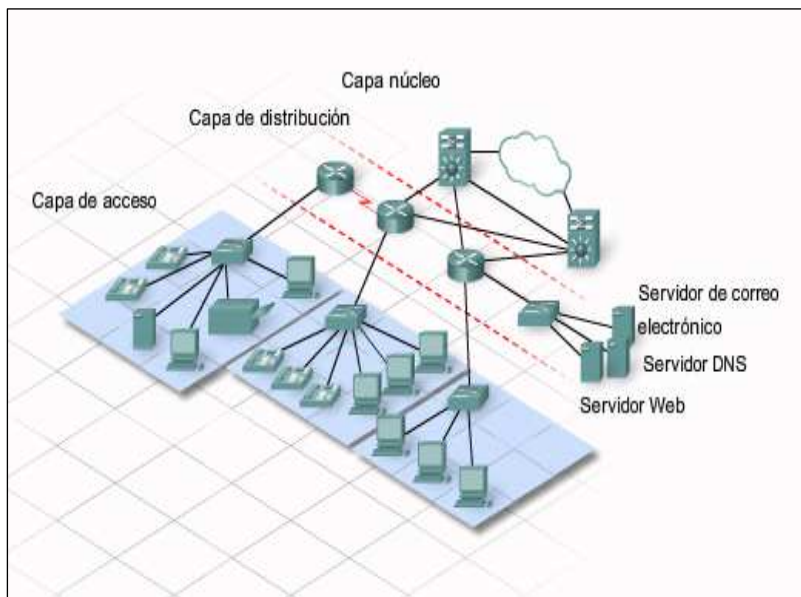
- Proporciona un punto de conexión para redes locales independientes.
- Controla el flujo de información entre redes locales.
- Garantiza que el tráfico entre hosts de la misma red local continúe a nivel local.
- Deriva el tráfico que está destinado a otras redes.

- Filtra el tráfico entrante y saliente con fines de seguridad y administración de tráfico.
- Incluye switches y routers más eficaces que la capa de acceso.
- Envía datos a la capa de núcleo para ser entregados a una red remota, si la red local no está directamente conectada.

La capa de acceso

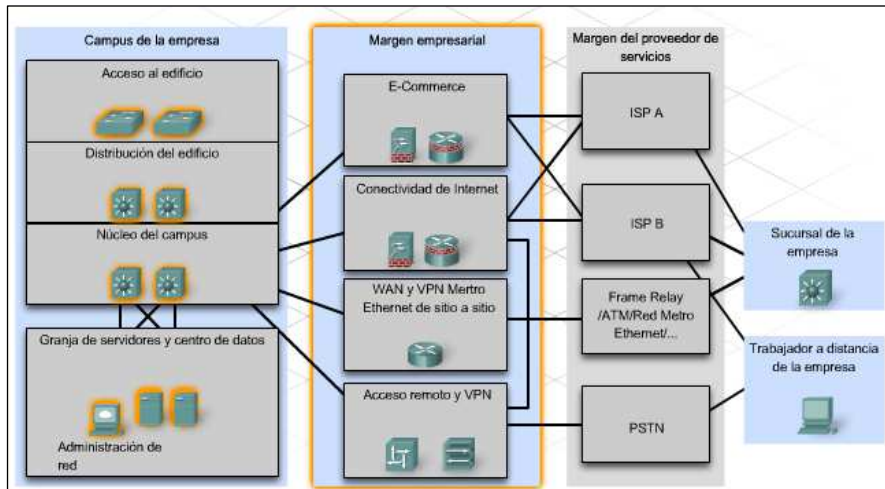
- Proporciona un punto de conexión con la red para los dispositivos del usuario final.
- Permite que varios hosts se conecten con otros hosts a través de un dispositivo de red, como un switch.
- Existe en la misma red lógica.
- Transmite tráfico a la capa de distribución para ser entregado si el mensaje está destinado a un host de otra red.

Gráfica: Diagrama de capas jerárquicas.



Arquitectura de tres capas básicas en una empresa

Gráfica: Arquitectura de tres capas.



Acceso al edificio

Este módulo de la capa de acceso contiene los switches de la capa 2 o de la 3 para proporcionar la densidad de puertos requeridos, y en éste tiene lugar la implementación de las **Vlan** y los enlaces troncales a la capa de distribución del edificio. Es importante la redundancia en los switch de distribución del edificio.

Distribución del edificio

Agrega acceso al edificio mediante los dispositivos de la capa 3, donde se ejecuta el enrutamiento, el control de acceso y la calidad del servicio **QoS**. Es fundamental proporcionar redundancia en esta área.

El núcleo (Core)

Proporciona ínter conectividad de alta velocidad entre los módulos de la capa de distribución y las granjas de servidores del Datacenter. La redundancia, la convergencia rápida y la tolerancia a fallas son el centro del diseño de esta área.

Administración de la red

Controla el rendimiento mediante el monitoreo de dispositivos y la disponibilidad de la red. La arquitectura divide la red en componentes funcionales pero mantiene el concepto de capas de acceso, distribución y núcleo. Los componentes funcionales son:

Campus empresarial

Consta de la infraestructura de campus con granjas de servidores y administración de red.

Extremo empresarial

Está compuesto por los módulos de Internet, **VPN** y **WAN**, que conectan la empresa con la red del proveedor de servicios.

Extremo del proveedor de servicios

Proporciona los servicios de Internet, red de telefonía pública conmutada (**PSTN**, Public Switched Telephone Network) y WAN. Todos los datos que entran al módulo de red del campus empresarial (ECNM) o salen de él pasan por un dispositivo de extremo. Es en este punto en donde se pueden examinar todos los paquetes y tomar la decisión de permitir el ingreso de éstos a la red empresarial o no. Los sistemas de detección de intrusiones (**IDS**) y los sistemas de prevención de intrusiones (**IPS**) también pueden configurarse en el extremo empresarial para proteger la red contra actividades maliciosas.

Tipo de tráfico en el Datacenter

Un Datacenter bien diseñado tiene patrones de flujo de tráfico definido y predecible. En algunas circunstancias el tráfico permanece en la porción de la LAN de la red, mientras que otras veces atraviesa los enlaces WAN. Por ende, es importante considerar la cantidad de tráfico destinado a una ubicación específica y dónde se origina dicho tráfico con mayor frecuencia. Por ejemplo, el tráfico que normalmente es local para los usuarios de la red incluye:

- Uso compartido de archivos.
- Impresión.
- Copia de seguridad interna y espejo.
- Comunicaciones de voz (voip¹⁰).

Los distintos tipos de tráficos que normalmente se ven en la red local, pero que también suelen enviarse a través de la WAN, incluyen:

- Actualizaciones de sistemas.
- Correo electrónico de la empresa.
- Procesamiento de transacciones.
- Accesos remotos.

Además del tráfico de la WAN, el tráfico externo se origina en Internet o está dirigido a Internet. Por lo tanto, el tráfico VPN y de Internet se considera flujo de tráfico externo. El control de éste en una red optimiza el ancho de banda e introduce un nivel de seguridad mediante el monitoreo. Al comprender los flujos y los patrones de tráfico, el administrador de la red puede predecir los tipos y los volúmenes de tráfico esperables. Cuando se detecta tráfico en un área de la red en donde no se esperaba encontrarlo, es posible filtrarlo e investigar cuál es el origen.

¹⁰ Recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol)

Gráfica: Patrones de tráfico.



Aplicaciones y la administración del tráfico

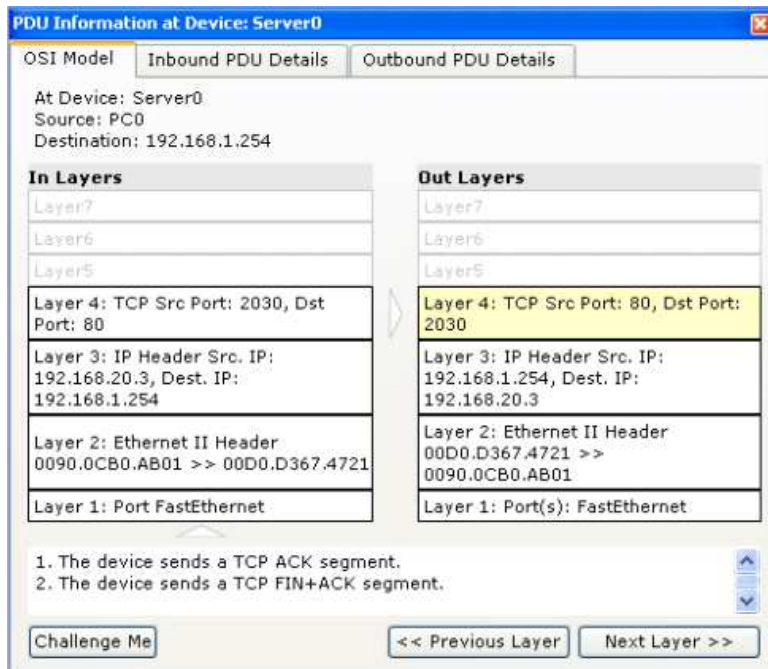
¿Cómo administrar el tráfico de la red? Es importante comprender el tipo de tráfico que atraviesa la red y el flujo de tráfico actual. Si los tipos de tráfico son desconocidos, se pueden utilizar programas que realizan la captura de tráfico y su posterior análisis.

Para determinar patrones de flujo de tráfico, es importante:

- Capturar tráfico en horas de uso pico para obtener una buena representación de los diferentes tipos de tráfico.
- Realizar la captura en diferentes segmentos de la red, porque parte del tráfico es local en un segmento en particular.

Con la información obtenida a través del programa detector de paquetes, los técnicos de la red pueden determinar flujos de tráfico. Los técnicos analizan esta información en función del origen y el destino del mismo, además del tipo de tráfico que se está enviando. Este análisis puede utilizarse para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente. Para hacerlo se pueden reducir los flujos de tráfico innecesarios o modificar patrones de flujo por completo mediante el traslado de un servidor. A veces, la simple reubicación de un servidor o un servicio en otro segmento de la red mejora el rendimiento de ésta. Mientras que otras veces, la optimización del rendimiento de la red requiere un rediseño e intervención importante.

Gráfica: Capturas de paquetes.



Priorización del tráfico de un Datacenter

No todos los tipos de tráfico de red tienen los mismos requisitos ni se comportan de la misma manera.

Detalle del tráfico en un Datacenter

La mayoría de las aplicaciones de red utilizan tráfico de datos. Algunos tipos de aplicaciones en línea transmiten datos de manera esporádica. Otros tipos de aplicaciones, por ejemplo las aplicaciones de almacenamiento de datos, transmiten grandes volúmenes de tráfico durante períodos prolongados. Algunas aplicaciones de datos se interesan más por los aspectos relacionados con el tiempo que por la fiabilidad y la mayoría de las aplicaciones de datos pueden tolerar retrasos. Por este motivo, el tráfico de datos normalmente emplea el Protocolo de control de transmisión (**TCP, Transmission Control Protocol**). El TCP utiliza acuses de recibo para determinar cuándo es necesario volver a transmitir paquetes perdidos y, por lo tanto, garantiza la entrega. Si bien el uso de acuses de recibo hace que el TCP sea un protocolo de entrega más confiable, también se genera un retraso.

El tráfico de voz y el de video son diferentes del tráfico de datos. Las aplicaciones de voz y video requieren un flujo ininterrumpido de datos para garantizar conversaciones e imágenes de alta calidad. El proceso de acuse de recibo del TCP introduce retrasos, lo que interrumpiría estos flujos y degradaría la calidad de la aplicación. Por lo tanto, las aplicaciones de voz y video emplean el Protocolo de datagramas del usuario (**UDP, User Datagram Protocol**) en lugar del TCP. Y como el UDP no tiene mecanismos de retransmisión de paquetes perdidos, minimiza los retrasos.

Además de comprender los retrasos del TCP en comparación con el UDP, también es necesario comprender el retardo, o latencia, ocasionado por los dispositivos de red que deben procesar el tráfico a medida que se transmite hasta el destino. Los dispositivos de Capa 3 del modelo OSI crean un mayor retraso que los dispositivos de Capa 2 a causa de la cantidad de encabezados que deben procesar. Por lo tanto, los routers introducen un mayor retraso que los switch. La fluctuación de fase, ocasionada por una congestión de la red, es la variación en el tiempo de los paquetes que llegan a destino. Por consiguiente, es importante reducir el impacto del retraso, la latencia y la fluctuación de fase para el tráfico sensible al tiempo.

La Calidad de servicio (**QoS**) es un proceso que se utiliza para garantizar un flujo de datos especificado. Los mecanismos de QoS ordenan el tráfico en colas según la prioridad. Por ejemplo, el tráfico de voz tiene prioridad sobre el tráfico de datos común.

Gráfica: Terminología.

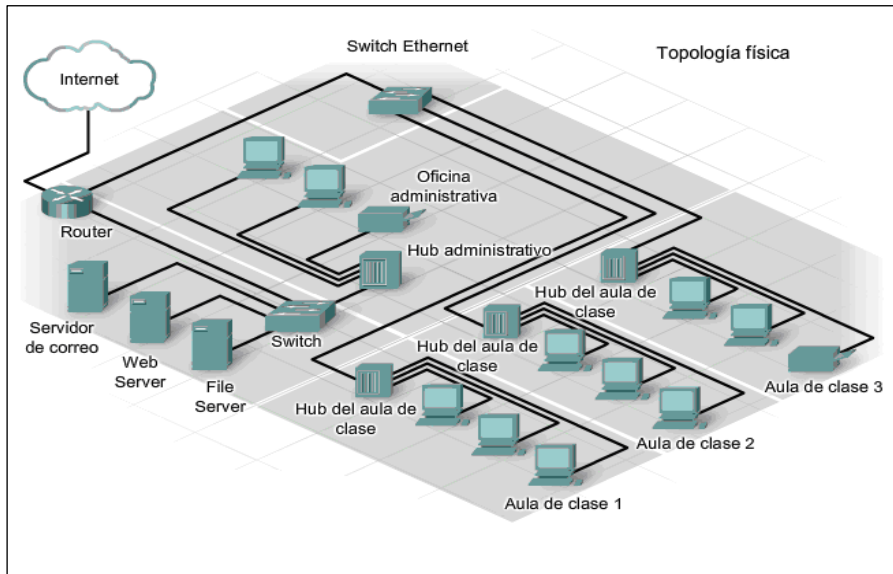
Término	Definición
UDP	Protocolo usado para tráfico sensible a los tiempos
Calidad de servicio	Ordena el tráfico en colas
Fluctuación de fase	Variación en el tiempo de llegada causada por la congestión de la red
retardo	Mismo significado que la latencia
Cola	Línea de tráfico ordenada en función de la prioridad
TCP	Protocolo que retransmite paquetes
voz	Tipo de tráfico sensible a los tiempos
latencia	Demora basada en los paquetes que se transmiten a través de los dispositivos de red

Documentar un Datacenter

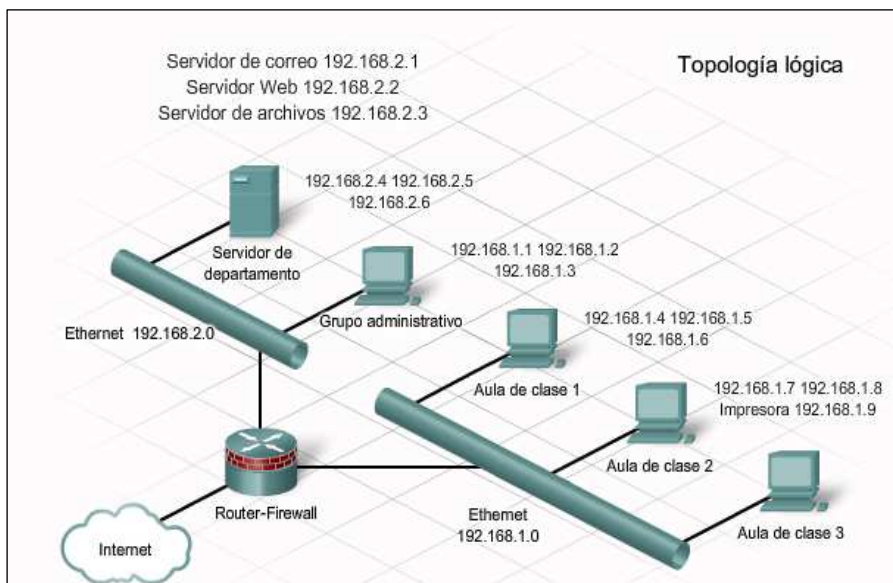
Una de las primeras tareas, para documentar un datacenter, es familiarizarse con la estructura de la red actual porque pueden tener miles de hosts y cientos de dispositivos de red, interconectados por tecnologías inalámbricas, de cables de cobre y de fibra óptica. Todas las estaciones de trabajo, los servidores y los dispositivos de red, como los switches y los routers, deben estar documentados. Los diversos tipos de documentación muestran diferentes aspectos de la red. Los diagramas de infraestructura de la red o los diagramas topológicos mantienen un registro de la ubicación, la función y el estado de los dispositivos. Los diagramas topológicos representan la red física o la red lógica. Un mapa de topología física emplea íconos para documentar la ubicación de los hosts, de los dispositivos de red y de los medios. Es importante mantener y actualizar los mapas de topología física para facilitar futuras tareas de instalación y de resolución de problemas, (**Networks Inventory NI**). Su actualización permite una eficiente explotación y operación de red. Un mapa de topología lógica agrupa los hosts según el uso de red, independientemente de la ubicación física. Y en ellos se pueden registrar los nombres de los hosts, las direcciones, la información de los grupos y las aplicaciones. Las conexiones entre sitios múltiples pueden aparecer, pero no representan ubicaciones físicas reales. Los diagramas de red pueden incluir también información del plano de control, ya que ésta

describe los dominios de fallas y define las interfaces en donde las diferentes tecnologías de red se interconectan.

Gráfica: Topología física.



Gráfica: Topología lógica.



Es fundamental que la documentación de la red permanezca actualizada y sea exacta, y normalmente lo es en el momento de la instalación, sin embargo, a medida que crece o cambia, la documentación no siempre está actualizada. Los mapas de topología de red están basados, con frecuencia, en los planos de pisos originales. Mientras que los actuales pueden haber sido modificados desde la construcción del edificio. Los anteproyectos pueden estar marcados o coloreados en rojo para indicar las modificaciones. El diagrama modificado se conoce como proyecto terminado o conforme a obra. Un diagrama de proyecto terminado documenta cómo se construyó realmente una red, lo que puede diferir de los planos originales. Asegúrese siempre de que la documentación actual refleje el plano de piso del proyecto terminado y todas las modificaciones en la topología de la red. Además de documentar cualquier cambio en la etapa de explotación en el mapeo de un proceso estipulado, es de vital importancia el Network Inventory que debe permanecer actualizado on-line y no permitir implementar cambios físicos/lógicos no registrados previamente en el NI.

Plan de continuidad del Datacenter

El Plan de continuidad del Datacenter (**DCP, Datacenter Continuity Plan**) identifica los pasos que se deben seguir para continuar con el funcionamiento del Datacenter en caso de que ocurra un desastre natural o provocado por el hombre.

Plan de seguridad del Datacenter

El Plan de seguridad del Datacenter (**CSP, Datacenter Security Plan**) incluye medidas de control físicas, de sistema y organizacionales. El plan de seguridad general debe incluir una porción de **TI** que describa cómo una organización protege su red y sus bienes de información. Por ejemplo políticas de seguridad de acceso.

Plan de mantenimiento de la red del Datacenter

El Plan de mantenimiento de red (**NMP, Network Maintenance Plan**) asegura la continuidad del Datacenter mediante el cuidado y el funcionamiento eficiente de la red. El mantenimiento de la red se debe programar durante períodos específicos, normalmente durante las noches y

los fines de semana, a fin de minimizar el impacto sobre las operaciones comerciales. Ejemplos: Tiempo de inactividad programado, monitoreo del rendimiento de la red.

Acuerdo del nivel de servicio (SLA)

El Acuerdo de nivel de servicio (**SLA, Service Level Agreement**) es un acuerdo contractual entre el cliente y un proveedor de servicios o ISP, en el que se detalla información como la disponibilidad de la red y el tiempo de respuesta del servicio.

Centro de operaciones de red (NOC)

La mayoría de los Datacenter tienen un Centro de operaciones de red (**NOC**) que le permite realizar la administración general y el monitoreo en tiempo real de todos los sistemas. Los empleados de un NOC típico de un Datacenter proporcionan soporte para ubicaciones locales y remotas, y, a menudo, administran problemas de redes locales y de redes de área extensa. Los NOC más grandes pueden ser áreas de múltiples espacios de un edificio en donde se concentra el equipo de red y el personal de soporte técnico. Al NOC también se lo llama Centro de monitoreo.

Generalmente, el NOC tiene como finalidad monitorear:

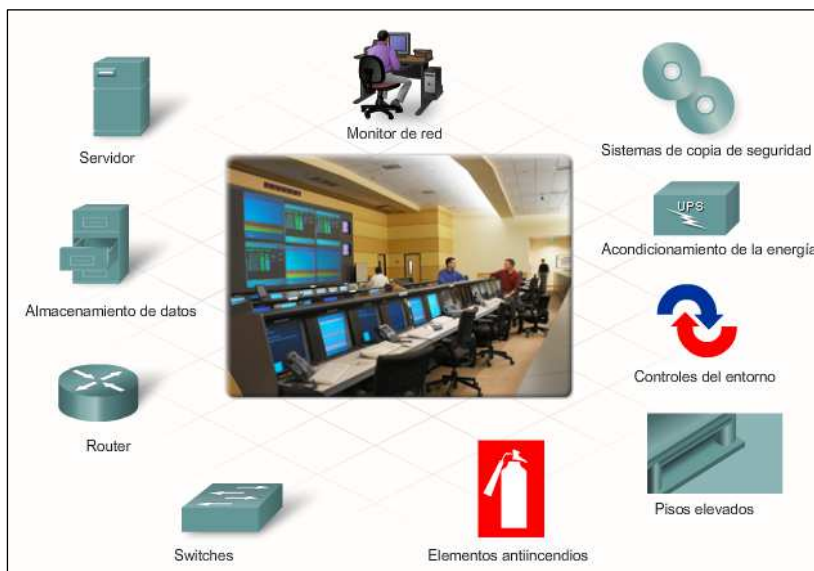
- Sistemas de aire acondicionado.
- Sistema de potencia ininterrumpida (**UPS**).
- Sistema de detección y extinción de incendios.
- Sistema de seguridad y control de acceso.
- Sistema de procesamiento de datos.
- Sistema de distribución eléctrica.
- Sistema de Generación.

El concepto general de un NOC es el de supervisar el estado de la red/servicios en tiempo real y disparar las acciones necesarias en caso de contingencias contemplando por ejemplo los siguientes escalamientos.

1. Intervención.

2. Derivación de técnico de campo.
3. Escalamiento a especialistas
4. Escalamiento a proveedores.

Gráfica: NOC o centro de monitoreo.



Además de proveer asistencia y administración de red, muchos NOC también proveen recursos centralizados, como servidores y almacenamiento de datos. Los servidores del NOC están normalmente agrupados juntos con el fin de formar una granja de servidores. Esta suele considerarse como un recurso único. Sin embargo, proporciona dos funciones: Copia de seguridad y balanceo de cargas. Si un servidor falla o se sobrecarga, otro toma el lugar del que fallo. Los servidores de la granja pueden estar montados en bastidor e interconectados por switches de muy alta velocidad (Ethernet Gigabit o superior). Además, pueden ser servidores blade montados en un chasis y conectados mediante un backplane de alta velocidad dentro del chasis.

Otro aspecto importante del NOC del Centro de Datos es el almacenamiento de datos de alta velocidad y de alta capacidad. Este almacenamiento de datos o almacenamiento con conexión a red (NAS), agrupa grandes cantidades de discos que están directamente conectados a la red y pueden ser utilizados por cualquier servidor. Generalmente, un dispositivo de NAS se

conecta a una red Ethernet y se le asigna su propia dirección IP. Una versión más sofisticada de NAS es Storage Área Network (SAN). Una SAN es una red de alta velocidad que interconecta diferentes tipos de dispositivos de almacenamiento de datos sobre una LAN o una WAN.

Todo el equipamiento del Datacenter está normalmente montado sobre bastidores, estos suelen estar montados verticalmente y pueden estar conectados entre ellos. El ancho más común de los bastidores es de 19 pulgadas (48,26 cm), y la mayoría de los equipos están diseñados para este ancho. El espacio vertical que ocupa el equipo se mide en unidades de bastidor (**RU, Rack Units**). Una unidad equivale a 1,75 pulgadas (4,4 cm). Por ejemplo, un chasis de 2 unidades mide 3,5 pulgadas (8,9 cm) de altura. Los bastidores o racks, están limitados por la velocidad de evacuación de calor con medios mecánicos y la refrigeración de la sala. Otro factor para tener en cuenta son los equipos con muchas conexiones, como los switch. Es posible que sea necesario colocarlos cerca de paneles de conexión y de donde el cableado se agrupa en bandejas de cables.

Gráficamente:



El NOC representa el sistema nervioso central del Centro Datos. Sin embargo, en la práctica, la mayoría de los usuarios se conectan a un switch ubicado en un cuarto de telecomunicaciones, el cual se encuentra a cierta distancia del NOC. Este cuarto también se conoce como un armario cableado o una instalación de distribución intermedia (**IDF, intermediate distribution facility**), cuenta con los dispositivos de red de la capa de acceso y mantiene

a la perfección las condiciones ambientales, como el aire acondicionado y el sistema de UPS, de una manera similar al NOC.

Factores de seguridad en el diseño de un Datacenter

Los usuarios que trabajan con tecnología conectada por cable se conectan a la red con switches o hubs Ethernet. Mientras que los que trabajan con tecnología inalámbrica se conectan a través de un punto de acceso (**AP Access Point**). Los dispositivos de capa de acceso, tales como los switches y AP representan una posible vulnerabilidad en la seguridad de la red. De modo que el acceso físico y remoto a este equipo se debe limitar únicamente al personal autorizado, y a su vez el personal de red también puede implementar seguridad en los puertos y otras medidas en los switch, así como diversas medidas de seguridad inalámbrica en los AP. Ya que proteger el cuarto de telecomunicaciones se ha convertido en algo aún más importante debido a los crecientes casos de robo de identidad. Las nuevas leyes de privacidad aplican duras sanciones si la información confidencial de una red cae en manos que no debe caer. Los dispositivos de red modernos cuentan con propiedades que ayudan a prevenir estos ataques y a proteger la información y la integridad del usuario.

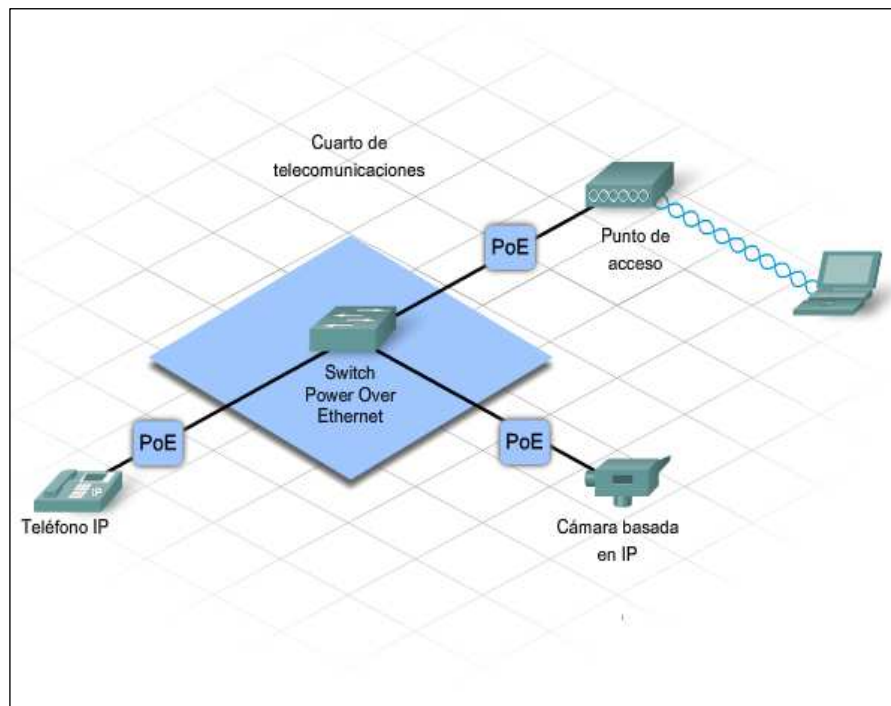
Gráfica: Auditoria informática in-situ.



Funcionamiento del sistema de alimentación sobre ethernet (POE)

Además de proporcionar conectividad de acceso a red básica, es cada vez más común suministra energía para los dispositivos de usuarios finales directamente desde Switches Ethernet del cuarto de telecomunicaciones. Estos dispositivos incluyen teléfonos IP, puntos de acceso y cámaras de vigilancia. El estándar **IEEE 802.3af**, Power Over Ethernet o **PoE**, suministra energía a un dispositivo por el mismo cable de par trenzado que transmite los datos. Esto permite que, por ejemplo, un teléfono IP se coloque en un escritorio sin necesidad de cable ni toma de alimentación independiente. Para aquellos switch que no soportan PoE también se le puede suministrar con inyectores de alimentación o paneles de conexión PoE. Panduit y otros proveedores que producen paneles de conexión PoE que permiten que los switch sin capacidad PoE participen en entornos de éste. Los Switches Legacy se conectan a un panel de conexión PoE que, a su vez, se conecta al dispositivo que lo admite.

Grafica: El sistema POE.

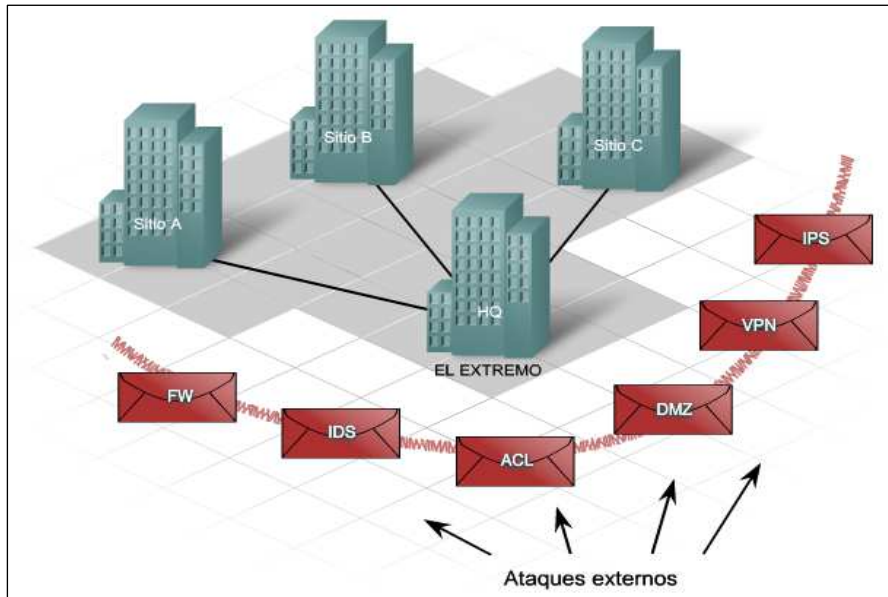


Seguridad del Datacenter

Los Datacenter, generalmente, cuentan con muchos sitios que se interconectan. Las ubicaciones múltiples pueden tener conexiones de extremo en cada sitio, que conectan la empresa con otras personas y organizaciones. El extremo es el punto de entrada para los ataques externos y representa un punto de vulnerabilidad. Estos pueden afectar a miles de usuarios. Por ejemplo, los ataques de denegación de servicio (**DoS, Denial of Service**) impiden a los usuarios legítimos, dentro y fuera de la red, de acceder a los recursos, lo que afecta la productividad de toda la empresa. Todo el tráfico que entra a la organización y sale de ella pasa por el borde. Los dispositivos de extremo deben configurarse para ofrecer protección contra los ataques y para proporcionar filtros basados en el sitio web, la dirección IP, el patrón de tráfico, la aplicación y el protocolo.

Una Datacenter puede implementar un firewall (**FW**) y aplicaciones de seguridad con un sistema de detección de intrusión (**IDS**) y un sistema de prevención de intrusión (**IPS**) en el extremo para proteger la red. Los administradores de redes externos necesitan tener acceso para realizar el mantenimiento interno y la instalación del software. Las redes privadas virtuales (**VPN, virtual private networks**), las listas de control de acceso (**ACL, Access control lists**), las identificaciones de los usuarios y las contraseñas proporcionan ese acceso. Las VPN también permiten que los trabajadores remotos accedan a los recursos internos.

Gráfica: Esquemas de seguridad.

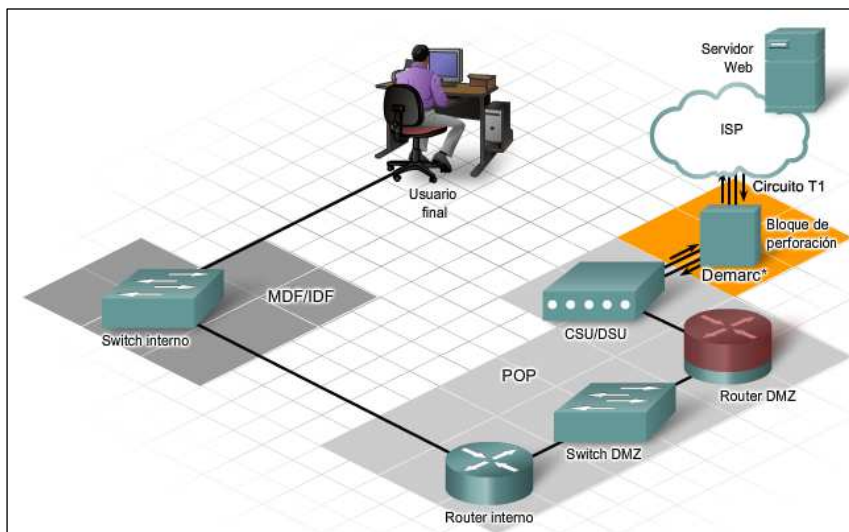


Conexión del Datacenter con servicios externos

Los servicios de conexión de red que normalmente adquiere un Datacenter incluyen líneas alquiladas (**T1/E1**¹¹), **Frame Relay** y **ATM** entre otros. El cableado físico lleva estos servicios al Datacenter mediante cables de cobre, como en el caso de T1/E1, o cables de fibra óptica para obtener servicios de mayor velocidad. Por ende, la sala de comunicación debe contar con determinados equipos para obtener cualquier servicio WAN que se requiera. Por ejemplo, para obtener el servicio T1/E1, se debe emplear un bloque de perforación para finalizar el circuito T1/E1, así como una unidad de servicios de canales / Unidad de servicios de datos (**CSU/DSU, Channel Service Unit/Data Service Unit**) a fin de proporcionar la interfaz y las señales eléctricas adecuadas para el proveedor del servicio. Este puede ser el propietario del equipo y encargarse del mantenimiento o el cliente, que en este caso es el propio Datacenter.

¹¹ Servicio de portadora de WAN digital que transmite datos con formato DS-1 a 1.544 Mbps a través de la red de conmutación electrónica, usando codificación AMI o sustitución de 8 ceros.

Gráfica: Sencillo esquema de un enlace proveedor – cliente.



Funcionamiento de un router

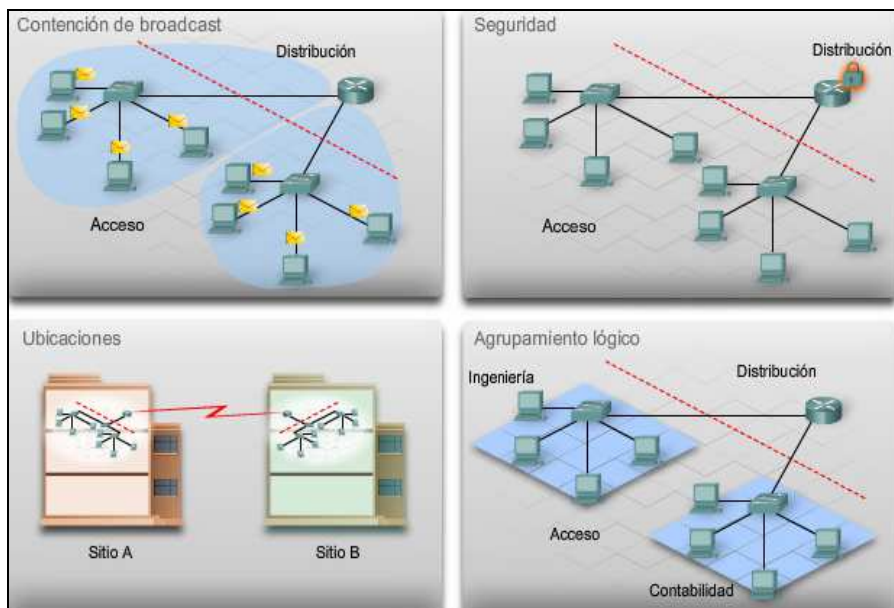
Un dispositivo importante de la capa de distribución de un centro de datos es el router. Sin el proceso de enrutamiento, los paquetes no podrían abandonar la red local. Este proporciona acceso a otras redes privadas, como también a Internet. Todos los hosts de una red local especifican la dirección IP de la interfaz del router local en la configuración IP. Esta interfaz del router es el gateway predeterminado. Los routers cumplen un papel muy importante en la red, ya que interconectan múltiples sitios dentro y fuera de la red, lo que proporciona rutas redundantes y conecta los **ISP** en Internet. Y también pueden actuar como traductores entre los diferentes tipos de medios y protocolos. Por ejemplo, un router puede re encapsular paquetes de una encapsulación Ethernet a un serial. Los routers usan la parte de la red de la dirección IP de destino para enrutar paquetes hacia el destino correcto. Seleccionan una ruta alternativa si el enlace deja de funcionar o si hay mucho tráfico.

Los routers también cumplen otras funciones útiles:

- Ofrecen contención de broadcast.
- Conectan ubicaciones remotas.

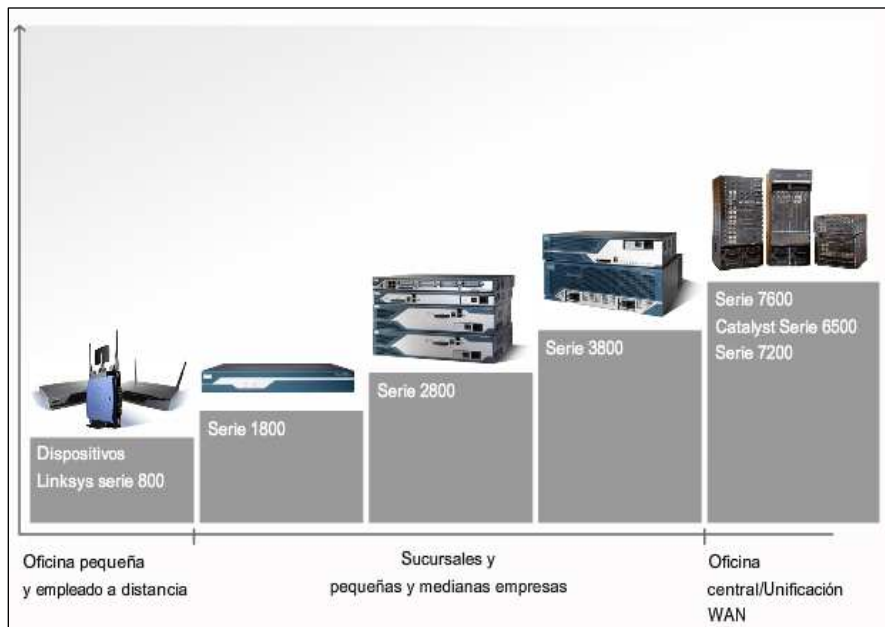
- Agrupan a los usuarios lógicamente de acuerdo con la aplicación o el departamento.
- Proporcionan seguridad mejorada (con **NAT** y **ACL**).

Gráfica: Propiedades de un router.



Los routers están disponibles en diversas formas y tamaños, llamados factores de forma. Los administradores de red en el entorno deben poder soportar diversos routers y switch, desde un modelo de escritorio hasta uno montado en bastidor o Blade. Estos también pueden categorizarse como configuración fija o modular. Con la configuración fija, las interfaces de router deseadas están incorporadas. Los routers modulares tienen múltiples ranuras que permiten al administrador de red cambiar las interfaces en el router. Por ejemplo, el router Cisco 1841 cuenta con dos interfaces Fase Ethernet RJ-45 incorporadas y dos ranuras que pueden alojar diversos módulos de interfaz de red. Los routers tienen una variedad de interfaces distintas, tales como Fast y Gigabit Ethernet, Serial y de fibra óptica. Las interfaces de routers usan las convenciones de controlador/interfaz o controlador/ranura/interfaz. Por ejemplo, al emplear la convención del controlador/interfaz, la primera interfaz de Fast Ethernet de un router posee la numeración Fa0/0 (controlador 0 e interfaz 0). La segunda es Fa0/1. La primera interfaz serial de un router que emplea controlador/ranura/interfaz es S0/0/0.

Gráfica: Familia de routers.



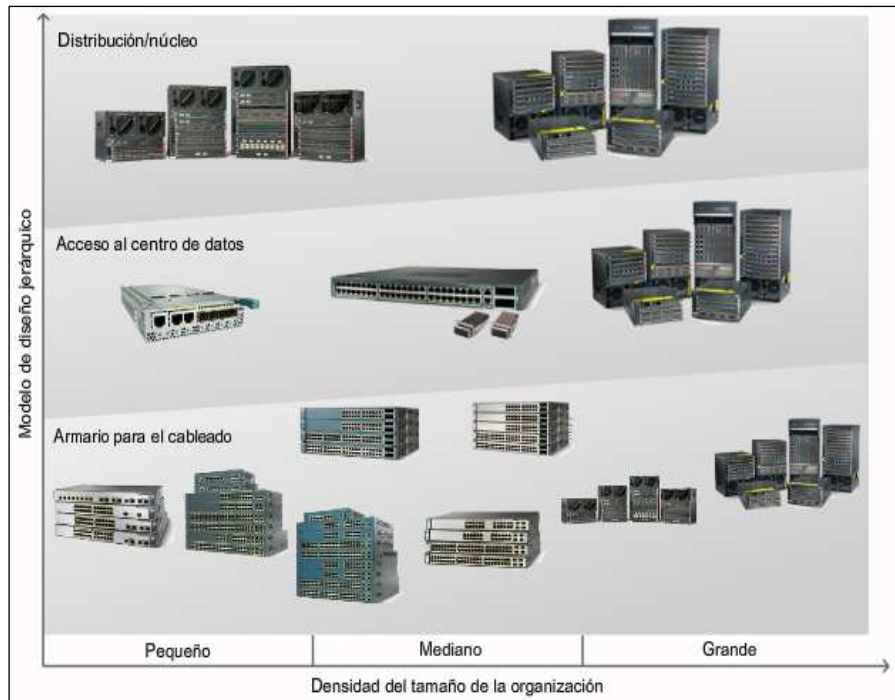
Funcionamiento de un switch

Aunque las tres capas del modelo de diseño jerárquico poseen switches y routers, la capa de acceso generalmente tiene más switches. La función principal de los switches es conectar los hosts, tales como las estaciones de trabajo de usuario final, los servidores, los teléfonos IP, las cámaras web, los puntos de acceso y los routers. Esto quiere decir que en una organización hay muchos más switches que routers.

Los switch poseen muchos factores de forma:

- Los modelos autónomos pequeños se colocan en un escritorio o en una pared.
- Los routers integrados poseen un switch incorporado al chasis que está montado en el bastidor.
- Los switches de alto nivel se montan en un bastidor y suelen tener un chasis del tipo blade.

Gráfica: Familia de switches.

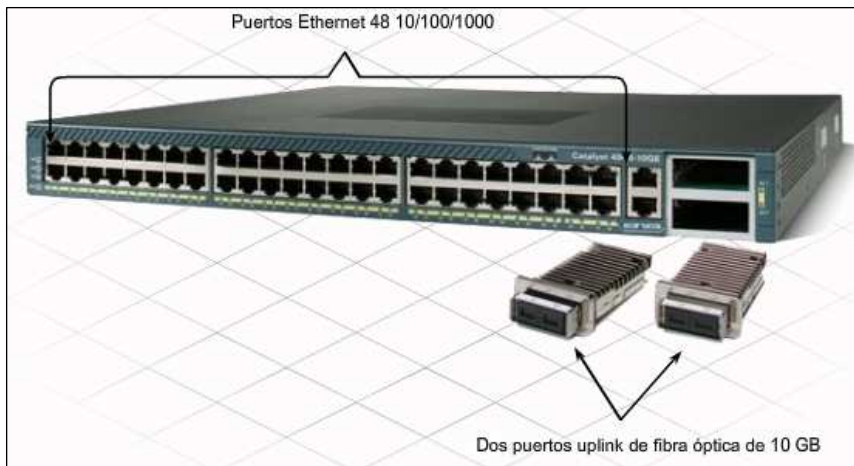


Los Switches de alto nivel utilizados en los Centro Datos y en los proveedores de servicios admiten puertos de diferentes velocidades, de 100 MB a 10 GB. Un switch de un **MDF** se conecta con otros switches desde los **IDF** a través de fibra Gigabit o cable de cobre. Un switch de la IDF, por lo general, requiere puertos RJ-45 Fast Ethernet para la conectividad de los dispositivos y, al menos, un puerto Gigabit Ethernet (de cobre o de fibra), para realizar un uplink al switch de la MDF. Algunos Switches de alto nivel tienen puertos modulares que se pueden cambiar si es necesario. Por ejemplo, podría ser necesario pasar de la fibra multimodo a una fibra de monomodo, para lo que se necesitaría un puerto distinto.

Al igual que los routers, los puertos del switch también están diseñados con las convenciones controlador/puerto o controlador/ranura/puerto. Por ejemplo, al emplear la convención del controlador/puerto, el primer puerto de Fast Ethernet en un Switch posee la numeración Fa0/1 (controlador 0 y puerto 1). La del primer puerto en un Switch que emplea un controlador/ranura/puerto es Fa0/0/1. Mientras que la del segundo es Fa0/2.. La designación de los puertos Gigabit es Gi0/1, Gi0/2, etc. La densidad del

puerto en un switch es un factor de importancia para un entorno empresarial en el que cientos o miles de usuarios necesitan conexiones. Un switch con 1 RU de altura y 48 puertos tiene una densidad de puerto superior que uno de 1 RU y 24 puertos.

Gráfica: Detalle de un switch.



Tradicionalmente, las redes están compuestas por dispositivos separados según sean de Capa 2 o Capa 3. Cada dispositivo utiliza una técnica diferente para procesar y enviar el tráfico.

Funcionamiento de la CAPA 2

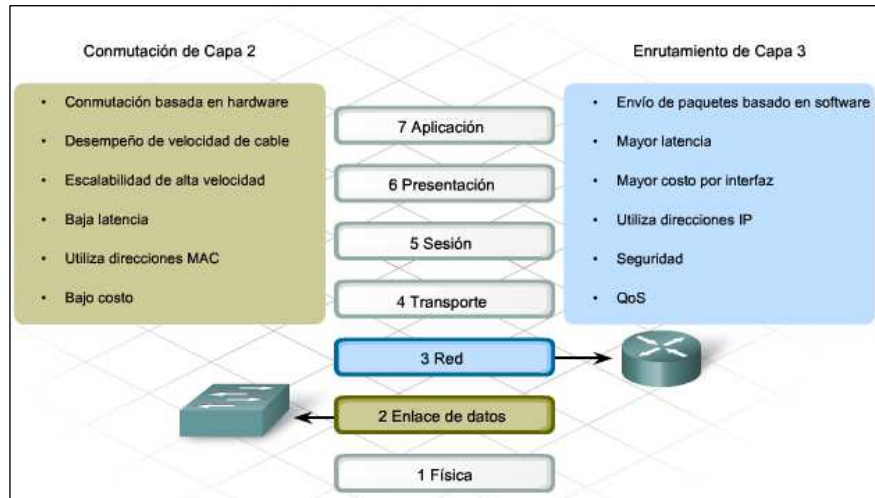
Los switch de Capa 2 están basados en hardware y envían el tráfico a la velocidad de cable, mediante los circuitos internos que conectan físicamente a cada puerto entrante con todos los demás puertos. El proceso de envío utiliza la dirección MAC y la existencia de la dirección MAC de destino en la tabla de direcciones. Un switch de Capa 2 limita el envío de tráfico a un único segmento o una subred dentro de la red.

Funcionamiento de la CAPA 3

Los routers están basados en software y utilizan microprocesadores para llevar a cabo el enrutamiento según las direcciones IP. El enrutamiento de Capa 3 permite el reenvío de tráfico entre diferentes redes y subredes. Cuando un paquete ingresa a la interfaz del router, éste utiliza software para

encontrar la dirección IP de destino y seleccionar la ruta más adecuada hacia la red de destino. Luego el router conmuta el paquete a la interfaz de salida correspondiente.

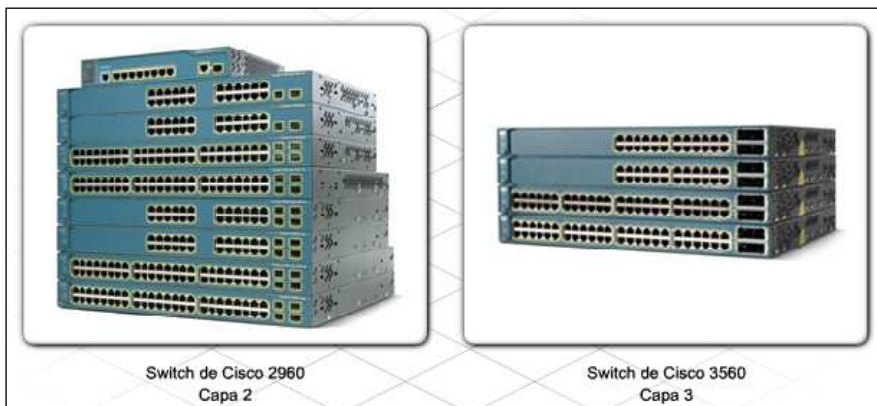
Gráfica: Esquema de conmutación.



La conmutación de Capa 3, o conmutación multicapa, combina la conmutación basada en hardware y el enrutamiento basado en hardware en el mismo dispositivo. Un switch multicapa combina las funciones de un switch de Capa 2 y un router de Capa 3. La conmutación de Capa 3 se lleva a cabo en hardware especial de circuito integrado de aplicación específica (ASIC). Las funciones de envío de trama y de paquetes utilizan los mismos circuitos ASIC.

Con frecuencia, los switches multicapa guardan, o almacenan en caché, la información de enrutamiento de origen y destino del primer paquete de una conversación. Para los paquetes siguientes, no es necesario ejecutar una búsqueda de enrutamiento, ya que la información de enrutamiento se encuentra en la memoria. Esta función de almacenamiento en caché contribuye al gran rendimiento de estos dispositivos

Gráfica: Switch capa 2 y 3.



CAPÍTULO 10 - Arquitectura

Arquitectura de red del Datacenter

La arquitectura de la red del Datacenter permite que empresas protejan sus aplicaciones críticas y los datos confidenciales. La eficiencia de las operaciones crea nuevos ambientes de aplicación seguros que pueden soportar nuevos procesos de negocios. La arquitectura de la red provee un fundamento escalable que permite que el Datacenter ofrezca una variedad de servicios. La infraestructura que suministra al usuario acceso seguro para utilizar los servicios que brinda el Datacenter, es una estructura confiable y escalable que da soporte a las más exigentes aplicaciones. Tanto de grandes empresas como también a las Pymes.

El conjunto de componentes que integra el Datacenter, incluye las aplicaciones propiamente dichas, los servidores, los equipos de comunicaciones, el storage, y son las articulaciones más importantes que un Datacenter planeado correctamente debe poseer para su óptimo desempeño. La red protege la integridad de los datos, optimiza la disponibilidad de aplicaciones y el rendimiento, y permite además responder a nuevos requerimientos de tecnología que rápidamente están cambiando. Dependiendo de las condiciones del mercado, y las prioridades de la empresa.

El marco de arquitectura **SONA** (*Arquitectura de red orientada a servicios*) da una idea general de cómo se puede desarrollar una red de información inteligente basada en las necesidades de las empresas, optimizando aplicaciones y procesos de negocios. **SONA** puede incrementar la productividad, la eficiencia del Datacenter, puede reducir gastos y mejorar la alianza de **IT** con la empresa. La arquitectura de la red del Datacenter basado sobre **SONA** suministra a las organizaciones de **IT** un marco de estandarización. Las Tecnologías de computación, dentro del contexto de un enfoque arquitectónico, presentan una arquitectura a los directores de **IT** más consolidada y flexibles a la hora de implementar nuevos requerimientos. La libertad de desplegar computación, tecnologías de storage y software de

administración mejoran la calidad del servicio que las empresas necesitan en su negocio como así también reducir el riesgo, el tiempo, y la inversión.

Sistemas y tecnologías que brinda un Datacenter

- Las aplicaciones de n capas: Las zonas seguras de la red soportan dos, tres o ambientes de aplicaciones de n capas, con las técnicas de optimización de aplicaciones disponibles y la utilización de almacenamiento.
- La aceleración de aplicaciones y tecnologías de optimización de servidores proveen mayor escalabilidad y entrega de aplicaciones a usuarios finales.
- Los servidores Blade: La arquitectura de red del Datacenter integrada por los servidores Blade brindan integración de tecnología de switching integrando Ethernet e Infiniband. Logrando así optimizar el rendimiento y la seguridad.
- Clustering: Computación de alto rendimiento y Grid son paradigmas desarrollados para realizar computación heterogénea distribuida.
- La arquitectura SOA y servicios web: La arquitectura del Datacenter facilita el despliegue rápido y seguro de SOA. Permitiendo el despliegue dinámico y la integración con servicios de mensajes, basados en una infraestructura segura, aumentando la integración del servicio.
- Mainframe: Despliega las tecnologías que soportan la arquitectura de la red de sistemas (SNA), SNA – IP.

Interconexión del Datacenter

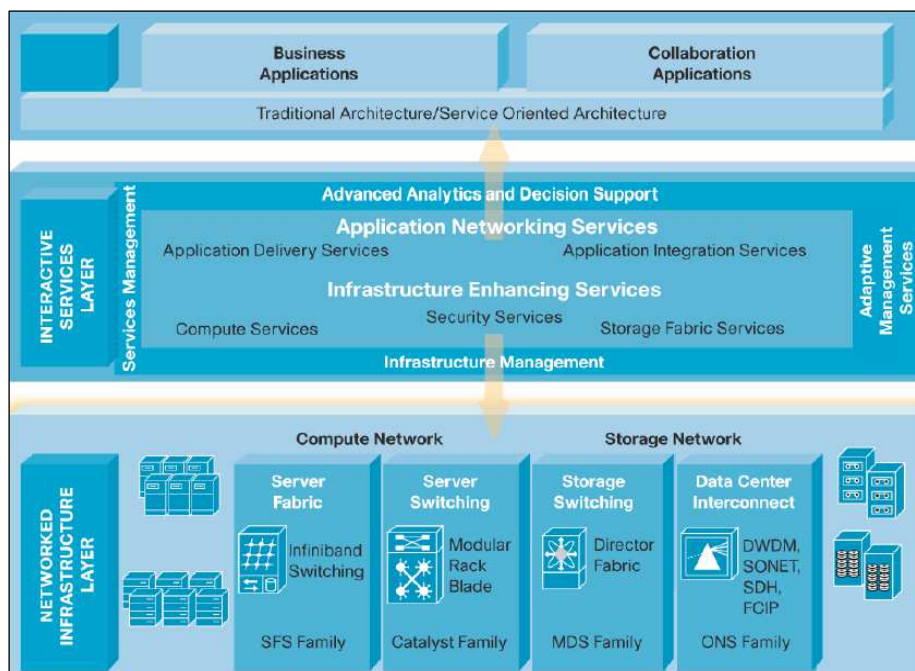
Conecta los Datacenter principales con los centros secundarios mediante circuitos ópticos o enlaces WAN tradicionales. Las prácticas recomendadas para la duplicación de datos y continuidad del negocio recomiendan la necesidad de conexiones de baja latencia y de alta velocidad entre las ubicaciones de los Datacenter. Las funciones inherentes a las redes ópticas (baja latencia, alto ancho de banda y alta densidad), son perfectas para la interconexión de redes SAN, nodos de clúster y granjas de servidores entre varios Datacenter. Cuando no es posible contar con redes ópticas, los protocolos del Datacenter, incluido FC, se puede transportar por IP en redes

WAN tradicionales. El acceso a redes proporciona un acceso seguro a los usuarios, empleados, y se conecta de forma remota mediante la intranet, extranet o Internet. La mayoría de los usuarios no se encuentran cerca del Datacenter por lo que es obligatorio contar con una conectividad segura y sólida al Datacenter. La adaptabilidad de la arquitectura de red del Datacenter ofrece a las empresas la capacidad para minimizar las repercusiones de situaciones de desastres gracias a una arquitectura que ayuda a reducir riesgos y también proporciona herramientas y tecnologías que aceleran la recuperación.

Servicios interactivos de capas

Esta capa suministra la capacidad de servicios y asegura los recursos de las aplicaciones, así como también brinda servicios de conexión a red que optimizan la integración de aplicaciones para usuarios finales. Aquellos servicios son integrados dentro de la plataforma de la red para así aumentar la escalabilidad, control y transparencia. Esta arquitectura soporta el despliegue de aplicaciones empresariales y de colaboración como así también aplicaciones tradicionales.

Gráfica: Arquitectura de red del Datacenter.



Servicios de seguridad

Defender recursos y aplicaciones de los ataques sofisticados y peligrosos es todo un desafío. La protección consecuente del Datacenter consolidado es estimulante, porque los ataques pueden extenderse no solo a un sistema aislado sino también a otros sistemas instalados en la infraestructura. La red debe proporcionar una seguridad integrada que proteja servidores, aplicaciones, y los datos dentro de zonas seguras. La arquitectura de la red del Datacenter debe brindar las estrategias de seguridad, la tecnología y su disponibilidad, y los productos diseñados para cumplir con ciertos requerimientos al pie de la letra dentro de la organización. Estas estrategias están basadas en políticas de seguridad que poseen un amplio dominio, como ser la seguridad IP, el almacenamiento, y las redes de interconexión. Los Módulos de servicio de seguridad integrados sobre plataformas de serie proveen capacidades muy variadas, desde la virtualización de cortafuegos hasta equipos físicos enlazados entre VLANs, la detección de intrusión, y la denegación de servicio (**DDOS**), además son capacidades de seguridad de software que no deben dejarse de lado, ya que son herramientas de administración de seguridad a tenerse en cuenta en una implementación de un Datacenter.

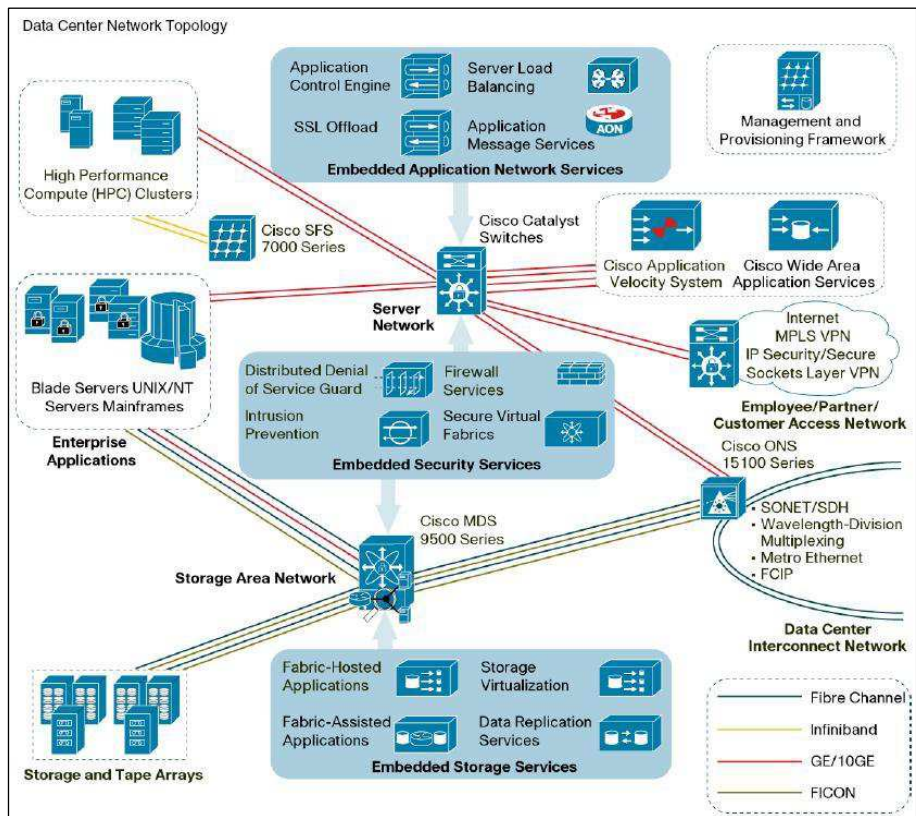
Servicios de computación

La consolidación de los datos en ambientes heterogéneos instalados sobre distintas plataformas y sistemas operativos es una realidad. Esto implica que los Datacenter son cada vez más densos y por ello deben proveer una arquitectura de red que soporte esta heterogeneidad y al mismo tiempo proveer los mecanismos para controlar los recursos utilizados para este procesamiento distribuido, CPU, memoria, y E/S. La virtualización de aplicaciones brinda capacidad de cómputo en tiempo real. Los servicios incluyen la inteligencia provista por la estructura de la red para comprender y apoyar los protocolos que mejor se adapten a sus requerimientos. El uso disponible de recursos y el intercambio de comunicación entre ellos, gracias a una estructura de comunicación inteligente, da como resultado que los servicios desarrollen una baja latencia.

Desarrollo de la capa de la infraestructura de red

Esta capa es la encargada de proveer servicios de conectividad inteligente a los elementos que integran el Datacenter, como por ejemplos los servidores y el almacenamiento, usuarios externos y otros Datacenter. Los Server Fabric brindan plataformas escalables que integran servicios inteligentes directamente en la estructura. Esta capa es la encargada de gestionar los distintos protocolos que conviven en la red. Además su diseño debe contemplar la capacidad de migrar de una tecnología a otra más reciente. En un storage trabajando con un enlace de 1 GB por razones de incremento del ancho de banda se lo debe llevar a enlaces de 4 GB por medio de fibra óptica. La figura siguiente describe cómo podrían interconectarse usuarios, computadores, recursos de storage y un Datacenter de respaldo. A continuación se describirá cada una de estas plataformas en más detalle.

Gráfica: Arquitectura de interconexión.



Funcionamiento de una red de granja de servidores

La consolidación de la infraestructura del Datacenter es acompañada por el desempeño que poseen los servidores de granjas, ya que su capacidad y escalabilidad brindan seguridad al entorno para cada una de las aplicaciones centralizadas. La infraestructura de la red de IP inteligente provee al usuario seguridad y optimización para poder acceder a aplicaciones y a comunicaciones confiables de alta velocidad entre los servidores granjas y los recursos de computación agrupados en aplicaciones. El Datacenter posee una infraestructura de red inteligente IP gracias al desempeño de los switch multilayer o multicapa. Estos equipos tienen la posibilidad de poder conmutar en capa 2 enlaces de datos trabajando direcciones físicas MAC o bien conmutar en capa 3 capa red donde se manejan direcciones Lógicas o IPs. El diseño del Datacenter posee innovaciones de nueva generación como por ejemplo alta densidad cableada Gigabit ethernet y 10 Gigabit ethernet. Esta tecnología es de alta disponibilidad para el desempeño de las aplicaciones que requieren grandes capacidades de anchos de banda sobre hilos de cobre. Estas plataformas son la base de la consolidación y la virtualización, suministrando ambientes aislados, y seguros para cada aplicación en su servidor sobre una única infraestructura de conmutación física.

Estas plataformas cubren las demandas rigurosas para la flexibilidad, disponibilidad y el rendimiento actual. Así también su diseño modular permite actualizar y respaldar futuras tecnologías con una baja tasa de interrupción. La habilidad para integrar servicios inteligentes esenciales como cortafuegos, protección de instrucción, servicio de balanceo de carga y seguridad en la capa de socket **SSL**, hace que el diseño de la infraestructura requiera un análisis previo sobre los servicios a brindar. La forma de implantar estos servicios a través de los nuevos paradigmas de las tecnologías de sistemas de información hace que sea todo un reto para los ingenieros encargados del proyecto. En conclusión, esta capa centraliza, dirige y controla servicios inteligentes sobre las aplicaciones que corren en entornos heterogéneos.

Paradigma de la computación de alto rendimiento HPC

Agrupar servidores de baja gama, para correr aplicaciones computacionalmente complejas, es un hecho que vemos día a día y, con la

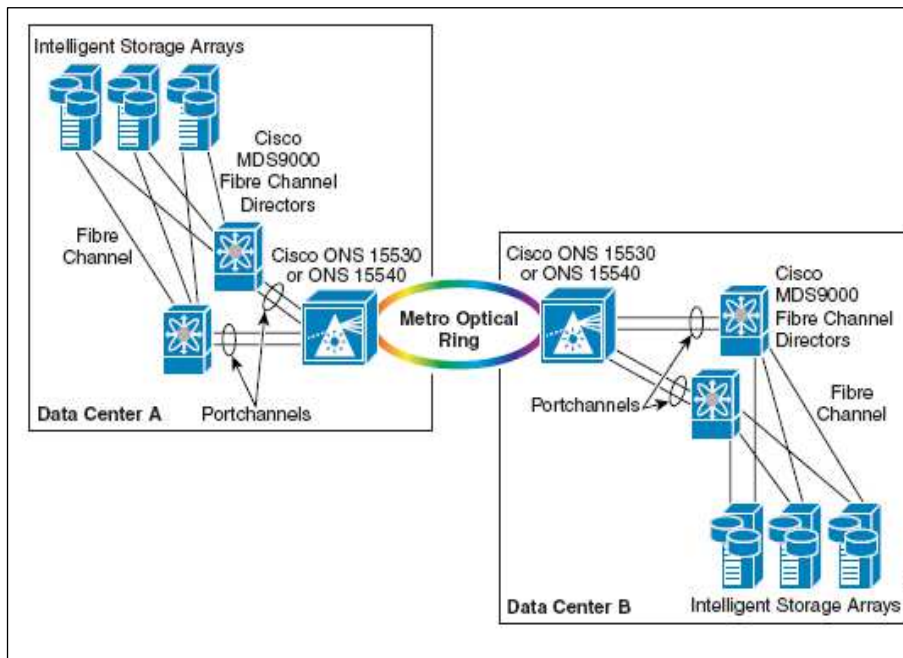
llegada de la tecnología clustering la alta performance, está al alcance de todos. Las empresas hoy en día necesitan de esta técnica ya que sus aplicaciones comerciales actuales de alta performance necesitan tecnología que pueda procesar datos de forma económica con un rendimiento determinado y que posibilite la escalabilidad de procesamiento. HPC Clustering son grupos de servidores comunes que operan un software que permite el procesamiento distribuido paralelo de una aplicación en múltiples nodos físicos. Una característica destacable HPC es el alto volumen de datos que manejan y su baja latencia. Básicamente un HPC son dos o más computadoras que computan un solo proceso o que realizan una sola tarea crítica, unos de los grandes aportes de este paradigma es por ejemplo simular a través de ecuaciones diferenciales de alta complejidad el cambio climático que está viviendo hoy en día nuestro planeta tierra. La tecnología Ethernet e InfiniBand proveen a los servidores y equipos de comunicaciones tecnología de interconexión fiable, de gran rendimiento en disponibilidad de ancho de banda y baja latencia de red requerida bajo demanda. En conclusión la tecnología de clúster es un paradigma digno de ser implementado en un Datacenter de primera tecnología.

Evolución de la tecnología SAN

Los requerimiento en almacenamiento están en constante crecimiento, por ello las industria de almacenamiento directo DAS es absorbida por la nueva tecnología SAN, que provee una tecnología de almacenamiento escalable e inteligente. La tecnología SAN es un híbrido de hardware y software disponible para la consolidación de almacenamiento, compartiendo, accediendo, replicando y administrando infraestructura de red de almacenamiento. Los switch multicapa de nueva generación denominados **MDS 9000** de la marca Cisco brindan un entorno avanzado de administración, esta tecnología evolucionó a partir de una mejora de las LAN Virtuales o Vlan protegidas a través de un canal de comunicación seguro brindado por el protocolo **IPsec**.

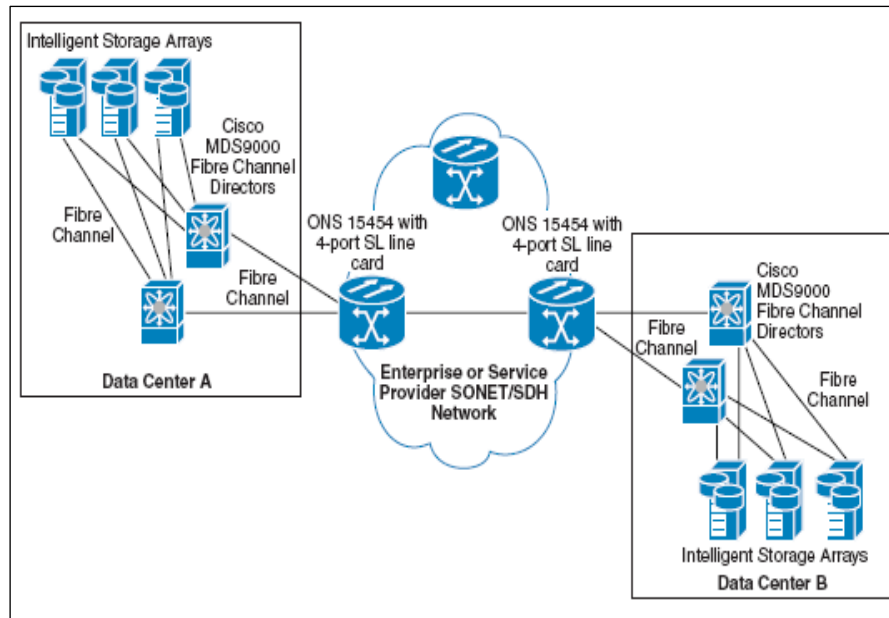
Topologías de soluciones SAN - Replicación de la información - Ejemplos

Solución: Anillo de óptico.

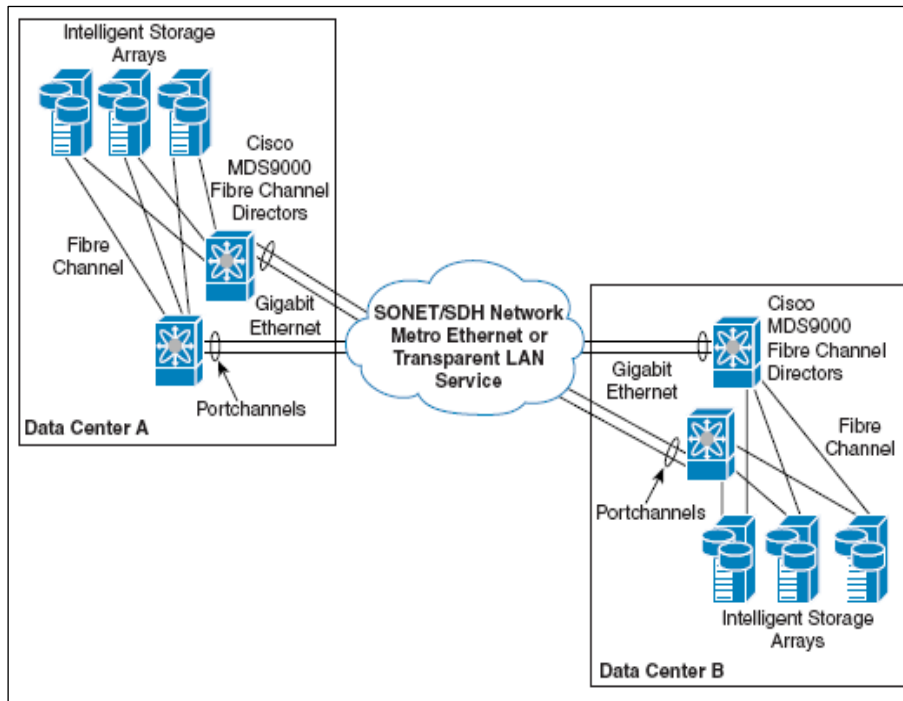


Las redes ópticas, como DWDM suministran a la red, latencias más bajas de replicación de datos.

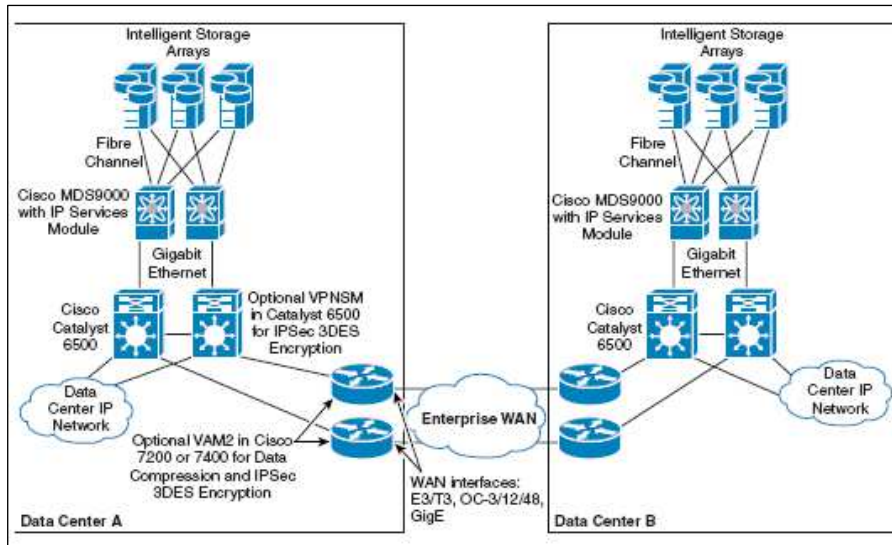
Solución: FIBER CHANNEL sobre SONET/SDH.



Solución: FCIP Transporte sobre SONET/SDH, METROETHERNET o LAN TRANSPARENTE.



Solución: FCIP Transporte sobre servicios WAN.



Canal de fibra

El canal de fibra es una tecnología adoptada para las redes de almacenamiento disponible en velocidades de 1 Gb/s y posteriormente 2, 4, 8 Gb/s. Hoy es un estándar en redes SAN la señalización del canal de fibra y puede funcionar tanto sobre pares de cobre como sobre los cables de fibra óptica. El protocolo de canal de fibra FCP es el protocolo de interfaz de SCSI sobre Fibre Channel.

Topología del enlace de fibra

Un enlace de canal de fibra consiste en dos fibras unidireccionales que transmiten en direcciones opuestas, y cada fibra está unida a un puerto transmisor TX y a un puerto receptor RX.

Dentro de las topologías podemos reconocer tres de ellas que son:

- *Fabric (FC-SW).*
- *Loop (FC-AL).*

- *Point to Point (FC-P2P).*

Bus de comunicaciones infiniband

Es un bus de comunicaciones serie de alta velocidad diseñado para conexiones internas y externas. Infiniband usa un bus serie bidireccional de tal manera que evita los problemas típicos asociados a buses paralelos en largas distancias. A pesar de ser una conexión serie posee una velocidad nominal 2.5 GB/s en cada dirección por enlace, además de esto tiene la capacidad de soportar hasta cuatro veces su capacidad nominal en la transferencia de datos, gracias a una codificación 8B/10B con lo que cada 10 Bits enviados solo 8 son de datos. La gran exigencia del ancho de banda como clúster de computadoras, y la interconexión de redes hace que sea una solución aplicable a la industria.

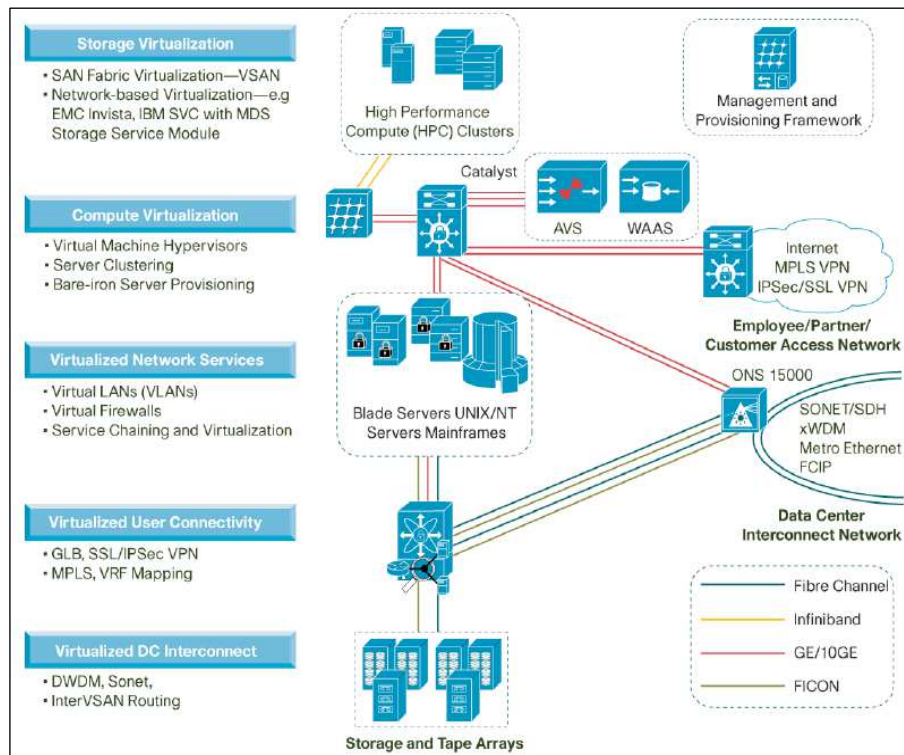
Gráfica: Interfaz infiniband.



Virtualización del Datacenter

El paso siguiente de la consolidación es la virtualización del Datacenter, que permite a los directores crear una capa de abstracción entre aplicaciones. La virtualización es la creación de una entidad lógica basadas en entidades físicas múltiples o, por otra parte, la creación de muchas entidades lógicas basadas en una entidad física. Una entidad puede ser la computación, el almacenamiento, la red, o los recursos de aplicación. La virtualización resulta en varios beneficios incluyendo la mejor utilización de recursos, el impacto aprovisionamiento y el reducido mantenimiento planeado. Grupos de trabajo, cada una con derechos de acceso para aplicaciones específicas y servicios. La virtualización es asumida en todo el ámbito del Datacenter. Las típicas tecnologías de virtualización de la red incluyen VLANs. Los PVC de un enlace WAN, Frame Relay, indica el camino a seguir a un paquete hasta llegar a su destino.

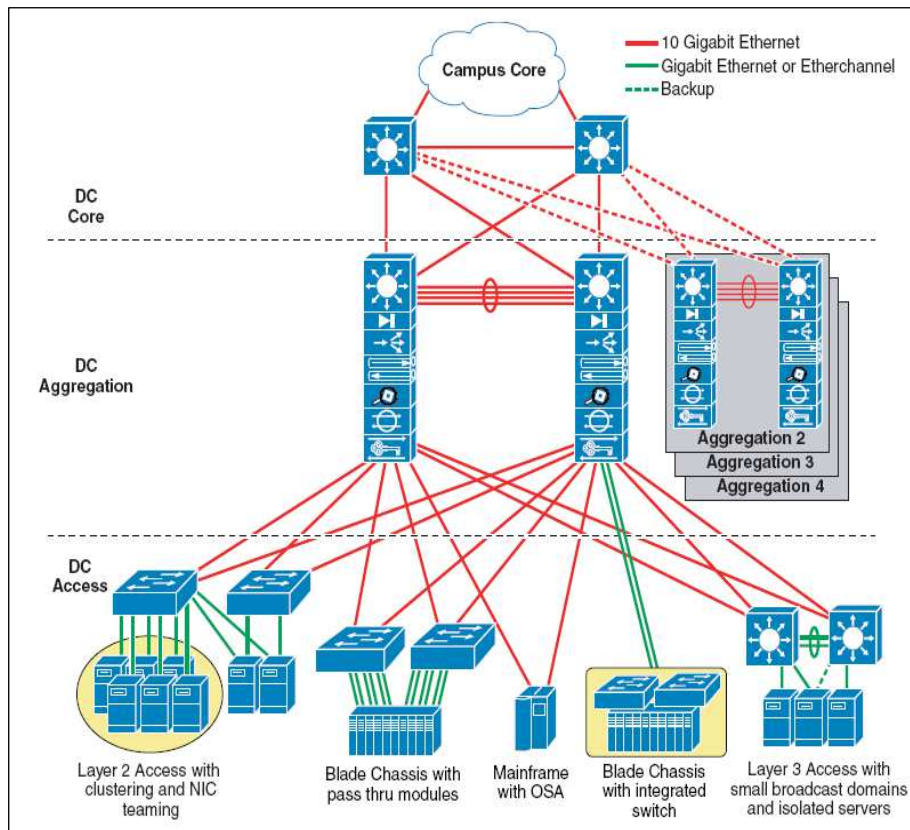
Gráfica: Virtualización del Datacenter.



Modelo de un Datacenter Multi-capa

El modelo de Datacenter de varios niveles de datos es un diseño común que define grados de servicios lógicos, entre ellos, direccionado web, funcionalidad de base de datos, etc. El modelo de varios niveles usa servicios de la red para proveer optimización de aplicaciones y seguridad.

Gráfica: Datacenter Multi-Capa.



Integración de servidores Blade

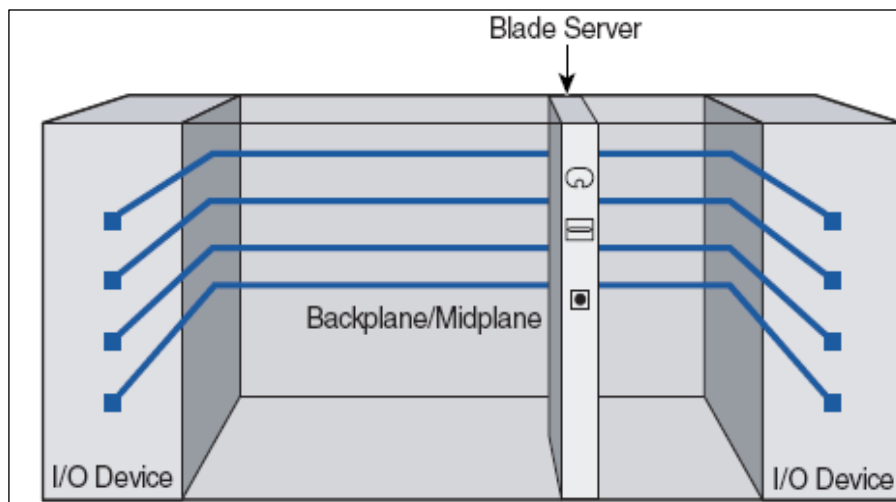
Los sistemas Blade son lo más reciente en plataforma de servidores que aparecen en el Datacenter. La tecnología basada en Blade permite colocar en un espacio reducido instancias múltiples de hardware independiente. Idealmente este tipo de tecnologías permiten, entre otras cosas, la reducción de espacio, la administración en lo que respecta a hardware (ubicaciones), y entre sus bondades podemos citar aquellas arquitecturas que presentan crecimientos inherentemente horizontales. La capacidad de apilar horizontalmente posibilita a esta tecnología a incursionar en cualquiera de los terrenos de las aplicaciones usadas actualmente en el mercado.

Los Datacenter buscan los beneficios que esta nueva plataforma puede proporcionar en relación con la potencia, el enfriamiento, y el servicio de consolidación. Los sistemas Blade permiten que interfaces incorporadas controlen la circulación del tráfico entre los servidores. Los sistemas Blade poseen variedades de interfaces de comunicaciones, incluyendo:

- Interfaces Ethernet incorporados (como los módulos Ethernet 10/100/1000Mb).
- Interfaces infiniband.
- Interfaces de fibra.

La estructura física reduce el número de cables requerido por cada servidor y provee un nivel de redundancia física de la red, controladores de interfaz (NICs) y la E/S conectan a una red de dispositivos. Los módulos de procesamiento de datos están separados de los módulos de I/O, y las placas CPU escalan independientemente a la energía del procesamiento requerido.

Gráfica: Sistemas de interconexión de servidores Blade.



Gráfica: Vista de un chasis de alojamiento.



Gráfica: Chasis Industrial de 19 Pulgadas (1RU).



Este tipo de chasis puede albergar una placa madre estándar así como también uno o varios discos duros, IDEs, SCSIs y ATAs seriales. Sin embargo, debido a que la cubierta no es muy gruesa, se recomienda que la placa madre incluya la mayor cantidad posible de periféricos de entrada y salida (placa de video, tarjeta SCSI, RAIDs, tarjetas de red, etc.), además, el ventilador y el radiador del procesador tienen una forma especial para caber en la cubierta. Casi siempre llevan una etiqueta que dice ventilador y radiador para cubierta de 1U.

Reducción del espacio, un concepto de consolidación

La reducción de espacio en un Datacenter es un tipo de consolidación, ya que puede ser el disparador para cualquier emprendimiento de reducción de instancias físicas o lógicas. Para tal fin, existen tecnologías que permiten en un espacio reducido diseñar soluciones para el ofrecimiento de servicios. Tal es el caso de las tecnologías basadas en Blades o los centros de datos móviles (Black Box). En ambos casos la idea fundamental es el ahorro de espacio, consolidando, múltiples entidades en un espacio reducido con ahorros importantes en el consumo de energía y menor calentamiento, lo cual

desemboca en menores costos de enfriamiento. El diseño de un Datacenter móvil está pensado para empresas que requieran continuar con el procesamiento de datos en contingencias ante desastres naturales, proyectos de procesamiento temporal, proyectos de migración de datos, etc.

El concepto de Datacenter móvil

Es una tendencia dinámica que permite llevar a cabo proyectos en muy corto plazo y con altos beneficios en lo que respecta a poder de cómputo y optimización del espacio físico, además se beneficia por las nuevas técnicas de enfriamiento forzado por agua a través de esquemas in-row, lo cual hace que no sea necesario la distribución clásica de pasillos frío y caliente. Este nuevo esquema de consolidación se realiza en contenedores especialmente diseñados para tal fin, y se puede estimar que el ahorro de espacio puede rondar en un cociente de 4:1 respecto al espacio ocupado por un Datacenter convencional, con capacidades similares de cómputo y con ahorros de energía de hasta un 40%, una de las ventajas competitivas de esta solución arquitectónica tecnológica a tener en cuenta. Estas estructuras móviles cumplen los mismos estándares de exigencia que los sistemas convencionales, con un detalle particular en la eficiencia energética en el proceso de refrigeración de los equipos.

Beneficios de esta tecnología:

- Escalabilidad: Dado su diseño modular, el crecimiento es un punto importante porque si se requiere mayor capacidad, solo restaría agregar módulos adicionales con su energía y climatización independiente, lo que evita operaciones complejas de migración.
- Eficiencia: Dependiendo de la cantidad de módulos y de la carga de los equipos en potencia consumida, con el sistema inteligente de climatización de áreas, se adapta al crecimiento dinámicamente.
- Economía: Al ser modular no se invierte en capacidad o espacio que no se usará, la optimización del uso de la energía y el enfriamiento conlleva a economías de costos operativos.
- Rapidez en la puesta operativo: Con un Datacenter móvil, se evitan los costos y retardos iniciales de tener que pasar por el proceso de

construcción de obras civiles y esto repercute en el desarrollo de un proyecto de esta envergadura. El Datacenter móvil está disponible en un tiempo mucho menor.

CAPÍTULO 10 - RRHH

Equipos de trabajo

La administración será realizada por personal con experiencia mínima de dos años en procesos de implementación y/o adecuación y/o remodelación de Datacenters. El proyecto debe tener un Director de Proyecto, quien deberá ser un profesional Ingeniero electrónico o eléctrico o de sistemas, con mínimo dos (2) años de experiencia en la gerencia de proyectos de infraestructura de tecnología, quien liderará los aspectos de la ejecución.

Experiencia del equipo de trabajo asignado al proyecto

Personal que posea la siguiente experiencia:

1. Profesional con experiencia en redes de datos

Perfil:

- 1.1. Deberá ser técnico o profesional ingeniero, en electrónica o eléctrico o de sistemas.
- 1.2. Deberá tener mínimo dos (2) años de experiencia.
- 1.3. Deberá ser certificado por el fabricante o el distribuidor autorizado del fabricante en la instalación y configuración de equipos de comunicaciones y/o telecomunicaciones.

2. Profesional con experiencia en cableado estructurado

Perfil:

- 2.1. Deberá ser técnico o profesional ingeniero, en electrónica o eléctrico o de sistemas.

2.2. Deberá tener mínimo dos (2) años de experiencia.

2.3. Deberá ser certificado por el fabricante o el distribuidor autorizado en la instalación de cableado estructurado de voz, datos y video.

3. Profesional con experiencia en redes eléctricas

Perfil:

3.1. Deberá ser un profesional ingeniero electrónico o eléctrico.

3.2. Deberá tener mínimo dos (2) años de experiencia.

3.3. Deberá ser certificado por el fabricante o el distribuidor autorizado en la instalación y mantenimiento del sistema **UPS**.

4. Profesional con experiencia en aires acondicionados de precisión

Perfil:

4.1. Deberá ser un profesional ingeniero mecánico, electrónico o eléctrico.

4.2. Deberá tener mínimo dos (2) años de experiencia.

4.3. Deberá ser certificado por el fabricante o el distribuidor autorizado en la implementación de soluciones de aires acondicionados de precisión.

El personal propuesto deberá tener la dedicación necesaria para la ejecución del proyecto y el cumplimiento del objeto propuesto dentro de los plazos definidos.

Capacitación de recursos humanos

Proyectos de capacitación

- ✓ Un curso de capacitación y transferencia de conocimientos en la administración y operación de los sistemas de aire acondicionado.
- ✓ Un curso de capacitación para la administración y operación del sistema UPS.

- ✓ Un curso de capacitación y transferencia de conocimientos en la administración y operación de los sistemas de detección y extinción de incendios.
- ✓ Un curso de capacitación y transferencia de conocimientos en la administración y operación del sistema general.

Plan de trabajo

Incluir un cronograma detallado de la secuencia de actividades a realizar en la ejecución del proyecto:

- Diseño detallado de la solución integral propuesta.
- Plan de entrega de equipos y demás elementos requeridos.
- Plan de adecuación e instalación de las redes eléctricas y de datos.
- Plan de realización de obras civiles.
- Plan de reubicación de equipos y demás elementos existentes.
- Plan de instalación de equipos.
- Puesta en funcionamiento de la solución.
- Protocolo de pruebas requeridas.
- Plan de capacitación y transferencia de conocimientos.

Dicho plan de trabajo deberá incluir los responsables y tiempos para cada una de las etapas incluidas en el proyecto. Durante el mismo lapso, previa coordinación entre la supervisión del contrato y el contratista, se aprobará el mencionado plan de trabajo.

Además se deberá presentar y entregar un plan de calidad que contemple como mínimo las siguientes actividades del proyecto:

- Esquema de escalamiento de problemas y decisiones.
- Plan de contingencias.
- Plan de reuniones de seguimiento y evaluación.
- Condiciones y normas generales.

Las pruebas serán realizadas antes de la puesta en funcionamiento del sistema operando en su totalidad.

CAPÍTULO 11 - Documentación

Documentación

La documentación del proyecto se deberá entregar en idioma español (en original y copia) impresa y en medio magnético que incluya como mínimo:

1. Manuales de usuario (operación del sistema) y técnico, deben enunciar los estándares utilizados para tales documentos.
2. Manual de contingencia e integridad de los elementos del centro de cómputo que contenga una descripción de los procedimientos para minimizar los riesgos de seguridad y garantizar la continuidad de los procesos sistematizados.
3. Manual de usuario y referencia de todas las herramientas de usuario final que complementan la solución.
4. Planos digitalizados e identificación de todos los sistemas implementados.
5. Recorrido y especificaciones de todo el sistema porta cables, indicando porcentajes de utilización.
6. Sistema Eléctrico.

6.1.1. Localización y diagrama unificado de todos los tableros de control de circuitos eléctricos regulados y no regulados.

6.1.2. Identificación y recorrido de las acometidas de entrada y salida del sistema UPS.

6.1.3. Diseño y memorias de cálculo del sistema de puesta a tierra, al igual que los planos de recorrido de la localización en planta de este sistema y sus componentes, donde se ubiquen e identifiquen rutas de cableado, barrajes, electrodos (varillas) y cajas de inspección.

7. Sistema de cableado estructurado

7.1.1. Copia de los documentos de registro y certificación del fabricante.

7.1.2. Diagrama de conformación del subsistema de administración.

7.1.3. Identificación y recorrido del subsistema horizontal.

7.1.4. Identificación del subsistema de área de trabajo.

8. Sistema de detección y extinción de incendios

8.1.1. Se debe entregar el cálculo del sistema de extinción generadas por un software especializado y homologado, según el fabricante.

8.1.2. Se debe entregar los manuales de operación y manejo del sistema, al igual que los planos de localización del cableado y los elementos del sistema.

9. Sistema de seguridad y control de acceso

9.1.1. Se debe entregar los manuales de operación y manejo del sistema del control de acceso, ubicación del cableado.

Garantías del equipamiento

Cada uno de los equipos (aires acondicionados, sistemas de UPS, consolas de administración, cámaras de seguridad, sistema de detección y extinción de incendios) deben ser entregados con los respectivos manuales técnicos, manuales de operación, cables de potencia, interfaces de conexión y software de configuración en medios magnéticos para los equipos que así lo requieran. Identificación mediante placas, todas las áreas de trabajo y espacios del Datacenter. Efectuar rotulación, marcación e identificación de puntos estratégicos tales como: Prohibiciones de comer, fumar o beber, salidas, restricción de acceso, corriente eléctrica peligrosa, ubicación de estaciones, y activación de los sistemas de detección y extinción de fuego, y aparte de todos los componentes que comprenden la solución, entre otros. Para el cumplimiento de las actividades de adecuación y mejoramiento del centro de cómputo requeridas, deberá tener en cuenta y cumplir con lo establecido en las normas vigentes.

Aspectos técnicos adicionales

Los elementos del cableado estructurado ofrecidos deberán ajustarse a lo estipulado en las normas y estándares:

- EIA/TIA-568B.1 Standard Commercial Building Telecommunications Wiring.
- STANDARD EIA/TIA-568B.2 100-ohm twisted-pair cabling standard.
- EIA/TIA-568B.2-1 Category 6.
- EIA/TIA-568B.3 Optical fiber cabling Standard.
- EIA/TIA-569A Commercial Building Standard for Telecommunications pathways and spaces.
- EIA/TIA-606A The Administration Standard for the Telecommunications Infrastructure of Commercial Buildings.
- EIA/TIA-607 Commercial Building and Bonding Requirements for Telecommunications.

- ISO/IEC-11801 The international Organization for Standardization.
- International Electro technical Commission.
- Specifies generic cabling for use within commercial premises. Single or multiple buildings on a campus.

Resultados obtenidos

Este trabajo tuvo como resultado la integración de distintos sistemas en un contexto muy amplio. Desde el punto de vista teórico se integraron distintos paradigmas que brindan la posibilidad de operaciones óptimas en un Datacenter.

Desde el punto de vista práctico se citaron una serie de soluciones disponibles en el mercado hasta el día de la fecha, gracias a los estándares definidos para cada caso particular.

El estándar internacional **EIA/TIA-942** que define los lineamientos generales de cómo diseñar un Datacenter, nos da las pautas necesarias para integrar distintas soluciones tecnológicas que están disponibles en el mercado.

La barrera entre el hardware y el software parece no tener límite con el paradigma de la virtualización que brinda soluciones de las más amplias necesidades.

Desde mi punto de vista, este trabajo cumplió con su cometido de hacer una breve reseña del diseño, de la implementación y puesta en funcionamiento de un Datacenter.

Conclusiones

Los Datacenter del mañana deben diseñarse con los estándares de facto, de esta manera se logra una ventaja competitiva tecnológica invaluable con los nuevos paradigmas tecnológicos. Nuestro único reto es realizar la reingeniería correspondiente, logrando así una fusión completa entre lo que tenemos funcionando y lo que depara el futuro en demanda de soluciones tecnológicas.

¿Qué es un sistema UPS?

Un Sistema **UPS** viene de la sigla en inglés (Uninterruptible Power Supply) que significa Sistema de Energía Ininterrumpida, el cual ha sido diseñado principalmente para proteger de cortes de energía a equipos de misión crítica. Asimismo este equipo ha sido diseñado para protegerlos de los problemas eléctricos más comunes. Es por esto que existen diversas tecnologías de UPS, las cuales se diferencian por su grado de protección que otorgan cada uno.

¿Cuántos tipos de sistemas UPS, existen en el mercado?

Existen varias tecnologías, pero actualmente las más usadas son las siguientes:

1. UPS Off Line o Standby: Equipo diseñado para proteger aplicaciones pequeñas o de poca criticidad como por ejemplo PC's, fax, periféricos. Provee de protección básica ante problemas eléctricos cortes de energía y pequeñas variaciones de voltaje. No incluyen regulador de voltaje.
2. UPS Line-Interactiva: Diseñadas para pequeñas redes LAN de computación y solo recomendado en lugares donde no existan gran cantidad de problemas de energía. Ofrece una solución intermedia de protección ante los problemas eléctricos. Presenta una gran eficiencia. Estos equipos poseen reguladores de voltaje, los cuales permiten mantener un rango aceptable para las cargas PC.
3. UPS Online: Por su principio de funcionamiento este equipo ha sido diseñado para entregar una energía limpia de perturbaciones eléctricas. Cabe destacar que un equipo Online o True Online doble conversión significa que la energía que recibe la carga es totalmente generada directamente por el sistema UPS. El equipo Online se compone principalmente de tres elementos, Rectificador/ Cargador

(AC-DC), banco de baterías (DC), Inversor (DC-AC). Como principio de funcionamiento el equipo Online recibe la energía de la red eléctrica (AC) y pasa a través de un rectificador el cual la transforma en corriente continua (DC) (primera conversión), alimentado un bus de continua que al igual se encarga de mantener cargada las baterías que se encuentran en espera que ocurra un corte de energía para automáticamente entregar energía, luego la energía es nuevamente convertida desde corriente continua (DC) a corriente alterna (AC) (segunda conversión), a través de un Inversor, alimentando así a la carga crítica. Con lo anterior se puede garantizar que la carga o consumo crítico va a recibir una energía totalmente libre de perturbaciones. Cabe destacar que dentro de los equipos Online existen distintas configuraciones:

- Monofásicas / Monofásicas: 1/1.
- Trifásicas / Monofásicas: 3/1.
- Trifásicas / Trifásicas: 3/3.

¿Qué tipo de sistema UPS, debo considerar para mi Datacenter?

Lo más importante a considerar es el tipo de carga, mientras que lo criticable es que ésta sea para el proceso involucrado. De acuerdo a esto se puede definir el tipo de tecnología a utilizar. Algunos puntos a considerar: potencia de consumo, esta pueda estar dada en Amperes(A), Watts(w), o VA. Voltaje de consumo, 110, 220V, pueden existir otros voltajes pero son menos solicitados.

¿Qué significa autonomía o tiempo de respaldo en un sistema UPS?

Autonomía o tiempo de respaldo es lo mismo y significa el tiempo por el que permanece entregando energía la UPS hacia la carga conectada después de un corte de energía que haya sido detectada por la misma (cortes en la red eléctrica). Normalmente este tiempo está dado entre 5 y 15 minutos como estándar. Pudiendo obtenerse mayor autonomía con bancos adicionales de baterías de acuerdo a cada necesidad.

¿Qué mantenimiento debe tener un sistema UPS?

Este punto es muy importante ya que se debe poner especial atención al proveedor que la representa o distribuya y confirmar si cuenta con Servicio Técnico permanente. Uno de los puntos importantes a considerar es que la empresa cuente con atención de 7 x 24 horas y con repuestos legítimos de fábrica. Después de confirmado esto, se puede decir al respecto del tipo de mantenimiento que debe tener un equipo UPS. Principalmente al equipo UPS se le deben realizar mantenimientos preventivos para poder confirmar si es que alguna de las baterías del banco está con principios de deterioro (baja impedancia) o cortocircuito, previniendo así que cuando ocurra un corte de energía el sistema de baterías no responda y finalmente la carga quede sin respaldo.

Otro punto es verificar parámetros de operación del equipo.

¿Qué significa un sistema redundante?

Significa tener la disponibilidad de que existe otro equipo, dispositivo o elemento que respalde o reemplace en caso de que falle la unidad principal. En el caso de los sistemas eléctricos de respaldo de energía, existen varios puntos que pueden tener alguna posibilidad de falla y es por esto que un buen proyecto debe ser capaz de que la disponibilidad del sistema esté por sobre el 99.99% de UpTime. Actualmente podemos contar con redundancia a nivel de generación, distribución y cargas, pero en gran parte los problemas eléctricos suceden, con mayor frecuencia, a nivel de la distribución de la energía, ya que los sistemas de respaldo cada vez son más confiables. Es por esto que existen varios tipos de redundancia.

¿Es determinante la condición ambiental de operación para los equipos de respaldo dentro del Datacenter?

Aquí debe considerarse la temperatura, la humedad y la temperatura ambiente controlada. Estos factores pueden ser determinantes en relación con el lugar físico de operación de la unidad.

Problemas típicos que pueden ocurrir en un sistema de UPS

- **Apagón (Blackout):** Es la pérdida total del suministro eléctrico. Puede ser causado por diversos eventos; relámpagos, caídas de las líneas de energía, sobre-demandas, accidentes y desastres naturales. Puede causar daños en el equipo electrónico (hardware), pérdida de datos, o caída total del sistema.
- **Bajo voltaje momentáneo (Sag):** Es la caída momentánea de voltaje, generada por el arranque de grandes cargas, encendido de maquinaria pesada y fallas de equipos. Se presenta de manera similar a los apagones. El bajo voltaje momentáneo puede causar daños al hardware.
- **Alto voltaje momentáneo (Surge):** También conocido como pico. Los picos pueden ser producidos por una rápida reducción de las cargas, cuando el equipo pesado es apagado por voltajes que van por arriba del 110 % del nominal. Los resultados pueden ser daños al hardware.
- **Bajo voltaje sostenido (Undervoltage):** Bajo voltaje sostenido en la línea por periodos extendidos de unos cuantos minutos, hasta días. Puede ser causado por una reducción intencional del voltaje para conservar energía durante los periodos de mayor demanda. El bajo voltaje sostenido puede causar daños a los equipos.
- **Sobre voltaje (Overvoltage):** Sobre voltaje en la línea por periodos largos. Puede ser causado por un relámpago e incrementar el voltaje de la línea hasta 6000 volts en exceso. El sobre voltaje casi siempre ocasiona pérdida de la información y/o daño del hardware.
- **Ruido eléctrico (Line Noise):** Significa interferencia de alta frecuencia causada por RFI o EMI. Puede ser causada por interferencia producida por transmisores, máquinas de soldar, impresoras, relámpagos, etc., e introduce errores en los programas/archivos, así como daños a los componentes electrónicos.
- **Variación de frecuencia (Frequency Variation):** Se refiere a un cambio en la estabilidad de la frecuencia. Resultado de un generador o

pequeños sitios de co-generación siendo cargados o descargados. La variación de frecuencia puede causar un funcionamiento errático de los equipos, pérdida de información, caídas del sistema y equipos dañados.

- Transiente (Switching Transient): Es la caída instantánea del voltaje en el rango de los nanosegundos. La duración normal es más corta que un pico. Puede originar comportamiento extraño del equipo de cómputo y coloca estrés en los componentes electrónicos quedando propensos a fallas prematuras.
- Distorsión armónica (Harmonic Distortion): Es distorsión de la forma de onda normal. Es causada por cargas no lineales conectadas a la misma red que los equipos de cómputo y/o aplicaciones críticas. Motores, copiadoras, máquinas de fax, etc., son ejemplos de cargas no lineales. Puede provocar sobrecalentamiento en los equipos de cómputo, errores de comunicación y daño del hardware.

Consecuencias de una mal suministro energético

Un mal suministro de energía eléctrica afecta el funcionamiento del Datacenter, ya que:

- 1.- Destruye la información: Una variación en el flujo de energía eléctrica puede dañar datos confidenciales, documentos de operación diaria, estadísticas e información financiera.
- 2.- Daño la infraestructura: Cada variación en el voltaje va disminuyendo la vida útil de: computadoras personales, servidores, controles computarizados, estaciones de trabajo y redes entre otros.
- 3.- Genera estrés: Las constantes interrupciones en la continuidad laboral y consecuente caída de productividad genera estrés y desmotivación en los recursos humanos.
- 4.- Afecta la productividad: Las interrupciones de operación de las compañías afectan la productividad y la generación de ingresos.

5.- Genera pérdidas: Los problemas eléctricos interrumpen la continuidad de operación, ocasionando importantes pérdidas en la empresa.

Sistema de UPS con tecnología ON-LINE

El funcionamiento de los UPS de tecnología On-Line se basa en que la señal de alimentación es rectificadora, obteniéndose una señal de voltaje continua. Esta señal carga el banco de baterías del equipo hasta que éstas llegan a su voltaje de flotación. Simultáneamente, dicha señal alimenta el inversor del UPS el cual, gracias al sistema de control del equipo y una modulación PWM, genera una señal de voltaje alterna, de gran estabilidad y libre de perturbaciones para alimentar las cargas.

Por esta razón, se puede decir que cuando un UPS de este tipo respalda una carga, ésta se encuentra completamente aislada de las anomalías que puedan estar presentes en la red eléctrica comercial, ya que recibe una señal de alimentación generada permanentemente por el inversor del UPS (lo que no quiere decir que esta señal sea entregada por el banco interno de baterías). Cabe hacer notar que las baterías sólo funcionan en caso de ausencia de energía u otra anomalía que provoque que el UPS entre en respaldo.

Algunas características generales de la tecnología

- Los UPS On Line, están preparados y diseñados para operar en condición de respaldo continuo, debido a que su inversor se encuentra en constante operación. En este aspecto, cuando se requieren largos tiempos de respaldo, es importante que el cargador de baterías sea bien dimensionado.
- El comportamiento de los UPS Online es muy adecuado al operar bajo condiciones eléctricas inestables. Una situación típica de falla eléctrica es la variación de voltaje. En este caso, un UPS On Line responde normalmente debido a que están diseñados con márgenes de voltaje de entrada más amplios, de modo que el equipo pueda operar bajo condiciones normales la mayor parte del tiempo sin

requerir el uso de baterías, como ocurre con otras tecnologías (ver figura).

- En general, se puede decir que la tecnología On line reduce la distorsión de armónicos hacia la red. Dependiendo del tipo de carga respaldada, sabiendo que el rectificador genera armónicos y la adición de filtros en algunos UPS, se puede tener menor cantidad de armónicos que los asociados a la carga respaldada (para la red comercial, la carga es el rectificador del UPS).
- Cuando se presenta una anomalía y el equipo está en modo respaldo, un banco de condensadores se encarga de seguir suministrando voltaje al inversor, de manera de no producir micro cortes que afecten el funcionamiento de las cargas, en especial cuando éstas son sensibles y de gran importancia para el funcionamiento de una corporación. Estos micro cortes (anomalía presente en la red) pueden, en algunos casos, producir corrupción de datos en procesos computacionales y daños en equipos.

A continuación se muestran algunos esquemas de funcionamiento de un UPS On-Line doble conversión.

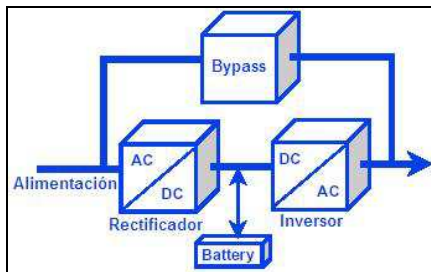


Figura 1.- Esquema general del UPS On Line.

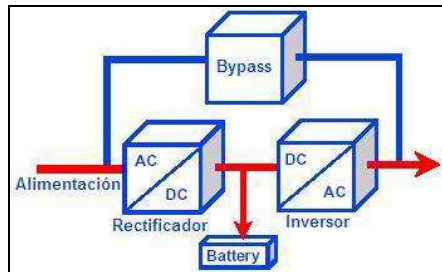


Figura 2.- UPS funcionando en estado normal.

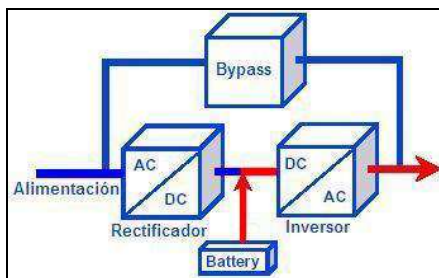


Figura 3.- Sistema funcionando en estado de respaldo (sin tiempo de transferencia).

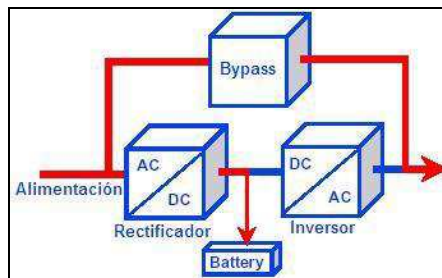


Figura 4.- UPS operando en bypass estático y cargando.

Referencias

Sitios web

- www.cisco.com
- www.cisco.com.ar
- www.ciscoredaccionvirtual.com.ar
- www.sun.com
- www.sun.com/blueprints
- www.sun.com/blackbox
- www.nfpa.org
- www.wikipedia.com
- www.ieee.org
- www.docs.sun.com
- www.sun.com/service/refresh/datacenter.html
- www.apc.com
- www.upsite.com
- www.cisco.com/go/dcservices
- www.ISO27000.es

Bibliografía

- José Manuel Díaz. Fundamentos De Redes Inalámbricas. Companion Guide Cisco System Cisco Networking Academy Program Año 2006.
- Vito Amato. Cisco Networking Academy Program. Guía Del Segundo Año 2001.
- Vito Amato. Cisco Networking Academy Program. Guía Del Tercer Año 2001.
- Steve McQuerry, CCNA. Interconexión De Dispositivos De Red Cisco. Libro Auto estudio CCNA Segunda Edición. Año 2004.
- Héctor Riso – Omar Saibene. Redes De Telecomunicaciones. Año 2003.