Germán Pacio

Data Centers hoy

Protección y administración de datos en la empresa

Apoyo en la

Alfaomega

Data Centers hoy

Germán Pacio

Data Centers hoy

Germán Pacio

Alfaomega

Buenos Aires • Bogotá • México, D.F. • Santiago de Chile

Pacio, Germán

Data Centers hoy. - 1a ed. - Buenos Aires: Alfaomega Grupo Editor Argentino, 2014.

272 p. ; 23x17 cm.

ISBN 978-987-1609-41-3

1. Informática. I. Título

CDD 005.3

Queda prohibida la reproducción total o parcial de esta obra, su tratamiento informático y/o la transmisión por cualquier otra forma o medio sin autorización escrita de Alfaomega Grupo Editor Argentino S. A.

Edición: Damián Fernández
Corrección de estilo y diagramación: Adriana Scaglione
Revisión de armado: Vanesa García
Diseño de tapa: Iris Biaggini

Internet: http://www.alfaomega.com.mx
Todos los derechos reservados © 2014, por Alfaomega Grupo Editor Argentino S. A.
Paraguay 1307, PB, oficina 11
ISBN: 978-987-1609-41-3
Queda hecho el depósito que prevé la ley 11.723

NOTA IMPORTANTE: La información contenida en esta obra tiene un fin exclusivamente didáctico y, por lo tanto, no está previsto su aprovechamiento a nivel profesional o industrial. Las indicaciones técnicas y programas incluidos han sido elaborados con gran cuidado por el autor y reproducidos bajo estrictas normas de control. Alfaomega Grupo Editor Argentino S. A. no será jurídicamente responsable por errores u omisiones, daños y perjuicios que se pudieran atribuir al uso de la información comprendida en este libro, ni por la utilización indebida que pudiera dársele.

Los nombres comerciales que aparecen en este libro son marcas registradas de sus propietarios y se mencionan únicamente con fines didácticos, por lo que Alfaomega Grupo Editor Argentino S. A. no asume ninguna responsabilidad por el uso que se dé a esta información, ya que no infringe ningún derecho de registro de marca. Los datos de los ejemplos y pantallas son ficticios, a no ser que se especifique lo contrario.

Los hipervínculos a los que se hacen referencia no son necesariamente administrados por la editorial, por lo que no somos responsables de sus contenidos o de su disponibilidad en línea.

Empresas del grupo:
Argentina: Alfaomega Grupo Editor Argentino S. A.
Paraguay 1307 P.B. “11”, Buenos Aires, Argentina, C.P. 1057
Tel.: (54-11) 4811-7183 / 0887
E-mail: ventas@alfaomegaeditor.com.ar
México: Alfaomega Grupo Editor S. A. de C.V.
Pitágoras 1139, Col. Del Valle, México, D.F., México, C.P. 03100
Tel.: (52-55) 5575-5022 – Fax: (52-55) 5575-2420 / 2490. Sin costo: 01-800-020-4396
E-mail: atencionalcliente@alfaomega.com.mx
Colombia: Alfaomega Colombiana S. A. – Calle 62 N° 20-46, Bogotá, Colombia
Tel. (57-1) 7460102 - Fax: (57-1) 2100415
E-mail: cliente@alfaomega.com.co
Chile: Alfaomega Grupo Editor, S. A. Av. Providencia 1443, Oficina 24, Santiago de Chile, Chile
Tel.: (56-2) 235-4248 / 2947-5786 – Fax: (56-2) 235-5786,
E-mail: agechile@alfaomega.cl

Dedicatoria

A mi familia en general por apoyarme en todos los momentos, pero muy en especial a mi papá Eduardo por haberme transmitidos los valores que me formaron como persona y a mi mujer Paula por su amor incondicional.

Germán Pacio

Agradecimientos

A la UTN en general por haberme formado como profesional de la Ingeniería en Sistemas de Información, pero especialmente a Carlos Tomassino por su apoyo para este proyecto.

A mi hermano Lic. Gastón Pacio por su asesoramiento y colaboración en los temas de responsabilidad social empresaria.

A Damián Fernández de la Editorial Alfaomega, por haber confiado en este libro y por sus continuos consejos mejorar la calidad durante el proceso de elaboración.

Germán Pacio

Mensaje del editor

Los conocimientos son esenciales en el desempeño profesional, sin ellos es imposible lograr las habilidades para competir laboralmente. La universidad o las instituciones de formación para el trabajo ofrecen la oportunidad de adquirir conocimientos que serán aprovechados más adelante en beneficio propio y de la sociedad; el avance de la ciencia y de la técnica hace necesario actualizar continuamente esos conocimientos. Cuando se toma la decisión de embarcarse en una vida profesional, se adquiere un compromiso de por vida: mantenerse al día en los conocimientos del área u oficio que se ha decidido desempeñar.

Alfaomega tiene por misión ofrecerles a estudiantes y profesionales conocimientos actualizados dentro de lineamientos pedagógicos que faciliten su utilización y permitan desarrollar las competencias requeridas por una profesión determinada. Alfaomega espera ser su compañera profesional en este viaje de por vida por el mundo del conocimiento.

Alfaomega hace uso de los medios impresos tradicionales en combinación con las tecnologías de la información y las comunicaciones (TIC) para facilitar el aprendizaje. Libros como éste tienen su complemento en una página Web, en donde el alumno y su profesor encontrarán materiales adicionales.

Esta obra contiene numerosos gráficos, cuadros y otros recursos para despertar el interés del estudiante, y facilitarle la comprensión y apropiación del conocimiento. Cada capítulo se desarrolla con argumentos presentados en forma sencilla y estructurada claramente hacia los objetivos y metas propuestas.

Los libros de Alfaomega están diseñados para ser utilizados dentro de los procesos de enseñanza-aprendizaje, y pueden ser usados como textos para diversos cursos o como apoyo para reforzar el desarrollo profesional.

Alfaomega espera contribuir así a la formación y el desarrollo de profesionales exitosos para beneficio de la sociedad.

Sobre el autor

Ing. Germán Pacio

Es Ingeniero en Sistemas de Información, egresado de la Universidad Tecnológica Nacional. Se desempeña en el sector de IT en grandes empresas, nacionales y multinacionales de diversos rubros desde 2001 hasta la fecha. Además, está certificado por: Data Center University, de APC; MCP, de Microsoft; e ITILv3, por EXIN.

En el 2006 fue finalista del concurso organizado por la Asociación de Graduados en Sistemas de Información por su trabajo: El costo de la mala utilización de los recursos informáticos.

Blog: `www.datacentershoy.com`

Twitter: `http://twitter.com/GermanPacio`

Linkedin: `http://www.linkedin.com/pub/german-pacio/25/579/29a`

Contenido

Capítulo 1
Introducción 1
Definición de un Data Center 1
Clasificación 2
Importancia 3
Catástrofes y pérdidas 3
Tendencia evolutiva del negocio 11
Costo de la complejidad 12
Pilares 14
Capas de redundancia 14

Capítulo 2
Filosofía del diseño 21
Objetivos 21
Selección de la ubicación geográfica 22
Selección de la ubicación edilicia 24
Establecer la disponibilidad deseada 25
Planificación de elementos críticos 27
Evaluación y análisis de costos 29
Presupuesto de IT típico de una empresa 32

Capítulo 3
Componentes básicos 35
Piso técnico 35
Tipos de baldosas 37
Consideraciones para la implementación del piso técnico 39
Tamaño del Data Center 39
Racks 40
Servidores y equipos de comunicaciones 45
Monitoreo ambiental 46

Capítulo 4
Alimentación eléctrica 49
Red Eléctrica 49
Potencia eléctrica: Monofásica o Trifásica 58
Estrategias de distribución eléctrica para la optimización 59
UPS 60
Generadores 70
Problemas eléctricos frecuentes 76

Capítulo 5
Control ambiental 81
Temperatura 81
Humedad 83
Funcionamiento básico de un aire acondicionado 87
Tipos de unidades de aire acondicionado 88
Estimación calórica 93
Estrategias de refrigeración 98
Diseño de pasillos 101
Circulación del aire 103
Sensores de temperatura, humedad y mantenimiento 107

Capítulo 6
Seguridad y prevención de incendios 109
Seguridad física 109
El fuego y su clasificación 115
Etapas del fuego 116
Reducir riesgos es la salvación 116
Barreras contra incendios 119
Sistemas de extinción de incendios gaseosos 121

Sistemas de extinción de incendios líquidos 126
Análisis de daños 128

Capítulo 7
Diseño de red 131
Topologías 131
Cableado estructurado 133
Red troncal o backbone: puntos de distribución 137
Cables de red: UTP 138
Cables de red: STP 143
Cables de telefonía 143
Elementos terminales 144
Cables de fibra óptica 147
Cable coaxial 151
Transmisión inalámbrica 153
Recomendaciones de instalación 156
Etiquetación de cables 158

Capítulo 8
Organización 161
Visitas guiadas 161
Recepción de equipos 163
Medidas básicas para proteger equipos en ambientes chicos 164
Estrategias para manejo cableado 165
Estrategias de gestión de cableados 167
Definición y documentación de políticas y procedimientos 168
Nomenclatura lógica de equipos 169
Gestión del Data Center 171
Tablero de control 176
Estándares en el Data Center 177

Capítulo 9
Optimización 179
Técnicas actuales de optimización: virtualización y nube 181
Data Centers ecológicos 186
Costos 192
Desafíos actuales 194
Data Centers modulares 199
Viabilidad técnica para alojar servidores en Data Centers externos (Housing) 200
Viabilidad económica para alojar servidores en Data Centers externos (Housing) 201
Consolidación de Data Centers 201
Monitoreo centralizado 204

Capítulo 10
Continuidad del negocio 207
Ciclo de vida del plan de continuidad del negocio o BCP (Business Continuity Plan) 208
Planes para la recuperación de desastres o (DR, Disaster Recovery) 211
Implementación de un plan DR en IT 213
Nociones básicas de backup y estrategias 215
Beneficios de un DR centralizado 220
Data Center de respaldo para DR 222
Fallas comunes BCP 224

Capítulo 11
Mejores prácticas 225
Recomendaciones para construir un buen Data Center desde el inicio 225
Utilización metodología ITIL 232
Métricas de disponibilidad 234
Control ambiental 236
Administración de riesgos 237
Rol del Responsable del Data Center 243
Notificaciones de cambios en la infraestructura 243
Consejos para el verano 244
Herramientas 245
Errores comunes 246

Bibliografía 249

Prólogo

El continuo avance de la informática suele provocar, a veces, creencias equivocadas. Quienes provenimos de la primera era de esa disciplina, denominada "de las grandes computadoras", sabemos que muchas cosas han cambiado en el transcurso de las décadas, pero hay algunas que no solo han sobrevivido, sino que se han fortalecido con el continuo cambio tecnológico.

La problemática de los Data Centers es una de ellas. Estos esquemas lograron sobreponerse a la segunda era, la de los "computadores personales", donde todo se miniaturizaba; y a la tercera, la "de Internet", en que todo se distribuía. Y hoy, en la era informática que vivimos – y que denominamos "las redes sociales", una última sofisticación-, adquieren una vigencia inusitada producto sin duda de la necesaria concentración de información, lo que implica un retorno al punto de origen.

El diseño, la organización, la seguridad, la confiabilidad, la optimización y las mejores prácticas en los Data Center de hoy en día, examinados desde la perspectiva de las nuevas tecnologías y de las acciones que deben desarrollarse para asegurar su eficaz y efectivo funcionamiento, hacen necesaria su explicitación documental.

Germán Pacio es un joven profesional de los Sistemas de Información, excelente y recordado ex alumno de la Universidad Tecnológica Nacional Regional Buenos Aires, recibido de ingeniero, quien ha dedicado sus últimos doce años a estudiar y trabajar sobre esta temática. Lo ha hecho en continua aplicación de la tecnología informática que sobrevino en estos años.

Su apreciación aquí escrita, por ende, no solo demuestra el conocimiento adquirido en ellos, sino su experiencia ante circunstancias concretas.

Por ello estimo importante recorrer las páginas de su primer libro: *Data Centers Hoy*, En ese sentido, recomiendo su lectura a todos aquellos que actúan en las organizaciones donde existan estas estructuras de procesamientos de datos, Ciertamente, este libro no aspira a agotar el tema, que por otra parte, está en contante evolución, pero les brindará a los profesionales algunas claves indispensables para ayudarlos a encontrar soluciones informáticas a la medida de cada empresa.

Lic. Carlos Tomassino,

Presidente

del Consejo Profesional en Ciencias Informáticas, A.C

Prefacio

En el contenido de este material se podrá descubrir y profundizar los conocimientos acerca de los elementos que componen un Data Center, ya sea para niveles iniciales o para aquellos que ya tienen diversos niveles de conocimientos teóricos y/o prácticos en la administración de los mismos. Esto incluye desde principiantes o estudiantes universitarios que deseen incursionar en el tema, hasta aquellos responsables que ya poseen experiencia en Data Centers, independientemente del tamaño, ya sean chicos, medianos o grandes y desean ampliar sus conocimientos.

Luego de cientos de horas de investigación, desarrollo y la experiencia propia de la autor, aplicada en este libro se dan consejos, estrategias y recomendaciones basados en las técnicas y estándares más novedosos para optimizar el funcionamiento, buscando brindarle al negocio una mejora competitiva.

El principio de este ejemplar se comienza explorando los distintos niveles iniciales del Data Center y su clasificación. Así mismo se explican los motivos por los cuales son tan importantes y cuáles son los posibles impactos sino son correctamente planificados.

Seguidamente se irán explicando cuales son los dispositivos físicos que lo conforman y además la relación con los componentes operativos que se utilizan para su funcionamiento, como son la electricidad, los mecanismos de redundancia para evitar situaciones de interrupciones no deseadas, condiciones termo ambientales, la seguridad, la disposición de la red en función al negocio y como es la interacción entre todos esos elementos mencionados para maximizar el rendimiento desde el punto de vista organizativo, permitiendo la mejor optimización de los recursos en base a las recomendaciones y mejores prácticas de la industria con una visión de sustentabilidad a largo plazo , así como el diseño de planes de contingencia en casos de desastre.

Por último se incluyen una serie de recomendaciones y mejores prácticas sugeridas para adoptar por los responsables de los Data Centers, buscando un mejor desempeño y disponibilidad de los componentes actuales.

Ing. Germán Pacio

.

Acceso al material complementario

Para tener acceso al material complementario del libro Data Centers hoy para desarrolladores, es necesario:

1. Ir a la página: `http://libroweb.alfaomega.com.mx/`

2. Regístrese como usuario y guarde en un lugar seguro su nombre de usuario y clave de acceso para emplearla para futuros ingresos.

3. Ingrese con su usuario a la sección de libros.

4. Busque y seleccione la imagen correspondiente a este libro para descargar su material complementario como:

- Croquis de un Data Centers (formato PDF)
- Data Center Framework v3 (formato PDF)
- Fe de erratas

Introducción

Este libro está concebido para todos aquellos que desean abordar por primera vez la comprensión de los elementos que integran un Data Center o están ya familiarizados con el tema, pero desean profundizar y ampliar sus conocimientos previos. Por ese motivo, este libro es una herramienta práctica tanto para los estudiantes universitarios como para los responsables del planeamiento, diseño, implementación y operación de un Data Center en las empresas.

Los consejos, estrategias y recomendaciones que se encuentran a lo largo de la obra son el resultado de una extensa investigación y mi amplia experiencia en esta materia. Se inspiran en las nuevas técnicas, los estándares más novedosos y las últimas tendencias a fin de optimizar el funcionamiento actual del Data Center, y brindarle al negocio una mejora competitiva. En ese sentido, he intentado desarrollar una serie de propuestas destinadas a la mejora de las prácticas actuales de la industria así como al diseño de planes de contingencia.

Para facilitar su lectura, he divido al libro en 11 capítulos donde he analizado los aspectos fundamentales del Data Center con un enfoque práctico y orientado a brindar soluciones adecuadas al tamaño y volumen de negocio de cada empresa.

- El Capítulo 1 presenta una introducción al tema, ofreciendo una visión general de la cuestión, una clasificación de los Data Centers y sus prestaciones.
- El Capítulo 2, “Filosofía del diseño”, explora todos aquellos aspectos relacionados con la construcción edilicia y el diseño, la ubicación geográfica y su relación con el ambiente. También, aborda el tema del presupuesto y los costos que se deberán tener en cuenta para optimizar los recursos.
- El Capítulo 3, “Componentes básicos”, describe en profundidad los componentes de un Data Center, los Racks, y estudia también el tamaño idóneo del Data Center en función del volumen de negocio.
- El Capítulo 4, “Alimentación eléctrica”, estudia exhaustivamente todos los elementos eléctricos presentes en un Data Center, y analiza desde cómo seleccionar la alimentación o potencia eléctrica hasta cuáles son los problemas eléctricos más usuales, y cuál es el generador adecuado para cada empresa.
- El Capítulo 5, “Control ambiental”, desarrolla el tema del enfriamiento y la importancia de la correcta fluidez del aire frío en el ingreso a los equipos así como los distintos tipos de aire acondicionado y métodos de refrigeración o de ventilación del aire.

- El Capítulo 6, “Seguridad y prevención de incendios”, detalla tanto las amenazas que puede sufrir un Data Center como los métodos de prevención y seguridad para evitar los incendios.
- El Capítulo 7, “Diseño de red”, describe los diversos tipos y categorías de cables y cableados, sus características; además, enumera una serie de recomendaciones para su óptima instalación.
- El Capítulo 8, “Organización”, define los distintos aspectos relacionados con la gestión de un Data Center, desde el tablero de control hasta la documentación de políticas y procedimientos.
- El Capítulo 9, “Optimización”, examina las técnicas actuales de optimización: virtualización y nube. Además, discute los desafíos actuales y futuros para ir hacia un Data Center más ecológico.
- El Capítulo 10, “Continuidad del negocio”, plantea el ciclo de vida del plan de continuidad del negocio, cuáles son las fallas más habituales, y cómo implementar planes de recuperación ante desastres o contingencias, utilizando diversas estrategias de *backup*.
- El Capítulo 11, “Mejores prácticas”, ofrece un abanico de propuestas y consejos para construir un buen Data Center desde el inicio, evitando los errores más frecuentes. Asimismo, discute cuál debe ser hoy en día el rol del Responsable de Data Center para administrar con eficiencia los riesgos que debe enfrentar en su función.

Espero que su lectura amplíe sus conocimientos de manera agradable y a la vez sea útil para la práctica profesional de sus tareas diarias.

Introducción

1

"El mayor enemigo del conocimiento no es la ignorancia, sino la ilusión del conocimiento".

-- Stephen Hawking (1942) físico, cosmólogo británico

Definición de Data Center

Un Data Center o también llamado CDP (Centro de Procesamiento de Datos) es un espacio con determinadas características físicas especiales de refrigeración, protección y redundancia, cuyo objetivo es alojar todo el equipamiento tecnológico de la compañía brindando seguridad y confiabilidad. Todas estas condiciones aseguran la disponibilidad de los servicios de red.

Es un lugar crítico para las empresas, ya que en él se alojan los activos más importantes de las empresas, y además es una unidad de negocio muy importante con valor propio. En este espacio físico se almacenarán los servidores que enviarán sus correos electrónicos, alojan a los servidores Web de la empresa: su cara al cliente. También se procesarán las transacciones del negocio y los balances, se guarda información sensible financiera, e incluso secretos industriales.

Los costos de construcción y mantenimiento de un Data Center tienen un porcentaje importante dentro del presupuesto total de IT (Infraestructura Tecnológica). Por ello es fundamental no fallar en el momento del diseño estructural y de sus componentes centrales. Debido a la infraestructura especial necesaria los costos de construcción y operación por metro cuadrado son mucho más altos comparándolos con los espacios de oficinas tradicionales.

Todas estas condiciones hacen que un Data Center sea un lugar clave dentro de la empresa.

Clasificación

Los Data Centers se caracterizan según su dimensión y según sus prestaciones físicas hacia los elementos que almacenan. Existen tres tipos.

- **Sala de servidores**: es una estructura chica, pocos servidores. Muy informal.
- **Centro de cómputos**: dimensión mediana, puede tener Rack, condiciones de seguridad y ambientales básicas.
- **Data Center**: gran dimensión, obligatoriamente todo los elementos que lo componen esta alojados en Racks de forma ordenada, bajo condiciones de seguridad reguladas, controles estrictos eléctricos y ambientales (incluso alguno o varios sistemas redundantes).

Prestaciones generales típicas

Característica	Sala servidores	Centro de cómputos	Data Center
Piso Flotante	No	No/Si	Si
Tamaño	< 20 mts^2	< 40 mts^2	> 40 mts^2
Cantidad de servers	< 20	<50	> 50
Aire Acondicionado	Hogareño	Profesional	Profesional/Central
Acceso	Cerradura	Tarjeta magnética	Tarjeta magnéti-ca/Biométrico
Red	Hub/switch	Switch	Fiber switch
Cableado	UTP 5/5E	UTP 5E/6	UTP 6a/fibra óptica
Sistema eléctrico de contingencia	Ninguno o UPS	UPS	UPS + Generador
Prevención de incendios	No	Extintores manuales	Detección de humo + Extintor de fuego + Rociadores
Registro de accesos físicos	Manual	Manual	CCTV
Sensores o detectores	No	Si	Si
Monitoreo Centralizado	No	No	Si

Importancia

Hoy en día no existe actividad económica que no tenga dependencia de algún tipo de sistema informático, y sin dudas el Data Center toma un rol estratégico para el buen desarrollo de cualquier empresa a la hora de proteger el correcto funcionamiento de todos los sistemas. Una interrupción en el servicio (de red, electricidad, enfriamiento) puede impactar a los servidores, generando millones de dólares en pérdidas económicas directas o indirectas. Por eso, es vital para el establecimiento tener todos los servicios disponibles, especialmente, si hablamos de negocios *online*, donde no solo se pierden las transacciones y se afecta a la imagen de la compañía, sino que los clientes puede usar servicios de nuestra competencia. De esa forma no solo se perdería una venta potencial, sino que también al cliente, que es mucho peor.

Catástrofes y pérdidas

Una de las funciones básicas de un Data Center bien diseñado es eliminar los riesgos potenciales que causarían pérdidas evitables, y minimizar el impacto de las no evitables como las catástrofes naturales.

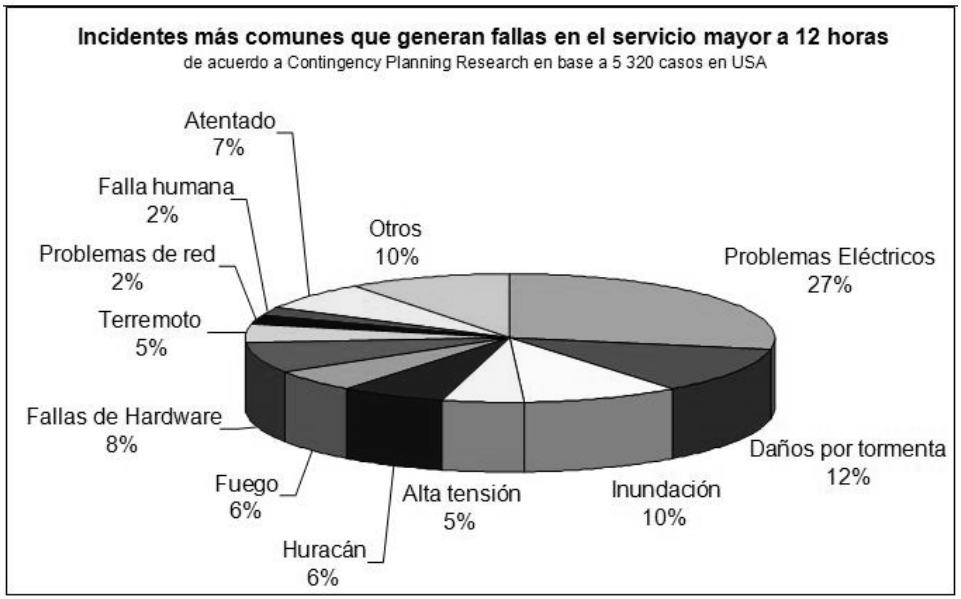
Es importante remarcar que en los casos en que las empresas sufren daños importantes o catástrofes naturales en sus sistemas, es casi a menudo un daño irreversible que puede llevar a la compañía a su cierre parcial o, en algunos casos, definitivo.

Una investigación de la Universidad de Texas revela que de las empresas que sufren una pérdida masiva en sus sistemas de información, **el 43% nunca vuelve a abrir, el 51% cierra antes de los dos años**, y solo **el 6% puede continuar** con su actividad, enfrentando grandes pérdidas en sus sistemas de información.

Según otro informe de la Agencia Nacional de Archivos y Registros en Washington D.C. (National Archives and Records Administration), el 93% de los negocios que tienen una interrupción importante en sus Data Center por más de 10 días, quedan en bancarrota en menos de un año.

La contundencia de estos números deja a la vista cuán importante son los datos de las empresas para poder permanecer con las puertas abiertas.

Existen muchas causas que pueden generar una interrupción importante en un Data Center, que involucran desastres naturales: huracanes, inundaciones, terremotos, tornados, incendios, tsunamis. También, pueden ser causados por el hombre: sabotajes, fallas humanas, fallas en el suministro eléctrico, fallas en la red, etcétera. A continuación, en el gráfico, se detallan como una tendencia general, las principales causas y la frecuencia en que estos incidentes ocurren:



Por otra parte, es importante señalar que sin que haya un indisponibilidad de servicios importante, las pérdidas pueden llegar a ser de alto impacto. De acuerdo con una investigación de Infonetics Research (2005), realizada a 230 grandes compañías de los Estados Unidos (con más de 1000 empleados), se pierden entre el 2% y el 16% del beneficio neto anual debido a indisponibilidades de IT.

Algunos ejemplos de casos reales

Empresa	Rubro	Fecha	Tiempo sin servicio	Causa	Costo	Acción correctiva
Last.fm	Comercio música digital	31/05 (2009)	6 horas	Fallas en el sistema de enfriamiento	16 millones de usuarios afectados	Sin datos
Fisher Communications	Comunicaciones y Hosting	02/07 (2009)	2 semanas	Incendio	Servicios de comunicaciones y clientes afectados	6,8 Millones de dólares
NaviSite	Hosting	19/01 (2010)	24 horas	Falla en el sistema eléctrico	Cientos de clientes afectados	Sin datos

Gmail	Correo	2/03 (2011)	24 horas	Error humano	150.000 cuentas de usuarios fueron cerradas por error	Sin datos
Alaska Air Group	Aerolínea	26/03 (2011)	32 horas	Falla en el sistema eléctrico	150 vuelos cancelados (12.000 pasajeros)	Sin datos
Westpac	Finanzas	05/05 (2011)	48 horas	Problemas en el sistemas de refrigeración	Problemas para acceder al *homebanking* y cajeros automáticos	Sin datos
Oracle	Software	29/06 (2011)	30 horas	Falla en el sistema eléctrico	Miles de usuarios no pudieron acceder al sitio OpenOffice	Sin datos
Amazon Web Services (Virginia)	Hosting	14/06 (2012)	8 horas	Falla de refrigeración en el generador	Afectó a clientes. Externos: Netflix, Pinterest, Heroku, Quora, Foursquare y otros	Sin datos
Amazon Web Services (Virginia)	Hosting	29/06 (2012)	8 horas	Problemas en el cableado eléctrico.	Afectó a clientes. Externos: Netflix y Pinterest entre otros	Sin datos
Salesforce.com	CRM/ Hosting/ Cloud	10/07 (2012)	9 horas	Problemas eléctricos	100.000 clientes afectados	Sin datos
Wikipedia	Enciclopedia Virtual	06/08 (2012)	2 horas	Problemas eléctricos (error humano)	$ 0	Restauración cables

Algunos ejemplos de casos reales no asociados directamente con problemas en el Data Center

Empresa	Rubro	Fecha	Tiempo sin servicio	Usuarios afectados	Causa	Costo	Acción correctiva
Sony	Entretenimiento	20/04 (2011)	3 semanas	77 Millones	Ataque informático	U$S 171 millones	Reestructuración seguridad de la red PSN
GoDaddy	Registro dominios	14/06 (2011)	3 horas	6 Millones	Fallas en la actualización del sitio	Sin datos	Sin datos
BlackBerry	Telefonía	10/11 (2011)	3 días	40 Millones	Problemas en la red RIM de distribución de mensajes	U$S 100 millones	Sin datos
Entel (Chile)	Telefonía	03/01 (2012)	5 horas	1,3 Millones	Falla en nodos	Sin datos	Sin datos
Microsoft	Hosting (Azure)	29/02 (2012)	4 horas	Muchos clientes	Falla en el servidor de certificados	Reducción de facturación: 33%	Actualización software
Movistar (Arg.)	Telefonía	02/04 (2012)	5 horas	18 Millones	Posible sabotaje	U$S 40 millones	Sin datos
Claro (Arg.)	Telefonía	09/05 (2012)	4 horas	2 Millones	Corte fibra óptica	U$S 2,2 millones	Plan Contingencia
LinkedIn	Red Social	07/06 (2012)	N/A	6 Millones	Ataque informático	Sin datos	Cambio de claves.
Telecom (Arg.)	Comunicaciones	12/06 (2012)	6 horas	5 Millones	Corte fibra óptica	Sin datos	Plan Contingencia
Twitter	Red Social	21/06 (2012)	3 horas	500 Millones	Ataque informático	Sin datos	Plan Contingencia
Gtalk	Chat	26/7 (2012)	3 horas	435 Millones	Fallas de software	Sin datos	Sin datos

Estos ejemplos son tan solo una pequeña cantidad de casos que tomaron público conocimiento y se describen a modo ilustrativo, pero día a día ocurren interrupciones que tiene impacto negativo en las empresas ocasionando grandes pérdidas económicas.

El 11 de agosto de 1999, se produjo un incendio en el Centro de Control de United Airlines, en Elk Grove, Illinois, que podría haber paralizado abruptamente las operaciones de la empresa deteniendo 24 000 vuelos que transportaban 300 000 personas. El impacto financiero en United podría haber sido tremendo.

Afortunadamente, la aerolínea había tenido la prudencia de desarrollar un plan de continuidad del negocio que incluía una instalación redundante. Aunque, en su momento, el desarrollo e implementación de este plan le costó a United millones de dólares, la compañía había comparado oportunamente el costo del plan con el costo de la interrupción del negocio y decidió que la inversión valía la pena.

Al igual que en United, el corazón de la mayoría de los negocios es el centro de tecnología de la información (IT), cuya continuidad operativa es crucial para sostener los procesos del negocio. La disponibilidad ininterrumpida de estos recursos se denomina "continuidad del negocio", estos conceptos serán desarrollados en profundidad en el capítulo 10.

También cabe señalar que ese daño no solo es la pérdida económica directa, sino también hay otros factores que podrían tener un costo negativo a largo plazo, ya que se si produce algún corte de servicio que afecta directamente a los clientes de las empresas pueden sufrir entre otros, el daño a la imagen de la compañía, la imagen hacia los accionistas, falta de cumplimiento de normas y estándares internacionales o desventaja hacia la competencia.

El 80% de las indisponibilidades de los servicios de IT es debido a fallos de las personas y los procesos.

Es altamente recomendable tener una estimación de cuánto dinero cuesta por hora la indisponibilidad de una aplicación o un servidor en particular, ya que nos puede ayudar a buscar un nuevo diseño de solución cuando sea necesario y la variable económica se torne fundamental a la hora de convencer a los ejecutivos, en caso de que se requiera una inversión adicional para dicha solución.

Existen tres tipos de costos que deben tenerse en consideración:

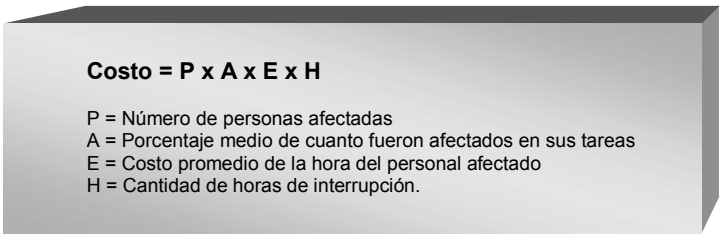
- **Costos de Oportunidad:** representa a todas aquellas utilidades que se perdieron de ganar por indisponibilidad. No poder vender en ese momento, o aun peor: el cliente se va a la competencia (no solo se pierde la venta, sino el cliente).
- **Costos Directos**: son los que influyen directamente en las finanzas de la empresa, por eso son más fáciles de medir, como por ejemplo:
  - Empleados esperando para poder trabajar.
  - Pérdida de transacciones y operaciones.

- Tiempo de recuperación de servicio.
- Tiempo de testeo post recuperación.
- Demandas legales por incumplimiento de obligaciones.

- **Costos Indirectos**: son los costos asociados a posibles situaciones de las cuales no se tiene un gran nivel de certeza, pero se sabe que existen. Por eso son mucho más difíciles de medir, pero impactan en el negocio de la misma manera:
  - Pérdida de satisfacción del cliente.
  - Clientes que se pierden y se pasan a la competencia.
  - Daños a la imagen de la compañía.
  - Relaciones públicas negativas.

Existe una fórmula para calcular el costo de una falla en el servicio. Un buen punto de inicio es evaluar los factores y recolectar los datos estadísticos asociados con los costos de las interrupciones pasadas y su duración.

Ecuación:



Ejemplo:

Existe un problema eléctrico en el cableado del Data Center que afecta a un servidor que maneja la línea de cajas de un banco.

P= 8 (cantidad de cajeros que estaban trabajando en ese momento.

A= 100 (al no tener sistema para operar, el cajero no puede trabajar, ya que la exigencia de los sistemas bancarios desde hace tiempo impiden la operatoria manual).

E= $60 u.m. (unidades monetarias).

H = 5 horas (considerando el tiempo que tarda en volver la corriente eléctrica y el tiempo que le llevará al administrador del sistema el restablecimiento del servicio normal.

Costo = 8 x 100 x 60 x 5

Costo = $ 240 000

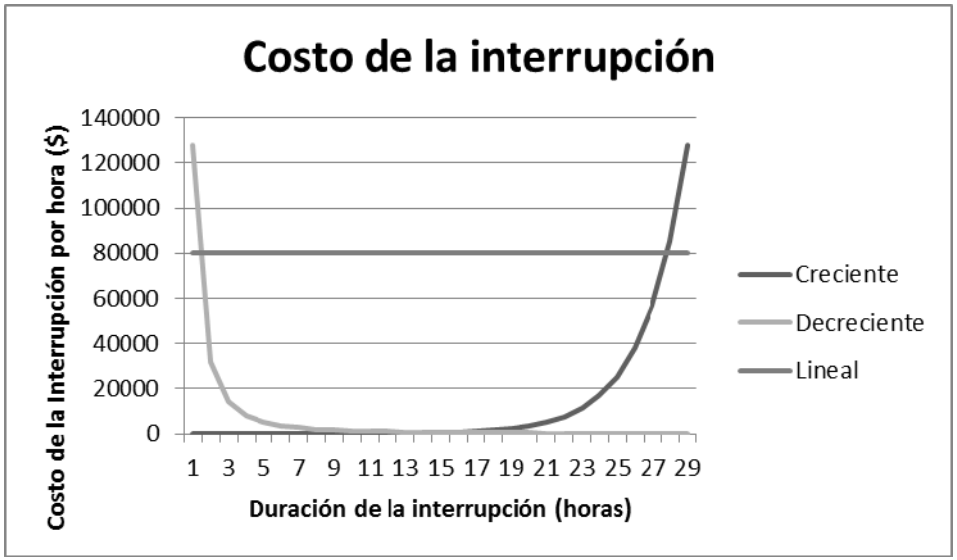
Es importante aclarar que no se está considerando el costo potencial de las acciones que derivarían de la interrupción. Por ejemplo: costo por transacción perdida, potencial pérdida de clientes, pérdida de imagen corporativa, demandas legales, etcétera. El daño a la imagen de la marca es la pérdida más difícil de cuantificar económicamente, ya que no existe una fórmula; se pueden hacer estimaciones, pero siempre con un índice de confiabilidad bajo.

Otra buena práctica ágil para determinar el costo de la interrupción en horas es tener una estimación por servidor o por aplicación sobre cuánto dinero pierde la empresa por cada hora de interrupción.

Según un estudio realizado por el Ponemon Institute (en 2011), sobre un análisis de 41 casos de Data Centers mayores de 230 m^2 de diferentes tipos de industrias, que abarcaban desde financieras, petroleras, salud, gubernamentales, entre otras, solo considerando una interrupción menor a 2 horas, arrojó como conclusión que las pérdidas varían entre los 40 000 y 1 000 000 de dólares por empresa (dependiendo del rubro), es decir, un promedio total de 4 700 dólares por minuto. El mismo estudio estableció un lapso duración medio de interrupción de 107 minutos, lo que equivale a más de 500 000 dólares. De todos esos casos analizados, se estima que el 80% pudo haberse previsto tomando medidas de protección adecuadas.

Es fundamental también saber que existen tres tipos de curvas distintas cuando se analiza el costo de interrupción en función del tiempo transcurrido, según el tipo de negocio en particular, pudiendo ser:

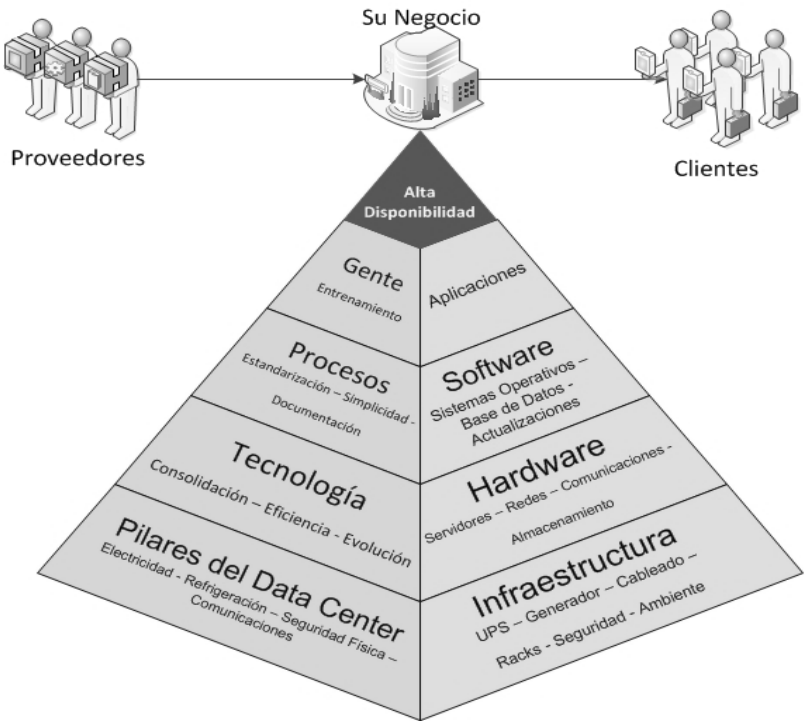
- **Creciente:** es el caso en donde la interrupción inicial no tiene un impacto muy grande, pero a lo largo del tiempo los costos se incrementan, principalmente los de tipo indirecto. Por ejemplo, sería el caso de un *homebanking*.
- **Lineal:** el costo por cada hora de interrupción se mantiene constante en el tiempo, afectados principalmente por costos directos. Por ejemplo, sería el caso de una aplicación interna de RR.HH.
- **Decreciente:** la interrupción tiene un impacto muy grande al inicio, pero a medida que trascurre el tiempo ese costo va en decremento. Un ejemplo, sería el caso de un horno industrial de una metalúrgica controlado por un servidor que falló. El impacto es muy grande al comienzo, ya que el horno demorará varias horas en volver a tomar la temperatura de fundición adecuada.



Años atrás los ejecutivos y directores de las empresas veían al área de sistemas como un centro de costos sin fondo donde el dinero iba allí, pero no se sabía bien para qué, cual era la finalidad, cuales era los motivadores, etcétera. Hoy en día esta tendencia se está revirtiendo, y los ejecutivos entienden que la tecnología e Internet son una puerta de acceso para hacer negocios de todo tipo, no importa el rubro, cualquier negocio puede potenciar sus ventas si hace un buen uso de la tecnología, aplicaciones, conectividad, dispositivos móviles o conexiones remotas, entre otras.

Por eso es cada vez más común encontrar a los Directores de IT (Chief Information Officer, CIO) integrando el directorio de las empresas formando parte de la junta directiva (sobre todo en compañías estadounidenses), porque pueden aportar desde su visión en la toma de decisiones estratégicas, como saber: qué cosas se pueden hacer; cuáles son inviables; cuáles sí son viables; cuáles son las tendencias actuales; qué solución sería la más rápida y económica para poder llevar a cabo un negocio; qué cosas se necesitan desde el punto de vista de la infraestructura para poder alcanzar los objetivos, como por ejemplo cuáles son las capacidades de los Data Centers.

Visión general:

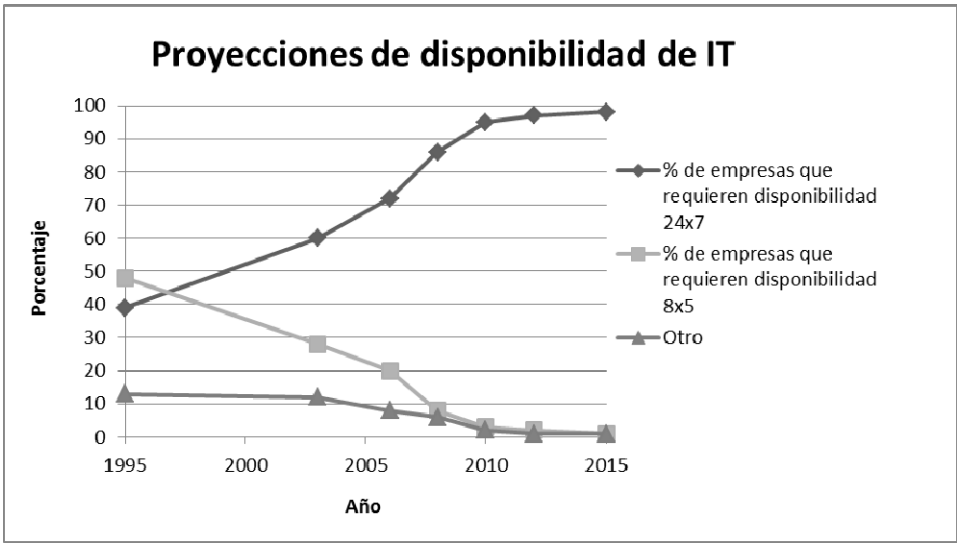


Este gráfico muestra que la meta consiste en alcanzar la mayor disponibilidad posible dentro de lo posible. Por el lado izquierdo se observan los diferentes niveles de interacción desde el punto de vista del negocio; y del lado derecho, se aprecian desde la perspectiva de la infraestructura. Ambas convergen para brindar alta disponibilidad a la empresa para que nunca se corte la relación con los clientes ni con los proveedores.

Tendencia evolutiva del negocio

La rápida evolución de los mercados y la dependencia que las empresas tienen hacia sus sistemas informáticos ha generado un cambio en la disponibilidad diaria que los sistemas deben ofrecer al negocio. Este fenómeno se vio acrecentado con la globalización, sobre todo en empresas multinacionales con servicios centralizados, donde hay alguna aplicación que presta un servicio global a toda la compañía y debe estar disponible en todo momento, ya que cuando en algún lugar del mundo es de noche, en otro lugar es el *prime time* del negocio. Día a día se requieren más servicios *full time* con disponibilidad 7 x 24, aspecto que antes no era habitual y

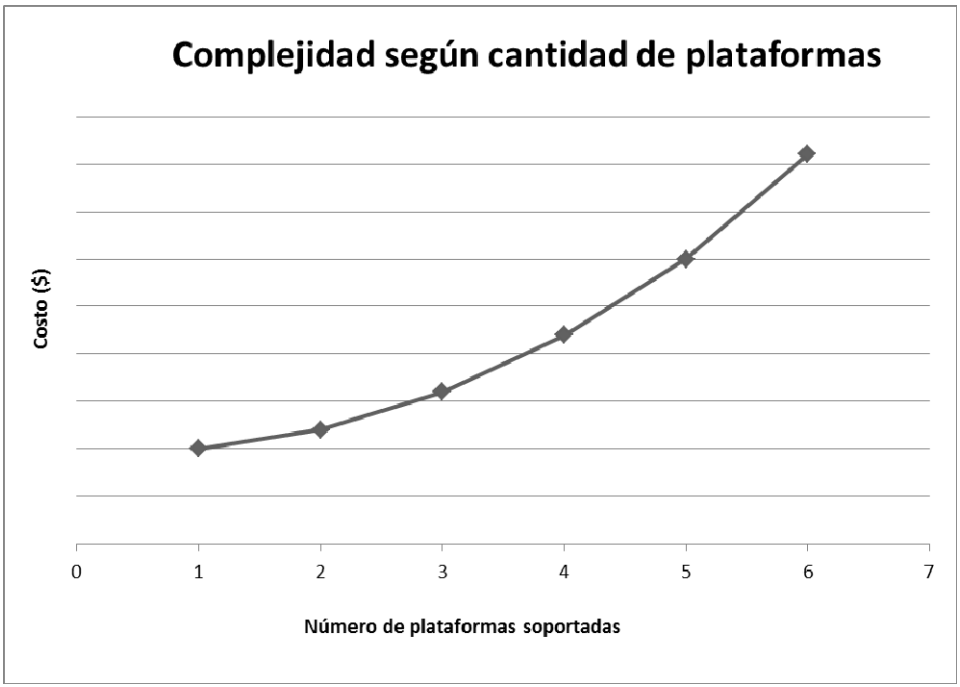
solo se dejaba para aplicaciones de alta criticidad. Históricamente, los bancos fueron el primer rubro en requerir este tipo de disponibilidad, principalmente por la red de cajeros automáticos.



Costo de la complejidad

En el diseño estructural de un Data Center se debe tener en cuenta la diversidad de plataformas que estarán contenidas en él, ya que a mayor cantidad de plataformas distintas, su complejidad aumentará y ello conllevará un incremento en los costos generales y de mantenimiento. Si bien es muy difícil de calcular, es posible hacer estimaciones de los costos, y así ver que una consolidación es necesaria, aunque para ello se necesite una inversión.

La premisa básica es que a mayor diversidad de plataformas resultará más costoso tener alta disponibilidad. Con menos plataformas, los costos serán menores, ya que el nivel de complejidad es menor.

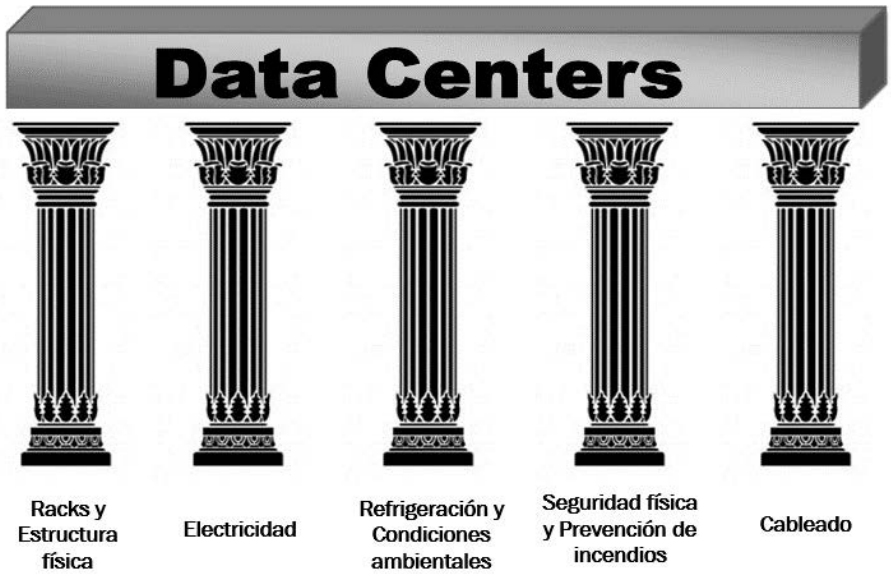


Este incremento de los costos se debe a que las distintas tecnologías de las diferentes plataformas difieren ampliamente, cada una de ella tendrán sus propios requerimientos y limitaciones. Un mayor número de plataformas obligará a tener más administradores, ya que tienen distintos conocimientos, aunque no haya una cantidad importante de servidores. Otro caso sería en un ambiente donde hay servidores virtuales, y por un nuevo requerimiento se necesita una nueva plataforma que no puede ser ejecutada como servidor virtual, por no ser soportada por la solución de virtualización disponible actualmente, obligando así a la compra de un equipo físico nuevo o a tener otra solución de virtualización distinta, que generará así un costo mayor. Las labores humanas suponen más del 40% del costo total de la prestación de servicios de TI.

Cada Data Center es único y distinto, pero todos tienen el mismo propósito, proteger el activo más importante de su empresa: la información.
¿Se imaginan un banco sin bóveda de seguridad blindada?

Pilares

Los elementos clave de un Data Center son:



Identificar los pilares dentro del Data Center es vital para establecer niveles de redundancia y confianza deseados. De esta forma, se pueden satisfacer las necesidades del negocio brindando:

- Alta disponibilidad.
- Reducción de costos.
- Una mejor utilización de activos.
- Agilidad y flexibilidad para adaptarse a nuevos escenarios.
- Valor agregado al negocio por diferenciación.

Capas de redundancia

Una buena aproximación para establecer niveles de redundancia y confianza es la nomenclatura propuesta por el TIA (Telecomunication Industry Association), definido en el documento "TIA-942", en el 2005, en donde se establecen cuatro capas o niveles de confianza según el grado de redundancia que el Data Center puede poseer en sus instalaciones, siendo uno el nivel más bajo y cuatro en nivel más alto.

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 pretenden alcanzar. Este es el primer estándar de clasificación de una entidad internacional, pero el concepto original de clasificación por capas fue propuesta inicialmente en 1995 por The Uptime Institute.

Para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto en el Data Center como en la infraestructura de soporte. Los niveles de capas que plantea el estándar se corresponden directamente con cuatro niveles de disponibilidad, considerando que a mayor número de capa, mayor será el grado de disponibilidad. Esto implica también mayores costos constructivos. A mayor nivel de capa que se desea como objetivo, se deberá cumplir con los requisitos de las capas anteriores. Por ejemplo: para un Data Center de Capa IV se deberán cumplir todos los requisitos de las Capas III, II y I.

En muchísimos documentos vamos a encontrar que los autores utilizan la letra N para describir los distintos tipos de configuraciones redundantes que puede haber. Pero: ¿qué es la N?

La N puede ser definida como la necesidad de la carga crítica o el requerimiento mínimo para operar de forma normal. Este concepto se aplica a nivel general, ya sea que estemos hablando de equipamiento eléctrico, equipos de refrigeración o sistemas de extinción de incendios.

A continuación se detallan las diferentes posibilidades que podemos encontrar, y un ejemplo práctico:

- N: representa el total. Es decir, si en nuestro Data Center necesitan 3 generadores para soportar el consumo eléctrico de todos los equipos; en caso de falla, solo tengo 3 generadores.
- N+1: tiene un generador de repuesto. Igual que en el ejemplo anterior, en total hay 4 generadores: 3 son iguales, más 1 de repuesto.
- 2N: redundancia total duplicada. Siguiendo el mismo ejemplo, en este caso tendría 6 generadores iguales.
- N+2: capacidad de N más 2 partes de repuesto. Análogamente al primer caso, aquí tendría 5 generadores.
- 2N+1: redundancia total duplica, más un equipo de repuesto para situación de contingencia. En este caso tendría 7 generadores: 6 para mantener toda la infraestructura duplicada, más 1 de repuesto.

No hace falta ser un genio en las matemáticas para darse cuenta que a medida que aumentan los números de sistemas redundantes, el costo aumenta, como mínimo, de manera proporcional, aunque podría ser más aún debido a la complejidad de instalación.

Capa I (Tier I): Data Center básico

Un Data Center Capa I puede ser susceptible a interrupciones tanto planeadas como no planeadas. Cuenta con sistemas de aire acondicionado y distribución de energía; pero puede tener piso técnico o no, 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 Data Center deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento. Situaciones de urgencia pueden motivar paradas más frecuentes y errores de operación o fallas en los componentes de su infraestructura causarán la detención del Data Center. La tasa de disponibilidad máxima del Data Center es 99.671% del tiempo.

Capa II (Tier II): Data Center con componentes de capacidades redundantes

Los Data Center con componentes redundantes son ligeramente menos susceptibles a interrupciones tanto planificadas como no planificadas. Estos Data Center cuentan con piso falso, 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 sistema de contingencia de cada componente de la infraestructura. La carga máxima de los sistemas en situaciones críticas, donde los sistemas de contingencia están activados es del 100%. El mantenimiento en la línea de distribución eléctrica u otros componentes de la infraestructura pueden causar una interrupción del procesamiento. La tasa de disponibilidad máxima del Data Center es 99.749% del tiempo.

Capa III (Tier III): Data Center de mantenimiento concurrente

Un Data Center de este nivel cuenta con capacidades técnicas que le permiten realizar cualquier tipo de actividad planificada de mantenimiento sobre cualquier componente de la infraestructura sin interrupciones en la operación. Actividades planificadas envuelven el mantenimiento preventivo y programado, reparaciones o reemplazo de componentes, el agregado o la eliminación de elementos, y la realización de pruebas de componentes o sistemas, entre otros. Para infraestructuras que utilizan sistemas de enfriamiento por agua. Debe existir suficiente capacidad y doble línea de distribución para los componentes, de forma tal de que sea posible realizar el mantenimiento o las pruebas en una línea mientras la otra atiende la totalidad de la carga sin generar interrupciones. En este nivel, las actividades no programadas, los errores de operación o fallas inesperadas en la infraestructura aún pueden causar una interrupción del Data Center. La carga máxima en los sistemas en situaciones críticas es de 90%. Existen muchos Data Center Capa III que han sido diseñados para poder actualizarse a Capa IV, en el momento en que los requerimientos del

negocio justifiquen el costo de dicha modernización. La tasa de disponibilidad máxima del Data Center es 99.982% del tiempo.

Capa IV (Tier IV): Data Center tolerante a fallas

Este Data Center provee capacidad para realizar cualquier actividad planificada sin interrupciones, pero además la funcionalidad tolerante a fallas le permite a la infraestructura continuar operando, aun ante un evento crítico no planificado.

Esto requiere dos líneas de distribución simultáneamente activas, típicamente en una configuración: "sistema" + "sistema"; Por ejemplo, si estamos hablando eléctricamente, esto significa dos sistemas de UPS independientes, cada una de ellas es un sistema con un nivel de redundancia individual N+1. La carga máxima de los sistemas en situaciones críticas es de 90%, y persiste un nivel de exposición a fallas. Además cuentan con un sistema para detener los equipos de manera controlada en casos de extrema necesidad. Por ejemplo, si se inicia una alarma de incendio o una persona inicia un procedimiento de apagado de emergencia o Emergency Power Off (EPO), los cuales además deben existir para cumplir con los códigos de seguridad contra incendios o eléctricos. La tasa de disponibilidad máxima del Data Center es 99.995% del tiempo.

Hay que tener en cuenta que para un nivel de Capa IV se establece que la única parada que se produce es por la activación de un EPO, y esto solo sucede una vez cada cinco años. No obstante para la exigencia que demanda un Capa IV, algunas empresas u organizaciones manifiestan la necesidad de una disponibilidad de "cinco nueves", esto significa un 99.999% de disponibilidad.

Históricamente, los primeros Data Center eran de Capa I, y surgieron en la década de los sesenta, Luego aparecieron los Data Center de Capa II, en los años setenta. Hacia fines de los ochenta y principios de los años noventa, aparecieron los Data Center de Capa III. Y recién hacia 1995 se vieron los Data Center de Capa IV.

Tabla Comparativa según las Capas (Tier)

Características	Capa I	Capa II	Capa III	Capa IV
Redundancia	N	N+1	N+1	2(N+1)
Año aparición	1965	1970	1985	1995
Número de alimentaciones eléctricas	1	1	1x activo/1x pasivo	2
Personal permanente	Ninguno	1 (un solo turno)	1 (uno por cada turno)	24x7x365
Mantenimiento en operación	No	No	Sí	Sí
Piso Técnico (altura)	30 cm	45 cm	70-75 cm	70-75 cm
Posibles puntos de falla	Muchos	Muchos	Algunos	Incendio, fallo humano
Tolerancia a fallos únicos	No	No	No	Sí
Interrupción de operación por mantenimiento al año	2 interrupcio-nes de más de 12 horas	1.5 interrup-ciones de más de 12 horas	0	0
Interrupción de servicios por año	2 cortes de más de 4 horas	1 cortes de más de 4 horas	0 cortes de más de 4 horas	0.2 cortes de más de 4 horas
Tiempo promedio de implementación (meses)	3	3 a 6	15 a 20	15 a 20
Tiempo anual de servicio de mantenimiento	28,8 horas	22,00 horas	1,6 horas	0,8 horas
Disponibilidad de servicio(*)	99,671%	99,749%	99,982%	99,991%

(*) La disponibilidad real, que es realmente la que importa puede ser confundida con la disponibilidad del servicio. Para entender el concepto de disponibilidad real en profundidad es necesario definir los conceptos descriptos a continuación.

Hay tres componentes que intervienen cuando hablamos de una interrupción: MTTF (Mean Time To Failure) es el tiempo promedio en el cual un componente o sistema tiene una alta probabilidad de falla; el MTBF (Mean Time Between Failures) nos indica el tiempo promedio en el cual se tiene alta probabilidad de otra falla después de que haya ocurrido una anterior; y el MTTR (Mean Time To Recover) es el tiempo promedio que se requiere desde que el sistema falla hasta su completa recuperación.

Cuando se habla de tiempo de interrupción, también debemos hablar de tiempo de disponibilidad, que no es lo inverso. Por ejemplo, si decimos que un servicio queda interrumpido durante 5 minutos no significa que el tiempo de disponibilidad

de ese día fue de 23:55 horas, ya que existe otro factor a considerar, que es el tiempo de recuperación y testeo, el cual muchas veces puede superar el tiempo de interrupción real. Por ejemplo: a un servidor que se reinicia inesperadamente, le toma 5 minutos volver a estar operativo, pero allí se está ejecutando un motor de base de datos que demora 10 minutos en volver *online*, y al administrador de base de datos le toma otros 10 minutos verificar la consistencia de los datos y asegurarse que la base esta operativa nuevamente, entonces el tiempo de interrupción fue de 25 minutos, por lo que la disponibilidad real del servicio fue 23:30 horas. Es decir:

Además del estándar de la TIA, existen otros estándares bastante similares, como ser los de Uptime Institute, ICREA, BICSI o Syska (no utiliza la clasificación por capas, sino que tiene otro método), más allá de las diferencias lo importante es encontrar el equilibrio justo entre los objetivos del negocio y lo que resulta económicamente rentable según esas necesidades, porque hay punto de algunas capas que son muy difíciles de cumplir y pueden requerir una inversión desproporciona según negocio, como por ejemplo para un Data Center Tier IV se requieren 2 generadores capaz de soportar toda la carga y un tanque de combustible capaz de proveer una autonomía de funcionamiento para 4días consecutivos, eso por nombrar tan solo alguno de los puntos, es decir que cumplir con todos ellos es realmente muy difícil y caro.

Algunas instituciones como el Uptime Institute ofrecen certificaciones totales o parciales (a distintos niveles): Documentación/Diseño, Construcción y Operación/Mantenimiento.

Filosofía del diseño

2

"Un experto es una persona que ha cometido todos los errores posibles en un determinado terreno".

-- Niels Bohr (1885–1962) Físico danés. Premio Nobel de Física en 1922

Objetivos

El objetivo principal de un Data Center es proteger los activos de la empresa brindando un servicio de calidad sin interrupciones que perjudiquen la operatoria normal. Por esa razón, debe cumplir con las siguientes características:

- **Escalable:** debe soportar un crecimiento sin interrupciones. La mejor manera de llevar a cabo esto es planificando y estimando correctamente. Organizar los Racks y los gabinetes de forma ordenada en filas, rotulados y de modo coherente le permitirá un crecimiento ordenado y sustentable. Por ejemplo, si una parte de su Data Center falla, usted podría conectarla a una parte que esté funcionando para poder restablecer el servicio nuevamente. La planificación juega un rol fundamental en este aspecto.
- **Flexible:** debe ser capaz de sostener los nuevos servicios que se vayan agregando a la infraestructura, ya que los elementos que pertenecen a los Data Centers como ser *switchs*, routers, cables, servidores, entre otros, se van modernizando al evolucionar las tecnologías. Las decisiones estructurales que se tomen deben ser pensadas con visión de futuro, para que el Data Center no resulte obsoleto, y se pueda aumentar o reducir el tamaño cuando sea necesario.
- **Confiable:** el Data Center debe ser de alta disponibilidad y robusto para prestar al negocio un servicio sin interrupciones, ya que éstas pueden causar pérdidas económicas muy importantes. Deberá contar con sistemas de contingencia para fallas eléctricas, de red o aire acondicionado, por ejemplo,

a cargo de un personal idóneo y disponible para realizar las tareas de mantenimiento.

- **Seguro:** la información contenida en el Data Center es de un gran valor y deberá estar resguardada de la mejor manera. Mientras más valiosa es, más mecanismos de seguridad se deberán proveer para asegurarla. Siempre se debe pensar en el peor escenario posible.
- **Modular:** un diseño simple y modular permite definir unidades más fáciles de replicar, mover, balancear y manejar, facilitando el cambio de ubicación de elementos en caso necesario.
- **Desarrollo veloz:** la ubicación seleccionada debe estar en una zona que permita que todos los materiales y proveedores necesarios para el desarrollo lleguen a tiempo.
- **Estandarizado:** es conveniente mantener los mismos procedimientos de operación en todo el Data Center, porque ello provee beneficios a largo plazo, ya sea para la compra de materiales, capacitación interna, costos de mantenimiento y de implementación, o confiabilidad en las políticas y procedimientos establecidos.
- **Ordenado:** un buen Data Center se caracteriza por ser prolijo, los cables deben estar correctamente pasados y etiquetados así como los servidores, equipos de comunicaciones, Racks, UPS, etcétera.

Selección de la ubicación geográfica

El lugar donde se construirá el Data Center juega un papel preponderante a la hora de evaluar costos y riesgos. Como ya se ha mencionado en el capítulo 1, los factores de riesgo ambientales o catástrofes naturales son un imponderable que podría dejar a nuestra compañía fuera del negocio en forma definitiva.

Algunas características geográficas que se deben evaluar son:

- Actividad sísmica (terremotos, volcanes, tsunamis, etcétera.).
- Estabilidad del terreno.
- Probabilidad de ocurrencia de vientos huracanados.
- Nivel de precipitaciones.
- Calidad del aire (polución, polvo, humedad).
- Zonas proclives a incendios forestales.
- Frecuencia de tormentas eléctricas.

- Amenazas creadas por el hombre (líneas de alta tensión que generan campos electromagnéticos, contaminación industrial, plantas químicas, vibraciones causadas por trenes o máquinas pesadas).
- Proximidad a aeropuertos.

Obviamente al momento de seleccionar un lugar donde construir el Data Center buscaremos evitar todas las posibles amenazas enumeradas anteriormente.

El Data Center deberá estar ubicado en una zona con gran facilidad de acceso, con buenas rutas que permitan la entrada de todo tipo de material (sobre todo de camiones grandes), pero se recomienda que no se encuentre directamente sobre la ruta, sino que esté alejado al menos unos 100 m. En cuanto al perímetro, por un lado, deberá estar protegido por rejas y árboles, los que servirán de protección visual y de intentos de intrusiones; y por otro lado, deberá tener una distancia moderada de la edificación del Data Center y del estacionamiento (ante la eventualidad de que un vehículo se incendie).

Otro factor de importancia a considerar al seleccionar un lugar es la disponibilidad física de elementos clave como el flujo eléctrico adecuado y la infraestructura de Internet disponible. Es preferible que exista más de un proveedor de esos servicios en la zona. Asimismo, conviene estudiar la disponibilidad de agua y combustibles (para los generadores), teniendo siempre en cuenta la posibilidad de expansión.

También es necesario analizar el material de construcción para las paredes, que deberá ser aislante térmico e ignifugo; y minimizar la cantidad de ventanas, que pueden ser colocadas solamente en lugares que servirán como área administrativa, ya que es lógicamente un lugar de pérdida de temperatura.

La cantidad de entradas y salidas deben limitarse al mínimo posible. Para ello, se deberá diseñar una cabina o garita de seguridad, que cuente con personal, cámaras, barreras (además de un semáforo visual), lectores de tarjetas para el control de acceso del personal, y preferentemente pilotes retráctiles para evitar accesos por fuerza bruta.

Adicionalmente, si las medidas de seguridad son realmente extremas, y la información que se debe proteger así lo requiere, se deberán instalar detectores de metales o materiales explosivos en los accesos.

Las puertas de emergencias del Data Center deberán ser usadas como salida solo en caso de incendio, de manera tal que no puedan ser abiertas desde el exterior (además de estar debidamente identificadas).

Debido al gran desarrollo de los enlaces de alta velocidad (fibra óptica), las distancias entre sitios remotos es cada vez es más pequeña en términos de proximidad lógica. Una empresa puede tener sus servidores ubicados a miles de kilómetros de distancia de su oficina central sin que los usuarios noten la diferencia. Por eso, este último factor puede llegar a ser una ventaja estratégica importantísima a la hora de elegir el lugar para establecer un Data Center, en términos de

optimización de recursos y reducción de costos, o incluso para almacenar los servidores en Data Centers externos que cuentan con mejores prestaciones o un costo aceptable.

Muchas empresas multinacionales optaron por establecer sus Data Centers en ubicaciones estratégicas donde las temperaturas son muy bajas durante todo el año. Esto les permite tener ahorros económicos extraordinarios y disminución de la contaminación ambiental sin tener que sacrificar performance. Un ejemplo es el Data Center que Google terminó de construir en Hamina (Finlandia), ubicado en una antigua papelera, con una inversión de 252 millones de dólares, y para el cual utilizarán un sistema de refrigeración por agua. Gracias a su excelente ubicación geográfica puede tomar el agua fría del Mar Báltico, ahorrando así una considerable cantidad de dólares por año en refrigeración. En agosto del 2012 anunció la su ampliación con una inversión adicional de 185 millones de dólares para los próximos 18 meses.

En general, los costos demandados para refrigeración superan 35% del presupuesto total de un Data Center. Por eso, seleccionar la ubicación óptima se puede traducir en ahorros millonarios.

Selección de la ubicación edilicia

Si nos referimos a un Data Center, ubicado en un edificio de varios pisos, se deberá estipular primero qué sector será destinado para tal función. Será preferible evitar lugares por donde pasen muchas cañerías (cocinas, baños), lo cual minimizará la probabilidad de posibles roturas de tuberías. El no tener un baño o una cocina cerca nos dará la posibilidad de usar más espacio en caso de que sea necesario agrandar el Data Center. Generalmente, es bastante problemático utilizar dichas habitaciones si están en uso, por la dificultad en su reemplazo. Eso asegurará que nuestro diseño cumpla con la flexibilidad que requiere cualquier Data Center.

Idealmente no debería estar en un piso alto, sobre todo si estamos en zonas afectadas por actividades sísmicas. El peso total estructural del Data Center es muchísimo más alto que el piso normal de cualquier tipo de oficinas, razón por la cual la mayoría de los Data Centers se encuentran al nivel del suelo. Solo para tener una referencia, el estándar de construcción de Data Centers TIA 942 exige una losa que soporte 1 200 kg/m^2, si tenemos en cuenta que un Rack con servidores puede pesar 1 000 kg en una superficie de 0,6 m^2, comprenderemos que no es un dato menor el lugar seleccionado para la instalación del Data Center.

Establecer la disponibilidad deseada

Cuando se diseña un Data Center, se deberá establecer su nivel de disponibilidad de acuerdo con el tipo de negocio, las necesidades de los sistemas y de los clientes. También se decidirá si se establecen todos los equipos en uno o más Data Centers. Al referimos a disponibilidad aludimos a todos los servicios necesarios para brindar continuidad al negocio en forma ininterrumpida, es decir, servicios de red, aire acondicionado, electricidad, etcétera.

La disponibilidad se representa como un lapso de tiempo, expresado en días, horas, minutos o segundos, los cuales estamos dispuestos a tolerar sin servicio.

Las empresas siempre buscan la mayor disponibilidad posible, porque una interrupción afecta directamente su productividad. La disponibilidad se expresa con nueves, a mayor cantidad de nueves más cerca estaremos del cien por ciento de disponibilidad.

Por ejemplo, si por tareas de mantenimiento eléctrico tendremos una interrupción eléctrica de dos horas por semestre, ello nos da una interrupción total de cuatro horas sobre las 8 760 horas del año. Dicho cálculo arrojará un porcentaje de disponibilidad del 99.954%. En la siguiente tabla, se detallan otras posibilidades.

Disponibilidad del Data Center

Nivel de disponibilidad	Porcentaje	Interrupción por año
Seis nueves	999.999	32 segundos
Cinco nueves	99.999	5 minutos, 15 segundos
Cuatro nueves	99.99	52 minutos, 36 segundos
Tres nueves	99.9	8 horas, 46 minutos
Dos nueves	99	3 días, 15 horas, 40 minutos

Seleccionar la estrategia de disponibilidad más adecuada para el negocio es una tarea que puede ser laboriosa, y donde intervendrán muchas personas de distintos sectores, desde Gerentes de IT hasta ejecutivos de Finanzas, incluso directivos de la compañía. Los gerentes deberán tener en claro que la decisión final será de suma importancia, y que de acuerdo con los niveles de calidad que se determinen para el Data Center, se incrementará la inversión, ya que implicará tener más sistemas redundantes, pero especialmente deberán considerar que la

base del negocio estará allí e impactará de manera directa en la actividad de la empresa.

Si hacemos referencia a un Data Center con presupuesto reducido deberemos establecer un orden de prioridades de acuerdo con las condiciones operativas para ser capaces de producir de manera confiable.

- ¿Cuántos dispositivos redundantes de refrigeración voy a colocar?
- ¿Cuántos dispositivos eléctricos voy a establecer?
- ¿Cuántos dispositivos de seguridad física necesitaré?
- ¿Cuántos proveedores de Internet o enlaces voy a contratar?

Muchas de estas preguntas pueden tener varias respuestas, que deberán ser analizadas sobre la base de las necesidades del negocio y el presupuesto.

Incluso puede darse la situación donde no toda la superficie del Data Center tiene la misma criticidad, y si éste presenta un buen diseño, se podrían focalizar los sistemas redundantes sólo a determinados equipos dentro del Data Center.

La estimación financiera de las posibles pérdidas es un argumento sólido a la hora de decidir la compra de un equipamiento redundante. Un generador de 200 kW puede costar 2 millones de dólares. Un sistema de UPS que soporte una interrupción de 20 minutos, puede costar 500 mil dólares. Si tenemos estimado que nuestro Data Center pierde 2.5 millones de dólares con una interrupción eléctrica de 5 minutos, entonces será viable la compra del generador y las UPS.

Debido a todos estos factores, el costo total de un Data Center puede resultar entre veinticinco o cincuenta veces más caro que una oficina normal de las mismas dimensiones

Al momento de la construcción, es recomendable utilizar los últimos estándares para todas las instalaciones que se prevea realizar (red, ventilación, incendio, entre otras), ya que éstos evolucionan rápidamente, y su actualización puede llegar a ser un costo mucho mayor si le lo compara con el momento inicial de construcción.

Para poder cumplir con todos estos objetivos y mantenernos dentro del presupuesto para la construcción, debemos invertir gran parte del tiempo en la **planificación**, ya que debemos ser capaces de cumplir con todos los objetivos, estándares necesarios, analizar propuestas, proveedores, materiales, etcétera.

La planificación de un Data Center debe hacerse pensando en una duración de al menos diez años, con capacidad de crecimiento en densidad y tamaño. Pero eso no quiere decir sobredimensionarse al día de hoy al máximo posible, sabiendo que dentro de diez años voy a necesitar más capacidad de enfriamiento. Una buena alternativa sería establecer aéreas donde se pueden colocar más equipos de enfriamiento cuando lleguen los servidores, que requerirán mayor capacidad de refrigeración.

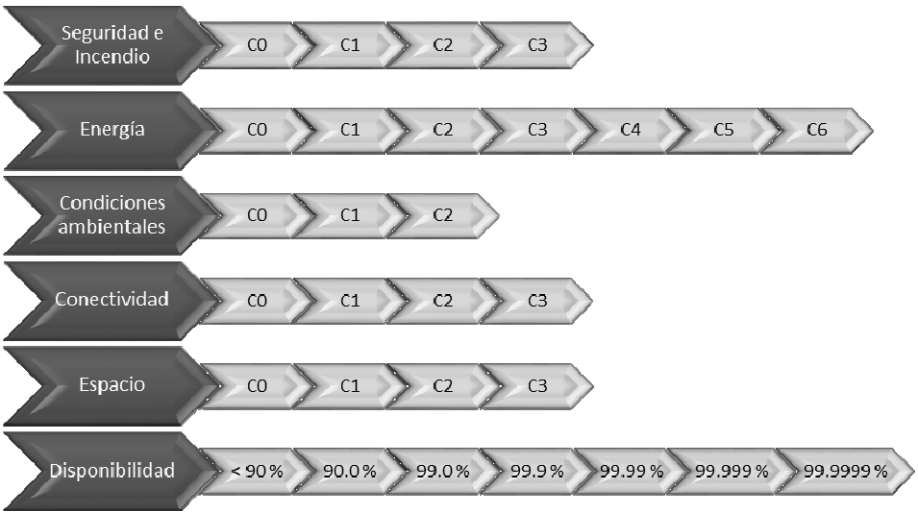
Cuando planificamos debemos poner mayor foco en las cosas que son más difíciles de modificar, ya que revertir esos cambios puede ser más difícil y costo.

Planificación de elementos críticos

- **Seguridad:** la protección de los activos es uno de los temas más importantes a tener en cuenta, ya que la información es invaluable.
- **Espacio:** el suficiente para los equipos así como para la operación y el mantenimiento, como por ejemplo los Racks.
- **Energía:** contar con la cantidad suficiente como para operar así como los elementos de respaldos eléctricos necesarios para garantizar la operatoria en caso de alguna falla.
- **Condiciones ambientales**: poseer la refrigeración adecuada para mantener los equipos en condiciones óptimas de operación durante todo el año.
- **Conectividad:** el centro de cómputos debe contar con servicios de banda ancha para poder operar.

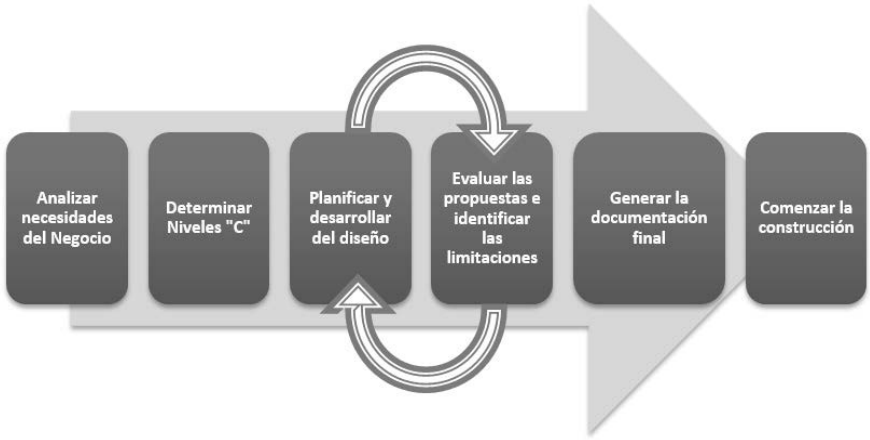
La limitación en alguno de estos elementos puede llegar a producir un cuello de botella, en el mejor de los casos. Por eso, es fundamental no fallar en la etapa de diseño, teniendo en cuenta todos los aspectos mencionados.

Un buen ejercicio a la hora de establecer el diseño del Data Center sería definir cuáles son las expectativas y requerimientos que se desean alcanzar según al tipo de negocio al cual se le proveerá el servicio, evaluando para cada uno de los pilares básicos del Data Center el nivel de criticidad **(C*)** que se establecerá. Recordemos que a medida que se elevan los niveles de criticidad, se elevan los costos. Pero también hay que estimar que no disponer de un Data Center en las condiciones adecuadas puede llegar a provocar fallas que generen mayores costos que los que se han pretendido ahorrar. **La clave está en encontrar el balance adecuado, siempre teniendo en cuenta el crecimiento a largo plazo.**



El diseño de la solución sobre la base del análisis de las necesidades del negocio puede tener muchas iteraciones con respecto a la evaluación de la propuesta real en relación al presupuesto disponible, ya que puede haber varias etapas de ajustes en relación a las necesidades, el equilibrio financiero, costos, tiempos, qué riesgos estamos dispuestos a asumir de no hacer dicha inversión, Por lo cual, hasta que se llega a la etapa donde se establece el diseño final para proceder a su documentación se puede atravesar muchas instancias de rediseño y evaluación.

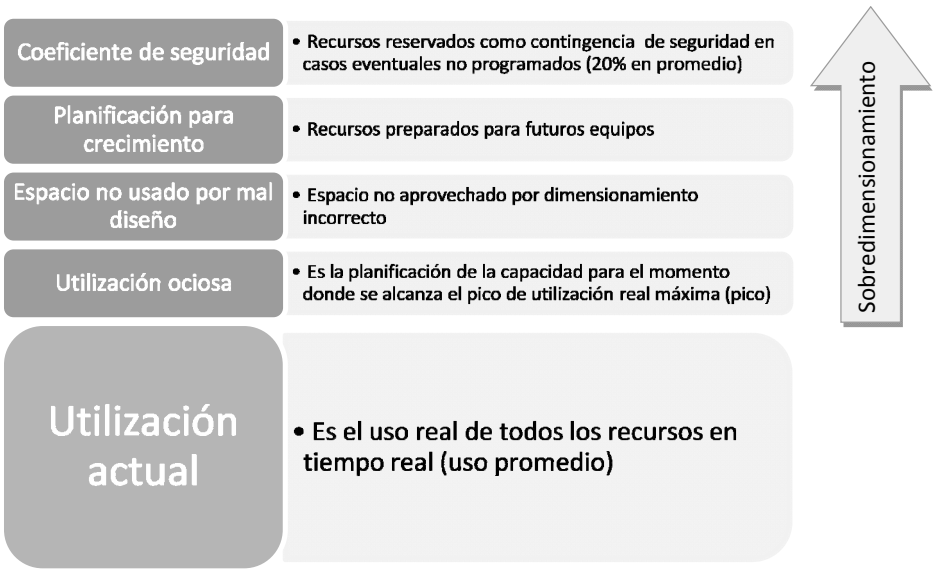
Si construyéramos una línea de tiempo de las etapas de la construcción de un Data Center sería así:



Como parte de la planificación se deben tener en cuenta las capacidades no aprovechadas de todos los elementos que conforman los servicios del Data Center (refrigeración, electricidad, UPS, red, etcétera.). Ellos generan un desperdicio de recursos, por los cual, es ideal que puedan ser activados de manera manual o automática, de forma tal de no generar un gasto innecesario.

Por regla general para todas las planificaciones, se considera un 20% adicional como coeficiente de seguridad, como prevención a eventos inesperados.

La administración de la capacidad de los recursos en función de la planificación se puede ver en el siguiente gráfico:



Evaluación y análisis de costos

Cuando se evalúa el costo de un Data Center financieramente se hace difícil de calcular el TCO[1] al momento de construcción. La premisa fundamental del TCO es que los costos iniciales directos de cualquier proyecto son solo una pequeña parte de sus costos totales, es decir, no solo se incluye el costo inicial de compra o inversión, sino que se le deben sumar todos los gastos que generará a lo largo de la vida útil, como pueden ser el consumo eléctrico, repuestos, mantenimiento, entre otros.

[1] El TCO es el costo total del propietario. (Total Cost Ownership), y es concepto creado por Grupo Gartner en 1987.

Para entender el concepto, hagamos un ejemplo muy simple:

Tenemos la impresora A: $ 500

Tenemos la impresora B: $ 800

Ambas son láser blanco y negro, tienen la misma velocidad de impresión en páginas por minuto, la misma calidad de impresión, el mismo consumo eléctrico, y el mismo costo de otros repuestos. Su vida útil es de 5 años. Se estima que se imprimirán 5 000 páginas por año. El cartucho para la impresora A cuesta $ 80 e imprime 1 000 páginas. El cartucho para la impresora B cuesta $ 50 e imprime 2 500 páginas.

*TCO A = $500 + ($80*5)*5 (se necesitan 5 cartuchos por año) x 5 años*

TCO A = $2 500

*TCO B = $800 + ($50*2)*5 (se necesitan 2 cartuchos por año) x 5 años*

TCO B = $1 300

Si bien a simple vista la impresora A valía casi la mitad de la B, evaluándola a lo largo de toda su vida útil resulta que cuesta más del doble que la impresora B.

Para construir el ejemplo simple solo se tomó como variable el precio del cartucho, pero todas las características que sean distintas, por ejemplo, el consumo eléctrico, deberían evaluarse de la misma forma.

Otro concepto a tener en cuenta desde el punto de vista financiero es el **ROI** (Retorno sobre la inversión, Return of Investment), que se utiliza para reflejar económicamente la viabilidad un proyecto o equipo a lo largo del tiempo, facilitando la toma de decisiones. Se trata de una tasa de retorno que compara los beneficios netos de un proyecto a lo largo del tiempo en relación a los costos totales. Para explicarlo brevemente, el ROI es el resultado de los ingresos netos menos los gastos, dividido por los gastos de la inversión, y multiplicado por 100%.

$$ROI(\%) = \frac{(Ingresos - Gastos)}{Invesión} \times 100$$

En otras palabras, ¿Cuál es el valor añadido de una inversión en relación con el sacrificio financiero que hay que hacer para que sea rentable? Por tanto, al calcular el ROI es de vital importancia presentar un desglose tan exhaustivo como sea posible de los gastos y de los ingresos atribuibles. Para ello, los factores que se mencionan se expresan en cifras financieras. Para entender el concepto hagamos un ejemplo muy simple:

Tenemos un aire acondicionado obsoleto que presenta desperfectos de manera muy frecuente, razón por la cual se evalúa comprar un equipo de iguales características, pero al ser más moderno tiene menor consumo eléctrico.

El equipo nuevo cuesta $10 000 (con tres años de mantenimiento y repuestos sin cargo) más $500 por la instalación. En los últimos años, el gasto promedio de mantenimiento y reparación fue de $3 000.

Se estima un ahorro en el consumo eléctrico equivalente a $1 000 por año.

Entonces el ROI será:

$$ROI\ (35\ \%) = \frac{((3.000 + 1.000) - 500)}{10.000} \times 100$$

En el ejemplo, se muestra un ROI de 35%, ya que consideramos como ingresos los $3 000 (del mantenimiento) más los $1 000 del ahorro eléctrico, y le restamos $500 de la instalación. Pero hay que tener en cuenta que un equipo de estas características tiene una vida útil de muchos años; por ello, si realmente quisiéramos hacer el ROI correctamente, deberíamos analizarlo en función del tiempo. Lo cual requiere hacer un análisis más profundo, utilizando el método de flujo de caja (*cash flow*), que si bien es un cálculo un poco más complejo, puede analizar de manera más adecuada y exacta en cuánto tiempo se recuperará la inversión inicial con un nuevo aire acondicionado.

Sigamos con el ejemplo anterior, pero para poder hacer el análisis detallado necesitaremos agregar más datos. Vamos a considerar una tasa de descuento o costo de oportunidad del 15% anual (que está definida como una actualización de rendimientos futuros esperados de dicha inversión, financieramente, sería aplicar el concepto de tasa de interés). Dicha tasa se utiliza para actualizar los valores totales de cada año a su correspondiente VAN (Valor Actual Neto).

A partir del cuarto año, los gastos de mantenimiento serán de $400 (ya que serán realizados por personal interno por ser bastantes simples), y se estiman gastos de insumos por $600 en el cuarto año, y $1 000 en el quinto año.

La amortización del equipo está planificada para hacerse a diez años, sin costo de desguace.

Año	0	1	2	3	4	5
Inversión inicial	-10.000					
Ahorro energía		1.000	1.000	1.000	1.000	1.000
Ahorro Mantenimiento		3.000	3.000	3.000	3.000	3.000
Insumos		0	0	0	-600	-1.000
Mano de Obra	-500	0	0	0	-400	-400
Amortización		-1.000	-1.000	-1.000	-1.000	-1.000
Utilidad Bruta		**3.000**	**3.000**	**3.000**	**2.000**	**1.600**
Impuestos (35%)		-1.050	-1.050	-1.050	-700	-560
Utilidad Neta		**1.950**	**1.950**	**1.950**	**1.300**	**1.040**
Flujo de Caja	**-10.500**	**4.950**	**4.950**	**4.950**	**3.300**	**2.640**

VAN con tasa 15%:	-10.500	4.304	3.743	3.255	1.887	1.313

VAN Total	**$4,001**
ROI	**2,78 Años**

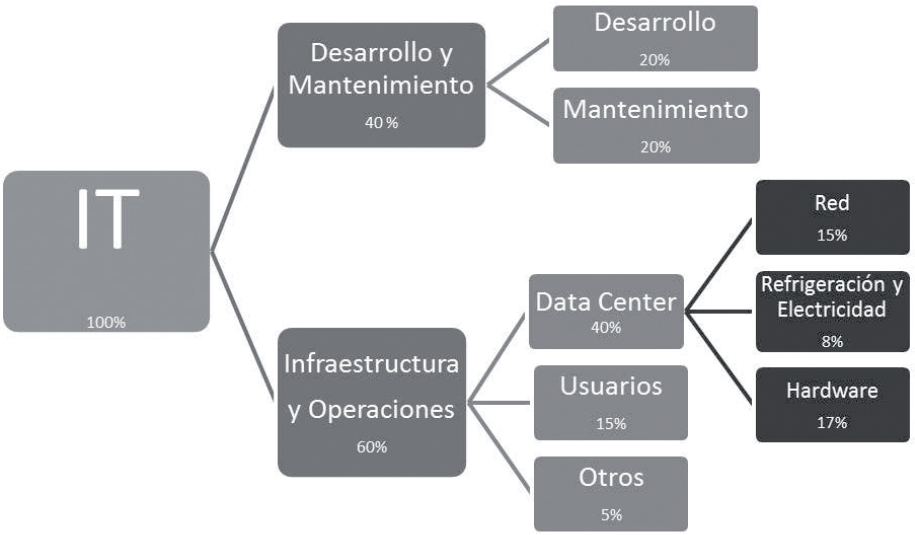
Monto Actualizado	Años
11.302	3
10.500	**2,78712612**

Haciendo una inversión inicial de $10 500, la inversión se recupera en menos de tres años.

Finalmente, en el capítulo 11, se abordarán cuáles son las mejores prácticas al momento de construir un Data Center desde el inicio.

Presupuesto de IT típico de una empresa

Por lo general, las empresas utilizan una parte bastante importante de su presupuesto total para mantener su infraestructura de Data Center. Aquí se ilustra un ejemplo típico promedio:



Éste es un caso ilustrativo (basado en un modelo de McKinsey & Company, del 2008), ya que en la práctica, cada empresa maneja su presupuesto sobre la base de las necesidades del negocio, tipo de industria o ramo, y el momento particular que esté atravesando. De todas formas, constituye un ejemplo promedio de cómo se distribuyen los porcentajes, habitualmente, aunque también pueden variar según las necesidades del negocio de año a año, como podría ser el lanzamiento de una nueva plataforma Web.

Componentes básicos

3

"Solo porque algo no haga lo que era previsto no quiere decir que sea inútil el esfuerzo".

-- Thomas Alva Edison (1847-1931) Inventor estadounidense

Dentro del Data Center existen muchos elementos que definen la estructura básica de los cuales dependerá su confiabilidad. En este capítulo se enumerarán los principales y sus características más importantes.

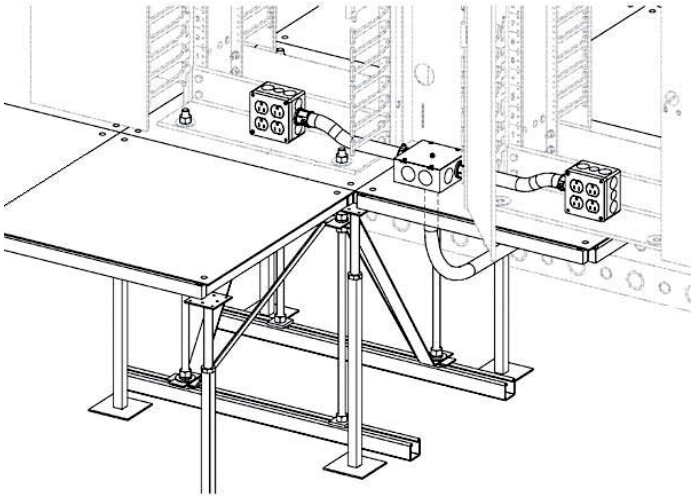
Piso técnico

El piso técnico (también llamado piso elevado o piso falso) es un elemento de diseño presente en la mayoría de los Data Centers que hayan sido construidos antes del año 2000, pero la tendencia actual de los Data Centers nuevos es distinta. Se imponen otras tecnologías y metodologías más modernas que permiten un diseño que no requiere piso elevado, ofreciendo mayor agilidad y flexibilidad, colocando los Rack directamente sobre el piso (no elevado), y en lugar de pasar los cables y el aire frío por debajo del piso, se instalan los cables por sobre los Racks, y el enfriamiento se realiza mediante ductos direccionales superiores. Esta nueva estrategia permite ahorrar el costo de instalación del piso técnico brindando mayores prestaciones generales.

El piso técnico está compuesto por barras de soporte de acero y paneles de aluminio que generan un espacio hueco entre el piso real y el piso elevado donde se apoyan los equipos dentro del Data Center.

Este espacio es utilizado para pasar cables red, cables eléctricos, fibra óptica, etcétera. El piso técnico suele tener una distancia con el piso real de entre 45 cm y 70 cm, según la cantidad de cables que se necesiten para el proyecto.

Su función principal es proveer un ducto por donde fluirá el aire que refrigerará los equipos y también por donde pasarán los cables.

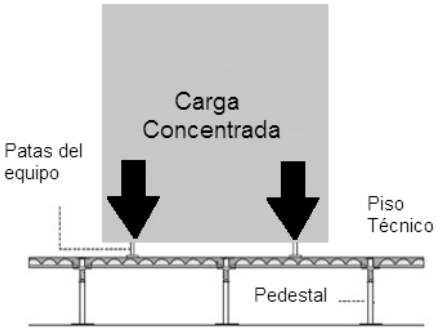


Pedestales

Los pedestales sirven como minicolumnas de soporte donde estarán apoyadas las guías (o travesaños) y las placas del piso técnico. Para seleccionar el tipo de pedestal se deberá tener en cuenta la altura deseada para el piso técnico, el peso por metro cuadrado que deberá soporta y el peso máximo posible. Su altura puede variar entre los 4 cm y los 70 cm con 2 cm de regulación.

Para la fijación de los pedestales a la carpeta se puede utilizar adhesivo especial y complementariamente se utilizan tornillos o clavos.

Placa de piso o paneles

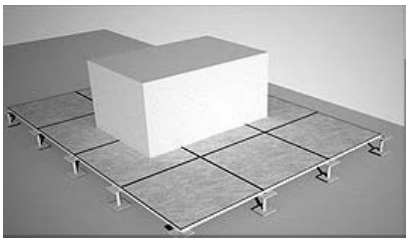


Son las baldosas que forman el piso técnico. Ellas están apoyadas sobre los pedestales, pueden ser de distintos materiales, pero las más recomendables son las de acero. También pueden ser de distintos espesores, para soportar el peso acorde a nuestras necesidades.

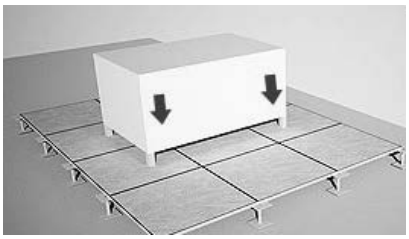
El tamaño de mayor difusión es 60 cm x 60 cm, aunque es posible encontrar fabricantes que utilicen otros tamaños (61 x 61, 70 x 70, etcétera).

Un dato no menor a tener en cuenta son las cargas concentradas o cargas puntuales. Las cargas concentradas son

puntos de pequeña superficie que soportan todo el peso de la carga. Por ejemplo: aplicadas en una zona de 25 mm x 25 mm y se miden en kilogramos (kg) o kilonewtons (kN). Normalmente se deben al mobiliario fijo provistos de patas que ejercen una carga puntual más fuerte que una carga que tendría el mismo mobiliario con una superficie de apoyo mayor. Esto le permite distribuir su peso en una zona más amplia, disminuyendo así la concentración de la carga.



Carga distribuida



Carga concentrada

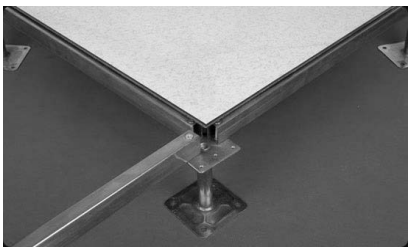
La carga límite se define como el punto hasta el cual una baldosa puede soportar un cierto peso sin experimentar fallas en el material. Este valor se fija para evitar potenciales desmoronamientos del piso técnico, y dependerá del material seleccionado para la baldosa, ya que existen de distintos espesores.

Para proporcionar un nivel de seguridad adecuado, la carga límite debe alcanzar por lo menos el resultado de la carga concentrada de diseño multiplicada por 3. Eso es conocido como el coeficiente de seguridad.

Tipos de baldosas

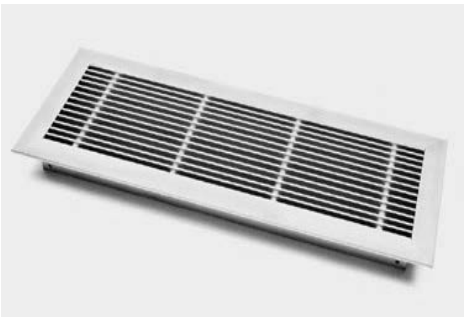
Espesor	Carga uniforme Kg/m2	Carga concentrada Kg/50mm2	Carga Máx. concentrada antes de ruptura Kg/50mm2	Carga Rodante Kg/50 mm2	Carga Impacto Kg	Peso de Baldosa en Kg
Medio	1220	370	1110	370	60	14
Grueso	2040	465	1395	460	60	15
Muy Grueso	3060	580	1740	580	70	16

Travesaños



Son barrales rectangulares utilizadas para la unión de los pedestales, la medida estándar es de 21 mm x 30 mm x 1 mm, y se fijan a los pedestales con tornillos de ¼". Los travesaños son de acero o zinc endurecido, que le darán sustentabilidad y estructura a todo el piso en su conjunto para así formar una estructura robusta, sólida y segura.

Rejilla de aluminio



Las rejillas se utilizan para controlar el flujo de aire frío que ingresa por debajo del piso técnico y disminuir la temperatura en los equipos. El tamaño de las rejillas puede variar entre 46 cm y 60 cm.

Siempre están ubicadas frente al Rack, donde se encuentra la toma de aire de los equipos, y son un factor determinante a la hora de definir el diseño de los pasillos que optimizará la refrigeración del Data Center. En el capítulo 5, se profundizará la importancia del la ubicación de las rejillas para establecer los pasillos fríos y cálidos.

En el caso de que la refrigeración sea enviada por tuberías que están por encima de los Racks, aquellas deberán estar direccionadas hacia el frente de éstos.

El flujo de aire en todas las rejillas deberá ser constante, asegurando la uniformidad de la temperatura de la sala.

En el capítulo 5, se desarrollará el tema de enfriamiento y la importancia de la correcta fluidez del aire frío en el ingreso a los equipos.

Consideraciones para la implementación del piso técnico

Es necesario contar con un plano o boceto del lugar donde se implementará el piso técnico para planificar la forma en que se colocarán las baldosas, cortes necesarios realizar en las baldosas para las terminaciones, esquinas y columnas. Esa planificación de las actividades permitirá acelerar los tiempos y reducir los costos del trabajo.

La loza o carpeta donde se colocarán los pedestales debe estar completamente limpia, libre de cualquier contaminante que pueda dañar los pedestales y totalmente nivelada.

El responsable técnico deberá analizar e indicar si la carpeta cuenta con una superficie lo suficientemente lisa para el propósito destinado.

La resistencia, composición y condición general de la loza y carpetas provista por el cliente deben ser las adecuadas para la instalación del piso técnico. Las lozas de cemento pulido son las más recomendables, por su acabado y alisado. Si se trata de una construcción nueva, el cemento debe estar fraguado y seco.

Las compañías dedicadas a la instalación utilizan niveladores láser[1]. Luego se instalan los travesaños, controlando en todo el proceso el nivel y sus posibles variaciones, de tal manera que se puedan aplicar las correcciones oportunamente.

El responsable técnico propondrá el diseño, siempre tratando de minimizar la cantidad de cortes para así optimizar tiempos y materiales.

Umbral de tolerancia para la terminación del piso:

- La separación máxima entre dos placas no debe superar 1 mm.
- El sistema no debe apoyarse en las paredes o columnas existentes, y su máxima separación no debe superar los 2 mm. En el caso de los niveles se acepta una diferencia de 1,5 mm en un máximo de 3 m, y de 2,5 mm en toda la planta.

Tamaño del Data Center

En el caso en que estemos diseñando un Data Center dedicado para una sola empresa, la decisión del tamaño deberá ser consensuada con los Gerentes de IT (Administradores de red, Administradores de Servidores, CIO, etcétera.) Ellos aportaran información importante en relación a:

[1] Amplificación de luz por emisión de radiación estimulada (Light Amplification by Stimulated Emission of Radiation).

- Planificación estratégica a mediano y largo plazo.
- Estrategias de virtualización.
- Identificación de equipos críticos para el negocio.
- Posibilidad de fusión o adquisición de otras empresas.

Todos estos factores darán un aporte importante al momento de analizar y calcular la superficie que necesitamos para el Data Center.

La cantidad de servidores puede ser una unidad de medición engañosa, un servidor tener un tamaño pequeño o de un Rack completo, quizás el criterio más acertado sea considerar el peso, calor que se generará y la potencia eléctrica necesaria para su funcionamiento.

Cualquier equipo que sea distinto del estándar (ya sea por características físicas o de funcionamiento) por el motivo que sea deberá considerarse al momento del diseño.

Otros factores adicionales a considerar a la hora de diseñar son:

- Ancho de los pasillos entre Racks: está condicionado por la superficie total del diseño, pero generalmente oscila entre los 90 cm y 120 cm.
- Donde se colocaran las unidades de refrigeración y UPS: generalmente se ubican dentro del área destinada a los servidores, pero no es estrictamente necesario. Pueden estar ubicados en el exterior de la sala en un ambiente contiguo con las debidas conexiones.
- Rampa: en el caso en que se utilice un piso elevado, se deberá considerar una rampa para poder entrar y extraer el equipo pesado y así facilitar el acceso.

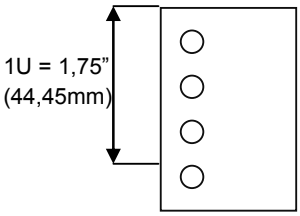
Racks

Un Rack es un bastidor metálico cuyo fin es alojar equipamiento informático. Su principal función es proteger los equipos, manteniéndolos ordenados, seguros y optimizando el espacio físico. Las medidas están normalizadas para lograr compatibilidad con cualquier fabricante de hardware. La medida más común es de 19 pulgadas (600 mm) de ancho, pero también existen Racks de 23 pulgadas homologados por EIA-310-D[2]. Los Racks de huecos cuadrados son más populares en el mercado por simplificar la instalación de las guías.

[2] Norma que define las medidas estándar para los Racks creada por Alianza de Industrias Electrónicas (Electronic Industries Alliance).

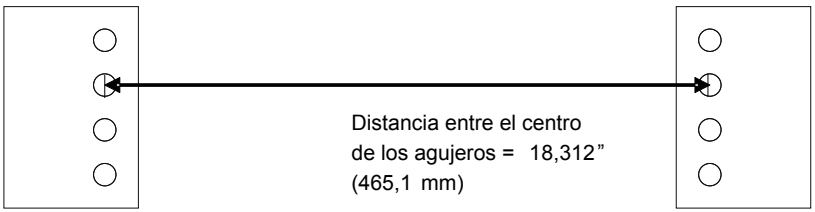
Espacio vertical

Los Racks poseen una guía con agujeros equidistantes en ambos laterales que sirven de sostén para el equipamiento informático. Esa guía cuenta con un patrón para la ubicación del equipamiento, eso equivale a 1U o RU (por sus siglas en inglés Rack Unit) y expresado en unidades métricas equivale a 1,75 pulgadas o 44.45 mm (espacio usable vertical). Comúnmente los fabricantes de servidores, *switchs*, paneles, en las especificaciones técnicas del equipo aclaran cuantas U ocupan. Para servidores lo más común son, 1U, 2U o 4U, por ejemplo, un *switch* de 24 puertos ocupa 1U.



Espacio horizontal

La distancia horizontal entre las guías también está definida por el mismo estándar, y debe ser respetado en todo el Rack. Esta distancia es 18.312" o 465.1 mm.



Si bien existen varias medidas de Racks de distintos fabricantes, en el mercado se pueden encontrar Racks de varias medidas de ancho, que pueden variar según las necesidades propias de los equipos que allí se colocarán. Por lo general, un Rack estándar tiene estas características:

Peso neto	120 Kg
Altura máxima	1991.00 mm
Ancho máximo	600.00 mm
Profundidad máxima	1070.00 mm
Capacidad de carga	1360 Kg
Capacidad	42U
Color	Negro, Gris o Blanco

La altura de los Racks puede variar mucho, se pueden encontrar modelos de distintas alturas como: 24U, 30U, 36U, 42U, 44U, 51U. Los más populares en el mercado son los de 42U debido a su relación costo/beneficio.

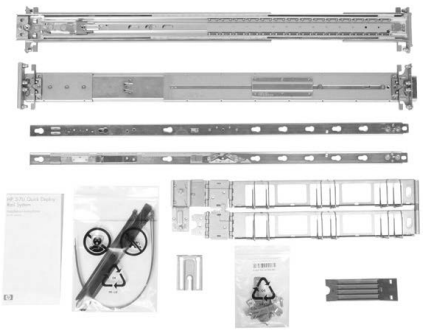
Es muy importante que los Racks cumplan con la norma EIA-310-D, en ella se establecen las pautas fundamentales de cómo y dónde se colocaran los agujeros y las distancias entre ellos. Estas serán las guías para colocar el equipamiento informático.

La mayoría de los servidores están diseñados para ser colocados en los Racks, mediante guías deslizables que se colocan en los laterales de los servidores, y se montan en las guías fijas que se colocan en los Racks. Esto otorga una gran versatilidad y movilidad dentro del Rack al momento de realizar tareas de mantenimiento en los servidores o de reemplazar partes sin perjudicar a otros servidores. Si el servidor está colocado con la guía deslizable, el administrador solo tiene que tirar de él hacia adelante, como si fuera un cajón (asegurándose que los cables sean lo suficientemente largos), y podrá realizar las tareas de mantenimiento sin tener que apagar el servidor ni afectar otros servidores.

Las piezas de hardware que se pueden cambiar sin apagar el servidor se llaman *hot swap*. En la actualidad, la mayoría de las fuentes de alimentación y los discos rígidos que forman parte de un RAID[3] pueden ser reemplazados **en caliente**, e incluso los servidores más avanzados permiten cambiar procesadores o módulos de memoria. De todos modos, **siempre deben referirse al manual del fabricante para saber cuáles piezas pueden ser cambiadas en caliente y cuáles no**.

Para que el aire frío ingrese por el frente del Rack, la puerta debe ser un panel perforado como si fuera una rejilla y protegido por una cerradura. En la parte trasera, debe tener espacio suficiente para pasar los cables de red y electricidad por los laterales, permitiendo la correcta circulación del flujo de aire caliente que sale expulsado.

En las zonas de riesgo sísmicos se deben tomar precauciones de como ajustar los Racks, ya que tienen particularidades especiales para brindarle más robustez. Por ejemplo, se requiere colocar una chapa angular para reforzar los vértices del Rack; de esa forma, se reducen las posibles deformaciones estructurales que puedan dañan los equipos.



Para montar los equipos en los Racks

[3] Redundant Array of Independent Disks es un conjunto de discos independientes que funcionan lógicamente como un solo disco de gran tamaño con capacidad de redundancia a fallos.

se utilizan guías, o también llamados *Rail kits*. Los rieles se instalan en los laterales de los servidores para luego ajustarlos a las guías que se encuentran a los lados de los Racks; de esa forma, el servidor puede ser extraído del Rack hacia la parte frontal, como si fuera un cajón de una cajonera, y así efectuar el mantenimiento necesario sin tener que mover otros servidores ni desconectar ningún cable.

En el mercado también existen Racks abiertos, que en realidad funcionan como **marcos** para colocar servidores, pero no se los puede considerar como Racks realmente, ya que no tienen todas las prestaciones, pero sí son útiles para algunas funciones y se utilizan frecuentemente.

En el mercado hay dos tipos de Racks abiertos, los de dos y los de cuatro postes, aunque estos últimos son muy poco usados:

Rack abierto de dos postes

- Ventajas
  - Baratos y fáciles de armar.
  - Ideales para organizar el cableado estructurado.
- Desventajas
  - No brindan seguridad.
  - No hay control del flujo del aire.
  - Tienen poca estabilidad y soportan poco peso.

Rack abierto de cuatro postes

Son más versátiles. En algunos casos son usados para servidores y equipos de telecomunicaciones. Son un poco más estables.

- Ventajas
  - Baratos y fáciles de armar.
- Desventajas
  - No brindan seguridad.
  - No hay control del flujo del aire.
  - Gozan de poca estabilidad.

Si bien económicamente pueden resultar más beneficiosos, al momento de decidir la compra de un Rack abierto, se debe evaluar si es realmente más conveniente que un Rack común, ya que éste tiene muchas más prestaciones, permitiendo alojar más equipos, brindando flexibilidad, seguridad, escalabilidad y disponibilidad para futuros cambios en la estructura del Data Center.

De acuerdo con las necesidades del Data Center, un Rack puede llegar a requerir hasta 2 000 cables UTP conectados entre entrantes y salientes.

Como se mencionó anteriormente, un Rack es un elemento pasivo dentro del Data Center, pero de gran utilidad. Y si bien existe una importante variedad de Racks en el mercado, la pregunta adecuada sería: ¿cómo elegir el Rack ideal según las necesidades de nuestro Data Center?

Aquí se detallan algunos puntos a tener en cuenta al momento de la compra. Estos atributos deben ser considerados, porque nos ayudarán al hacer la elección, evitando las equivocaciones:

- Costo ciclo de vida.
  - Estandarización: es recomendado instalar Racks que cumplan con los estándares internacionales, ya que mejoran el recupero de la inversión debido a la flexibilidad y agilidad que otorgan. Siempre se debe verificar la etiqueta de compatibilidad. En especial, las normas EIA-310-D, CEA-310-E, DIN 41494.
  - Velocidad de instalación: ¿qué tan rápido necesito tener el Rack disponible?
- Disponibilidad.
  - Flujo de aire inadecuado: el Rack no permite una correcta circulación del aire pudiendo afectar los equipos allí almacenados.
  - Redundancia eléctrica inadecuada: el Rack no permite instalar una fuente de alimentación redundante.
  - Si el equipamiento es crítico, el Rack debe cumplir con los requisitos de seguridad.
  - Si el Data Center está ubicado en zona de riesgo sísmico, debemos adquirir un Rack reforzado especialmente diseñado para tal fin.
- Mantenimiento y servicio.
  - Demora en la migración de servidores: si el Rack no es de buena calidad, es posible que los agujeros para la instalación de las guías y los rieles sea defectuosa. Eso puede generar demoras a la hora de la instalación de los equipos.
  - Dificultad para manejar el cableado.

- Flexibilidad.
  - Si existen cambios frecuentes en refrigeración y electricidad, se debe pensar en Racks que provean versatilidad.
  - Ídem al punto anterior, si hay cambios frecuentes de equipos entre Racks, aunque no es una práctica recomendada.
- Monitoreo.
  - Es deseable que los Racks puedan soportar sensores térmicos para detectar problemas.
  - Posibilidad de colocar sensores en la puerta del Racks con alarmas para detectar no autorizados.

Estadísticamente, el espacio utilizado en los Racks en grandes Data Center es menor del 50%. Lo cual puede suceder por dos motivos:

- **Fallas en la planificación:** no se aprovecha correctamente el espacio por desorganización o se cometen errores en el cálculo de la superficie necesaria, ya que los Racks abiertos son ideales para el cableado estructurado, pero se requiere considerar un espacio extra para los organizadores verticales.
- **Intencionalmente:** con el fin de mantener una estrategia de distribución de calor equitativa en todos los Racks no se maximiza el espacio para no tener que cambiar la estrategia de refrigeración por el cambio de densidad en ciertos Racks. Pero esto debe ser vigilado muy de cerca, ya que se deberá analizar en qué momento deja de ser económicamente viable tener Racks desaprovechados, en lugar de aumentar la concentración aprovechando el espacio, y hacer cambios en la estrategia de refrigeración.

Servidores y equipos de comunicaciones

Los equipos de comunicaciones como *routers*, *switchs*, *firewalls*, centrales telefónicas, entre otros, requieren baja capacidad de procesamiento para cumplir su objetivo. Por eso son unidades que tiene poco consumo eléctrico, y por ende generan poco calor.

Por otro lado los servidores son más complejos y poseen muchísimos componentes: memorias, discos, procesadores, etcétera. Por eso, consumen más electricidad y generan más calor.

De todos esos componentes del servidor, el que más consume es el procesador. Pese a que las empresas fabricantes de procesadores están permanente enfocadas en producir procesadores de bajo consumo, la búsqueda de hacerlos más potentes (para satisfacer las necesidades de los usuarios) lleva a que el procesador siga siendo el componente que más energía consume. El procesador

puede llegar a consumir el 45% de la energía total necesaria de un servidor para funcionar (y también es el componente que más calor genera). Este dato no es menor, sobre todo a la hora de realizar la compra de los equipos. Por eso, es conveniente prestar atención al consumo eléctrico, ya que puede representar un ahorro importante en el futuro.

Otro elemento a tener en cuenta son las fuentes de alimentación. En 2003, la eficiencia de las fuentes era en promedio del 72%. Los modelos salidos a partir del 2006, ya alcanzaba una eficiencia promedio de 79% mientras que en 2012 fue del 90% o más. Lo mismo ocurre con los procesadores.

Algunos servidores poseen capacidad de **autoapagado** si la temperatura excede el límite máximo establecido por el fabricante (generalmente entre 40 °C y 45 °C) como medida preventiva para evitar daños mayores; los servidores se apagan automáticamente, evitando así que se quemen transistores, memorias o dañen físicamente los discos rígidos entre otros inconvenientes.

Notablemente, la cantidad de transistores dentro del procesador aumenta según **La Ley de Moore**[4] enunciada en 1965, que dice: "aproximadamente cada 18 meses se duplicará el número de transistores en un circuito integrado". Pese a haber sido formulada hace muchos años atrás, notablemente esta ley continúa vigente hasta el día de hoy.

Desde el año 1999, los teléfonos móviles sobrepasan la capacidad de cálculo que tenía la nave Apolo XI, cuando llegó a la Luna en 1969; y para el año 2005, una PDA superaba a la capacidad total de procesamiento utilizada en el centro de mando de Houston (Texas) por la NASA para dicha misión.

Por esta evolución es que nada tiene que ver el consumo eléctrico, la capacidad de procesamiento y el calor que genera un servidor de hace 10 años con uno de hace 5 años, o con uno que se pueda conseguir hoy en día, tampoco los gastos que éste puede generar. Según un estudio reciente de Kenneth Brill, fundador del Uptime Institute en 1993, los gastos de consumo eléctrico de un servidor en cuatro años igualarán al costo de adquisición del equipo en sí mismo.

Monitoreo ambiental

Prevenir una falla o comenzar a trabajar en un problema antes de que los usuarios finales se den cuenta puede ser una ventaja muy significativa, ya que permitirá restablecer los servicios más rápidamente. Aquí es fundamental la proactividad y el saber definir correctamente los umbrales en los cuales se dispararán las alertas a

[4] Es una afirmación empírica formulada en 1965, por el Ph.D. físico-químico estadounidense Gordon Moore (cofundador de Intel), en la revista *Electronics Magazine*.

las personas indicadas. La comunicación fluida con todas las partes afectadas es de gran ayuda al momento de resolver el problema.

Sensores de temperatura

Múltiples factores influyen en la cantidad y ubicación de los sensores de temperatura en un Data Center, como: el diseño del Data Center, la carga total, la capacidad, el porcentaje de utilización del Data Center, la eficiencia eléctrica, etcétera.

En el modo clásico de funcionamiento de un Data Center, la mayoría no consideraba el costo y la eficiencia para alcanzar el estado de enfriamiento correcto, pero esa tendencia está cambiando por una metodología más ecológica, pensando en el medio ambiente y en la reducción de costos operativos.

Para mejorar las prácticas en torno a la colocación de sensores de temperatura se recomienda considerar los siguientes puntos:

- Ubicación ideal del sensor:
  - Colocar un sensor de temperatura en la parte frontal de los Racks (a una altura de entre 1.40 m y 1.70 m del Rack).
  - Colocar un sensor de temperatura en la parte posterior de cada cinco Racks (a una altura de entre 1.40 m y 1.70 m del Rack).

Sensores de humedad

Los sensores de humedad normalmente se colocan en los pasillos fríos, manteniendo una distancia lo bastante grande uno de otro, de manera que se puedan tener muestras en distintos puntos. Asimismo, se recomienda tomar en cuenta:

- Ubicación ideal del sensor:
  - Colocar un sensor de humedad por fila en la parte frontal del Rack a la mitad de la fila.

Sensores de líquidos

Los sensores de fuga de líquidos se deben colocar en el piso cerca de las potenciales fuentes de fuga, como por ejemplo, las unidades de refrigeración o cañerías.

Sensores de puerta

Los sensores de puertas se deben colocar en todas las puertas que proporcionan acceso al Data Center (incluso si existe un sistema de acceso restringido ya instalado) y en los Racks, o al menos en aquellos específicos que sean considerados críticos.

El cableado tradicional en sistemas de monitoreo ambiental suele consistir en sensores ambientales que se instalan en los Racks y son accesibles a través de la red TCP/IP, para así centralizar toda la información en una sola consola, o algún software del proveedor de los sensores. De esta manera, es factible enviar alarmas de notificación cuando se sobrepasen los umbrales establecidos como normales. También existen sensores que son inalámbricos, que facilitan la instalación, ocupan menos lugar, y el costo de instalación es menor.

Es importante que el software de monitoreo sea escalable, permita ubicar e identificar los sensores, ya que en caso de desperfectos facilita la localización, gestión centralizada, varios métodos de notificación (como SNMP, correo electrónico, HTTP Post), además debe tener capacidad de conexión con otras consolas de monitoreo, para una integración global.

Una vez que se eligieron y colocaron los sensores, el paso siguiente es la recolección y el análisis de los datos que éstos reciben. Es recomendable que en vez de enviar todos los datos de los sensores directamente a un punto central de recolección, fuera mejor tener varios puntos de recolección distribuidos, con funciones de alertas y notificaciones en cada uno de ellos. Esto no solo elimina el riesgo del punto único de falla, sino que ofrece soporte al monitoreo en puntos de uso de salas de servidores remotas y salas de telecomunicaciones. Luego, los dispositivos recolectores se comunican a través de la red IP con un sistema central de monitoreo.

La definición de los umbrales mínimos para la de activación de las alarmas deberá ser definido de forma centralizada, teniendo la posibilidad de cambiar esos límites según lo merezca la situación (por ejemplo, cambios de estación).

Existe una gran variedad de proveedores de sensores (algunos inalámbricos, que simplifican la tarea de instalación) como ser APC, ITWatchdogs, SafetyNet, SynapSense, entre otros. Deberán analizarse los requerimientos de monitoreo y cuáles de esos productos se adaptan mejor a las necesidades, en función la infraestructura existente y la capacidad de integración con otras herramientas de monitoreo.

Alimentación eléctrica

4

"Hay una fuerza motriz más poderosa que el valor, la electricidad y la energía atómica: la voluntad".

-- Albert Einstein (1879-1955) Físico alemán. Premio Nobel de Física en 1921

Red Eléctrica

Como se mencionó anteriormente en la etapa del diseño, se deberá considerar que la ubicación seleccionada del Data Center contará con el flujo eléctrico necesario para asegurar el funcionamiento todos los equipos, independientemente de las condiciones externas ambientales, ya sea el suministro eléctrico, las conexiones de red, u otras. Los equipos dentro del Data Center deberán seguir funcionando sin interrupción de manera transparente para los usuarios con el mayor grado de disponibilidad posible, ya que probablemente muchos equipos sean de misión crítica. Para esto, se deberán contar con los sistemas de contingencia adecuados que permitan esa confiabilidad y estabilidad.

Dependiendo de la ubicación del Data Center, ya sea un edificio dedicado o una parte dentro de un edificio de oficinas, la selección del método de contingencia eléctrica puede variar según la estrategia seleccionada, ya que los proveedores del servicio eléctrico tienen un nivel de confiabilidad menor al que necesita un Data Center; en el mejor de los casos puede llegar al 99.9%, pero a veces eso no es suficiente.

El primer paso es definir el consumo eléctrico que tendrá el Data Center, considerando el crecimiento a futuro. La instalación eléctrica correcta al momento del diseño puede ser un ahorro muy importante a futuro. Una vez que está en funcionamiento el Data Center, hacer un cambio en la estructura eléctrica puede

tener un costo diez veces superior comparándolo con el costo de hacerlo en el momento inicial.

Conceptos básicos de la electricidad

La energía que encierra la electricidad proviene de una de las partículas más pequeña conocida por la ciencia: los electrones, que poseen una carga eléctrica negativa. Toda la materia está formada por átomos, y los átomos están formados por partículas todavía más pequeñas: protones, neutrones y electrones. Algunos tipos de átomos tienen electrones que están menos apegados al núcleo (libre o suelto). Esto quiere decir que fácilmente pueden ser movilizados de un átomo a otro. Cuando los electrones se mueven entre los átomos de la materia, se produce una corriente (circulación) de electricidad.

Esto es lo que sucede cuando los electrones circulan por un filamento de alambre, pasan de un átomo a otro. La fuerza con la que pasan esos electrones es conocida como tensión (E o V), se mide en Volts, que podría entenderse eléctricamente como la fuerza con la que circulan los electrones a través del conductor, y algunos elementos son mejores conductores que otros debido a las características propias del material por el cual circulan. Esto se relaciona con la capacidad de los electrones de los átomos de esa materia, de movilizarse de un lugar a otro. A esta oposición al paso de electrones se la llama Resistencia (R) y se mide en Ohms. A menor resistencia del material al paso de electrones, mejor conductor de electricidad es el elemento.

Material	Resistividad (a 20°C- 25°C) (Ω·m)
Plata	$1{,}55 \times 10^{-8}$
Cobre	$1{,}71 \times 10^{-8}$
Oro	$2{,}35 \times 10^{-8}$
Aluminio	$2{,}82 \times 10^{-8}$
Hierro	$9{,}71 \times 10^{-8}$
Platino	$10{,}60 \times 10^{-8}$
Estaño	$11{,}50 \times 10^{-8}$

El cobre es un excelente metal conductor de electricidad, ya que su resistencia es baja (y su costo es aceptable; el oro, por ejemplo, tiene aún menor resistencia, pero su costo es muchísimo más alto, razón por la cual no existen cables de oro, pero si algunos conectores en las computadoras son de oro). A la capacidad de transferir electrones se la conoce como resistividad eléctrica (ρ letra griega minúscula rho) y se expresa en ohmios por metro. La resistividad de los metales aumenta con la temperatura, mientras que la resistividad de los semiconductores disminuye ante el aumento de la temperatura.

La Corriente(i) es la cantidad de electrones que circulan a la vez por ese material y se mide en Amperes.

Supongamos que una cañería de agua (que en nuestro caso sería la electricidad) los electrones libres que se mueven, están representados en el agua que fluye. La cantidad de electrones que circulan por el conductor es igual a la cantidad de litros por segundo que lleva la cañería. Si tomamos un caño de media

pulgada, que lleva un litro de agua por segundo, y en determinado lugar del caño midiéramos cuántos litros de agua pasan en un segundo por allí, eso representa al equivalente de amperes que circulan por un cable.

Análogamente, analicemos qué pasa con los Volts. Continuando con el ejemplo de la cañería, la electricidad es el agua, los amperes son la cantidad de agua que circula en un momento de tiempo y un lugar del caño. Los voltios (en homenaje a Alejandro Volta) serían la fuerza con la que circula el agua, y si uno multiplica la fuerza (voltios) con que circula el agua por la cantidad de agua que circula, vamos a obtener la presión generada, o lo que en electricidad se conoce como potencia (medida en Watt). En una lámpara de 40 watts circularan 0.18 amperes a una *fuerza* de 220 V.

Si la tensión es constante y el flujo de electrones aumenta, la sección del conductor deberá ser más grande para no causar un recalentamiento del cable, lo que sería análogo a aumentar la sección de la cañería.

Resumiendo

- La corriente (i) es la cantidad de electrones que circulan por el material: se mide en [Amperes] vendría a ser como la cantidad de agua que pasa por un caño.
- La resistencia (R) se mide en [Ohms] y es una oposición a la corriente, es un parámetro de un componente electrónico o de un material según su resistividad[1].
- La tensión (E o V) se mide en [Voltios] es la fuerza de circulación de los electrones y equivale a la fuerza con la que circula el agua por el caño.
- La potencia (P) es la relación de paso de energía de un flujo por unidad de tiempo y su unidad de medida es en [Watts].

Ley de Ohm:

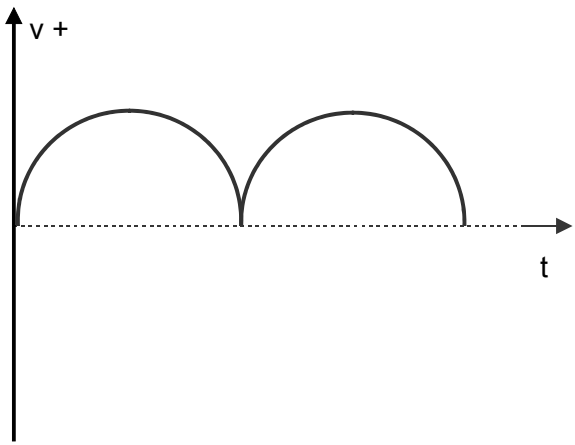
La corriente que circula en un circuito eléctrico es directamente proporcional a la tensión aplicada e inversamente proporcional a la resistencia del mismo. Expresado como ecuación queda así:

$$\text{I (amperes)} = \frac{\text{E (Volts)}}{\text{R(Ohms }\Omega)} \qquad \text{Ej: } 3\text{ (amperes)} = \frac{12\text{ (Volts)}}{4\text{(Ohms }\Omega)}$$

[1]Es la resistencia eléctrica específica de un material. Se designa por la letra griega rho minúscula (ρ) y se mide en ohmios por metro.

La **corriente continua** (CC o DC,*direc tcurrent*) se genera a partir de un flujo continuo de electrones (cargas negativas) siempre circulando en el mismo sentido, el cual va desde el polo negativo de la fuente hasta el polo positivo. Al desplazarse en este sentido, los electrones, los huecos o ausencias de electrones (cargas positivas) lo hacen en sentido contrario, es decir, del polo positivo al negativo.

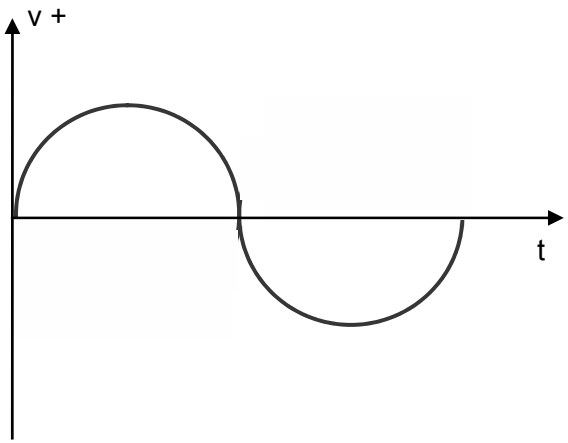
Por convención, se toma como corriente eléctrica al flujo de cargas positivas, aunque éste es a consecuencia del flujo de electrones. Por tanto, el sentido de la corriente eléctrica es desde el polo positivo de la fuente hacia el polo negativo, y contrario al flujo de electrones, siempre tiene el mismo signo y fluye hacia un solo lado.



La corriente continua se caracteriza por su tensión, porque al tener un flujo de electrones prefijado, pero continuo en el tiempo, proporciona un valor fijo de corriente (de signo continuo).

En la **corriente alterna** (CA o AC, *altern current*), los electrones no se desplazan de un polo a otro, sino que a partir de su posición fija en el cable (centro), oscilan de un lado al otro de su centro, dentro de un mismo entorno o amplitud, a una frecuencia determinada (número de oscilaciones por segundo).

Por tanto, la corriente así generada (contraria al flujo de electrones) no es un flujo en un sentido constante, sino que va cambiando de sentido y por eso de signo, continuamente, con tanta rapidez como la frecuencia de oscilación de los electrones.



La **frecuencia** es la cantidad de ciclos completos en una corriente eléctrica y se calcula por segundo. Por ejemplo, la corriente alterna oscila cambiando de signo de polaridad con una frecuencia de 50 ó 60 ciclos por segundo.

La unidad para medir estos ciclos es el Hertz (Hz), que debe su nombre al físico alemán Heinrich Rudolf Hertz, quien en 1888 demostró la existencia de las ondas electromagnéticas. Un Hertz o Hertzio equivale a un ciclo por segundo.

Normalmente, los equipos que están dentro del Data Center son capaces de absorber las variaciones en la frecuencia eléctrica sin problemas.

La forma sinusoidal (ilustrada más arriba) de la corriente alterna puede ser observada mediante una herramienta llamada osciloscopio, allí se aprecia el cambio de sentido positivo a negativo. La corriente eléctrica de red provee corriente alterna con una frecuencia que oscila entre 50 y 60 veces por segundo, manteniendo la forma de onda, que si se mantiene de manera perfecta (como está ilustrada en el gráfico) estaríamos hablando de condiciones ideales, pero no siempre ocurre esto en la realidad. Existen diversos fenómenos que pueden alterarlo, más adelante en este capítulo se detallarán algunos.

La **potencia eléctrica** es la relación que existe entre el paso de energía de un flujo eléctrico por una determinada unidad de tiempo, es decir la cantidad de energía consumida por un equipo en cierta cantidad de tiempo, se expresa en Watts (W).

$$P(Watts) = E(Votls) * I(Amper)$$

La potencia medida en Watts es la *potencia real* consumida por el equipo y se utiliza para estimar la carga de calor que producen los dispositivos. La relación Volts-Amperes (VA) se la conoce como *potencia aparente*, y es el producto de la

tensión aplicada y la corriente que por él circula. Se utiliza para estimar el consumo eléctrico, el tipo de cables, el tamaño de las UPS, circuitos de protección y todo lo que tenga que ver con consumo eléctrico.

Ambos conceptos tienen usos y propósitos distintos, ya que no son exactamente lo mismo, porque la potencia puede diferir del valor de VA, lo que se denomina como *factor de potencia* de la corriente alterna. Por ejemplo: una lámpara incandescente de 100 W tiene un valor de 100VA, eso quiere decir que el *factor de potencia* = 1. Pero, por ejemplo: un equipo de comunicaciones consume 60 W y tiene un valor de 75 VA, eso quiere decir que el *factor de potencia* es = 0.8 (al ser un indicador no posee unidad, ya que se simplifican).

$$Factor\ de\ Potencia = \frac{Potencia\ real\ (W)}{Potencia\ aparnete(V * A)}$$

Desde 1996 en adelante, la mayoría de los fabricantes de hardware utilizan para alimentar sus equipos, fuentes del tipo PFC (Power Factor Correction), es decir, que tienen el *factor de potencia* corregido internamente; de manera tal que es prácticamente igual a 1.

Conexión a tierra o aterramiento: consiste en una instalación física usada para desviar las corrientes indeseables de los equipos que están conectados a la red eléctrica, y así evitar daños causados por distintos fenómenos que ocurren en las instalaciones eléctricas, como por ejemplo: las descargas estáticas, picos de sobrecarga, etcétera. El objetivo de un sistema de puesta a tierra es principalmente brindar seguridad a las personas y proteger las instalaciones, equipos y bienes en general, al facilitar y garantizar la correcta operación de los dispositivos mediante este mecanismo de protección.

Existen varios estándares y/o regulaciones según el país. En el 2002, la organización ANSI publicó el documento J-STD-607-A: *Requerimientos para el aterramiento de telecomunicaciones de edificios comerciales*, bajo el estándar TIA/EIA-607-A, que es el más utilizado en Data Centers o el EN 50310 de la CENELEC (Unión Europea) publicado el mismo año.

La puesta a tierra o conexión a tierra consiste básicamente en un elemento conductor metálico clavado a cierta profundidad en la tierra (conocido comúnmente como jabalina debido a su forma alargada), que a su vez se conecta con el sistema eléctrico a donde se conectarán todos los equipos. La conexión a tierra es también usada como protección pararrayos del edificio, puentes, antenas, etcétera. Según el aérea total a proteger pueden instalarse más de una jabalina para poder canalizar la corriente indeseada hacia la tierra.

Los cables de conexión a tierra son distintos del resto y se identifican con un recubrimiento plástico de color verde con una línea amarilla, ya que no se utilizan para transmitir electricidad, sino que solo funcionan como método de descarga.

En los tableros o planos se identifican mediante el símbolo:

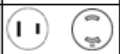
Una buena instalación a tierra permite reducir el riesgo de muchos tipos de alteraciones eléctricas que pueden ocurrir en un Data Center.

En zonas donde la corriente eléctrica provista por la red sea defectuosa adicionalmente se pueden colocar filtros a la entrada de distribución que mejoran su calidad.

Elementos eléctricos: dentro del Data Center nos encontraremos con los siguientes elementos eléctricos:

- **Transformadores**: se utilizan para subir o bajar voltaje según la configuración del Data Center. Si el trasformador es muy grande, según las especificaciones del fabricante es posible que requiera su propia conexión a tierra. Generalmente se coloca fuera de la superficie del Data Center (porque genera calor y es un foco de incendio potencial).
- **Tablero eléctrico principal**: el es elemento receptor del flujo eléctrico que ingresa al Data Center por medio de la red eléctrica suministrada por el proveedor. El tablero tiene como función proporcionar información y subdistribuir hacia el interior la energía eléctrica.
- **Subpaneles (*circuitbreaker*)**: sirven para distribución para grandes aéreas, de manera que permiten hacer tareas de mantenimiento sin tener que interrumpir el suministro eléctrico. Pueden soportar distintos voltajes según las necesidades desde 480V hasta 120V.
- **Unidades de Distribución de Energía (PowerDistributionUnit, PDU)**: es un dispositivo que distribuye energía eléctrica. También se utilizan para transformar el voltaje y amperaje para reducirlo a niveles más bajos y más útiles, por ejemplo, de corriente monofásica de 220V 30A a enchufes múltiples de 110V 15A o de 110V 20A. También puede transformar de trifásica a 220V 30 A.
- **Cables**: son los conductores que transportan la corriente desde el panel principal, transformadores, subpaneles y PDU.
- **Tomas**: son las fichas de entrada que permiten conectar los equipos a la red eléctrica y que están conectadas en cada Rack. Existe una gran cantidad de fichas distintas que varían según las regulaciones eléctricas de cada país, cambian en la forma de sus conectores, el voltaje y el amperaje que toleran.
- **Fichas eléctricas**: existen cientos de fichas para conectar los equipos a la red eléctrica, que principalmente dependen de la reglamentación del país en cuanto a la tensión suministrada 110/125/200/220/250V y el amperaje requerido por el dispositivo 10/15/20/30/50/60ª.

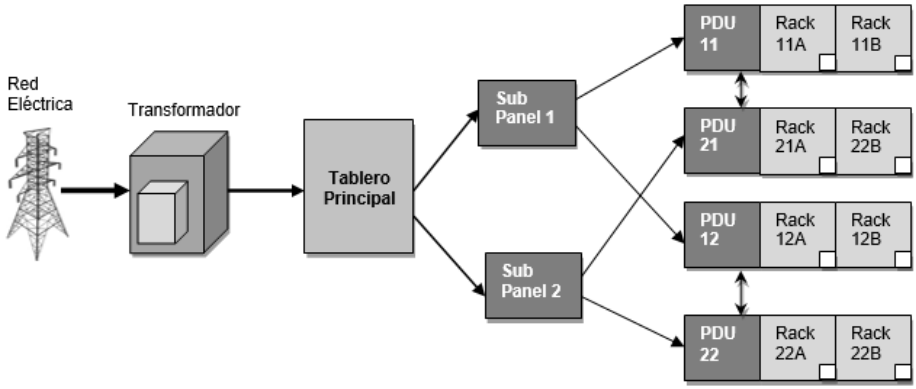
En este gráfico se muestran solo algunos de los más comunes, la mayoría pertenecen a la NEMA[2].

Amperaje	2 cables - 2 polos sin conexión a tierra		3 cables - 2 polos con conexión a tierra		4 cables - 3 polos con conexión a tierra
	hasta 125V	hasta 250V	hasta 125V	hasta 250V	125/250 V
10A			IEC-60320-C13/14	IEC-60320-C13/14	
15A	 1-15P L1-15P	L6-15P	5-15P L5-15P	6-15P L6-15P	
20A			5-20P L5-20P	6-20P L6-20P C19/20	L14/15-20P
30A			L5-30P	L6-30P	L14/15-30P
50A			L5-50P	L6-50P	L15-50P
60A			L5-60P	L6-60P	L15-60P

En este link, se puede acceder a los detalles técnicos de muchos más conectores, de distintos países y sus especificaciones técnicas:
`http://www.powerfig.com/reference.aspx`

En este gráfico, se pueden apreciar los elementos principales que permiten tener una distribución eléctrica con caminos redundantes, donde cada rack es alimentado por dos fases distintas.

[2]Asociación Nacional de Fabricantes Eléctricos (Nacional Electrical Manufacturers Association) Es una asociación industrial estadounidense que define los conectores para los equipos eléctricos.

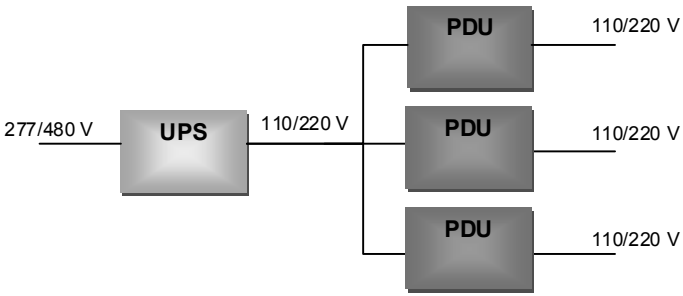


Factores a considerar para seleccionar la alimentación eléctrica más adecuada:

- Tamaño del Data Center.
- Naturaleza de los equipos que se van a instalar.
- Tipo y calidad de la red eléctrica en la zona donde se instalará el Data Center.
- Presupuesto.
- Costo KW/h (Kilo Watt por hora) del distribuidor, para las empresas proveedoras es más económico suministrar la corriente a mayor tensión.

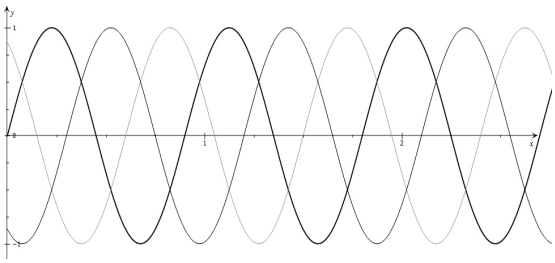
PDU

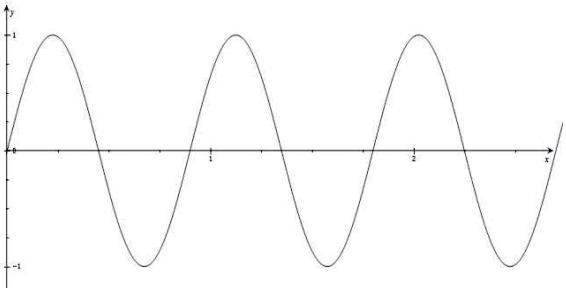
Para una distribución eléctrica optimizada es recomendable que el transformador esté integrado dentro de la PDU. Aquí se ve una distribución eléctrica típica de un Data Center con corriente trifásica que tiene una entrada a la UPS que varía de 277 V a 480 V. Luego, la PDU también posee un transformador que reduce la salida a un valor acorde a los equipos que están instalados que oscila entre 220 V a 108 V. En instalaciones medianas o chicas algunos modelos de PDU tienen la UPS integrada.



Potencia eléctrica: Monofásica o Trifásica

En los sistemas trifásicos, las tensiones circulan por cuatro cables, cada uno denominado por una fase R, S, T y N que representa al neutro (los nombres de las fases pueden ser distintas según el país), y que tienen una variación sinusoidal desplazada 120° con respecto al tiempo, es decir, que están desfasadas entre sí, equidistantes un tercio del período de frecuencia, por lo que la potencia nunca cae.





En cambio en los sistemas monofásicos solo hay una fase que circula por los cables, uno positivo, uno neutro y el de descarga a tierra. En ese período de tiempo, la tensión baja a 0 V por cada ciclo, aunque visualmente sea indetectable ya que esto se repite entre 50 y 60 veces por segundo.

El costo de la energía trifásica es más rentable comparado con el de la monofásica.

Estrategias de distribución eléctrica para la optimización

Si existe la posibilidad de elegir la tensión en la instalación del Data Center para los equipos, es preferible una tensión de 220 V en lugar de 110 V, la corriente es la mitad para la misma potencia, eso permite un ahorro en conductores y una mejor eficiencia de la corriente. El riesgo eléctrico de los sistemas que funcionan a 220 V es sólo un poco mayor en comparación con los que funcionan a 110 V (no significa que se duplican las muertes por descargas accidentes) y los requerimientos de aterramiento son iguales.

Por eso las instalaciones que operan a mayor voltaje tiene mejor eficiencia, aun más una entrada 480 V hasta la PDU y transformación a 220/240 V, comparadas con aquellas que utilizan voltaje más bajo con entrada 277 V hasta la PDU y transformación a 110/120 V.

Incluso algunos fabricantes de equipos, como servidores de gran tamaño, sistemas de almacenamiento masivo u otros, ofrecen fuentes de alimentación trifásica que brindan una eficiencia superior.

Para tener información básica es bueno saber cuál es el consumo eléctrico por cada Rack en kVA, y a su vez en consumo por cada fila de Racks, a fin de decidir con facilidad cuál es la PDU que se necesita.

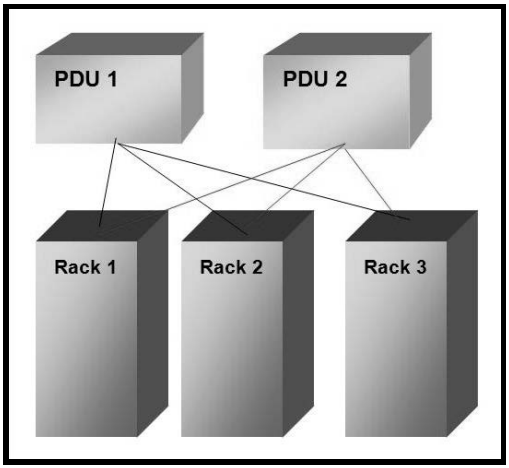
También, como medida de control general es bueno saber la densidad por kVA sobre la superficie total del Data Center, es decir, kVA por metro cuadrado.

Instalación redundante

Las mejores prácticas sugieren tener al menos dos fuentes de alimentación distintas para cada equipo; de manera tal, que si un elemento distribuidor falla (PDU) no se verá interrumpido el suministro eléctrico en el dispositivo crítico. Por ejemplo, si un servidor tiene dos fuentes de alimentación, cada una se deberá conectar a distintas fuentes de alimentación que están colocadas en la parte trasera del Rack, una en el lateral izquierdo y otra en el lateral derecho, cada una de ellas debe estar alimentados por distintas PDU.

Aquí se muestra un gráfico de conexión típico de cómo queda la distribución eléctrica:

- Ventajas
  - Funciona bien para ambientes chicos.
- Desventajas
  - Requiere muchos cables para cruzar entre las unidades con los Racks, provocando una posible congestión de cables, obstruyendo el flujo del aire si existe un piso técnico instalado. No es recomendado para Data Centers de envergadura.



Instalar la PDU por cada fila de Racks

Una buena forma de aprovechar el desempeño de la PDU, asegurando la capacidad redundante de alimentación para casos en que se necesita hacer mantenimiento sin apagar los equipos, es instalar una PDU por cada fila de Rack (en la cabecera de la fila o en el medio de la hilera), que brindarán una fuente de energía a toda esa fila, y además instalar otra PDU en la fila siguiente; de manera tal, de que ambas queden entrecruzadas, donde cada PDU alimenta a su fila y a la siguiente, proveyendo dos fuentes de alimentación a cada Rack.

En el capítulo 8, se explicarán con más detalles las estrategias de manejo de cableado.

UPS

Un UPS (Uninterruptible Power Supply) o en español SAI (Sistema de Alimentación Ininterrumpida) es una fuente de suministro eléctrico que es alimentada por una batería cuyo fin es seguir dando energía a dispositivos de misión crítica en el caso de interrupción eléctrica, con un tiempo de respuesta < a 250 milisegundos. De dicha forma, se asegura la continuidad de funcionamiento.

Las UPS se conectan a la red eléctrica, y proveen la alimentación a los servidores en caso de falla, permitiendo usarlos por varios minutos si se produjera un corte eléctrico de red.

Además agregan otras funcionalidades que mejoran la calidad del suministro eléctrico que llega a los equipos que están dentro del Data Center, como pueden ser: un estabilizador de energía eléctrica entrante, aislación de la fuente de energía eléctrica normal, filtrado de la energía entrante, corrección de la forma de onda, corrección de la frecuencia de línea, protección de equipos.

Algunas UPS también ofrecen capacidad de conectase a los servidores, y se encargan de apagarlos de manera controlada cuando los Administradores no estén en el momento del corte en el suministro eléctrico, y la UPS está llegando al límite de carga mínima.

Topologías básicas de UPS

Para seleccionar una UPS existen cuatro tipos de topologías disponibles, cada una con sus particularidades, ya que varían en costos y disponibilidad. Por ejemplo, si tenemos que la carga total de los equipos de IT es 600 kW, veremos cómo cambian las configuraciones según la topología seleccionada.

- **Capacidad normal (N):** esta configuración brinda la posibilidad de soportar la carga actual del Data Center por un tiempo limitado. Es la más económica, puede dar electricidad en caso de fallo de la red eléctrica, pero en forma reducida, y no puede responder satisfactoriamente a ningún tipo de fallo de la UPS. Además, los mantenimientos que requieran desactivar la UPS ponen en riesgo una interrupción, ya que no hay redundancia. Se utiliza en ambientes chicos. Para el ejemplo para soportar la carga total se necesitarían 3 módulos de 200 kW cada uno.
- **Redundancia paralela aislada (N):** ídem a la configuración anterior, pero con la particularidad que los módulos son independientes del fabricante, brindando mayor flexibilidad al momento de la adquisición, aunque complejiza y encarece la instalación, el monitoreo y el mantenimiento. Es utilizado en ambientes medianos. Para el ejemplo anterior, se necesitarían 2 módulos de un proveedor y otro módulo de otro proveedor de 200 kW cada uno.
- **Redundancia paralela (N+1):** similar a la de capacidad normal, pero con un módulo adicional que le permite tolerar el fallo de solo un módulo de la UPS y soportar la carga total sin inconvenientes, permitiendo realizar mantenimientos sin impactar al servicio. Son los más utilizados en Data Centers, porque funcionan 8 x 5 (8 horas por día hábil de la semana). Utilizado en ambientes medianos. Para el ejemplo, se necesitarían 4 módulos de 200 kW cada uno (solo un módulo de redundancia).
- **Redundancia doble (2N):** ofrece el doble de capacidad total de la carga del Data Center. Si un sistema completo de UPS entra en falla, hay otro capaz de soportar **toda** la carga. Es la configuración más robusta, pero también es la más cara. Para el ejemplo, se necesitarían 6 módulos de 200 kW cada uno: dos veces la capacidad total.

Un concepto muy importante a la hora de conocer y evaluar una UPS es la **eficiencia,** que puede ser definida como el cociente entre la salida y la entrada de energía expresado en porcentaje. La eficiencia nunca es del cien por ciento, ya que en todos los sistemas de UPS se pierde capacidad por el consumo de los componentes internos (transformadores, placas, circuitos, rectificadores,

transistores, inversores, etcétera) pero mientras mayor sea la eficiencia más conveniente será el dispositivo.

$$Eficiencia = \frac{Salida[W]}{Entrada[W]} \times 100$$

Por ejemplo

Si tenemos una UPS de 90 kW, que requiere 100 kW de entrada, significa que 10 kW se están perdiendo (en forma de calor u otras transformaciones internas). Esto quiere decir que la UPS tiene una eficiencia = 90%.

Si bien 10 kW de energía perdida podría no ser mucho, hay que tener en cuenta que estamos hablando de sistemas que trabajan 24 x 7 los 365 días del año. Si hacemos una pequeña cuenta veremos que estamos hablando de mucho dinero.

10 kW x 24 horas x 365 días = 87 600 kWh al año.

Si tomamos un valor kW/h de 3 dólares, significaría una pérdida de 262 800 dólares al año.

Componentes comunes a todos tipos de UPS

- Batería: se encarga de almacenar energía y suministrarla en caso de interrupción de la corriente eléctrica. Su capacidad se mide en Amperes por hora, y según el tamaño varía la autonomía (por los general, la UPS se calculan para tener una autonomía que oscile entre los 5 y los 15 minutos, dependiendo del caso). Todo el almacenamiento de energía en las baterías se hace en corriente continua. Por esa razón, para que esa energía potencial pueda ser usada por los equipos que funcionan con corriente alterna debe ser convertida de CC a CA.
- Inversor: transforma la corriente continua de las baterías en corriente alterna, la cual alimenta los dispositivos conectados a la salida del UPS. También cumple el proceso inverso, transformando corriente alterna de la red en corriente continua para almacenarla en las baterías.

Para un funcionamiento óptimo de las baterías, se recomienda una temperatura de operación de 20°C. Si la temperatura es mayor no se tendrán los resultados esperados de funcionamiento, durabilidad y eficiencia.

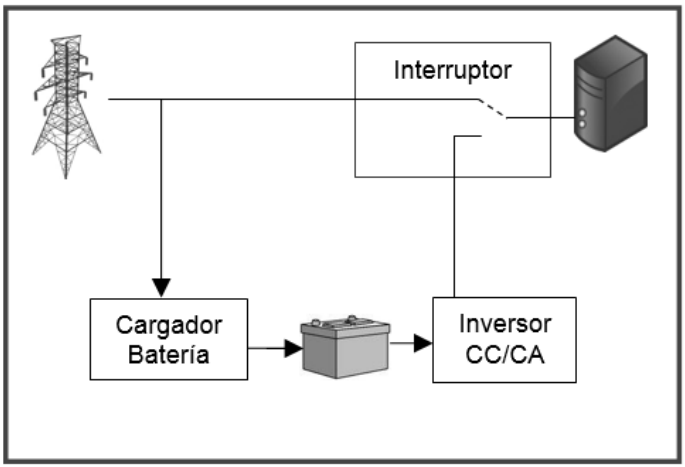
Un diseño planificado normal de vida útil de la batería es de 5 años (que es el promedio estándar). Pero si ésta funcionó permanentemente a una temperatura de 30°C, su durabilidad se reduce en un 50%. Esta reacción no es lineal, aun es peor si operó a 40°C, entonces, la vida útil se reduce al 20%. Por eso, se recomienda

instalar las baterías en un ambiente de temperatura controlada, con la finalidad de mantener la durabilidad y no aumentar los costos.

Tipos de UPS

En el mercado existen varios tipos de UPS que se adaptan a las necesidades funcionales de cada Data Center. A continuación, se detallarán las más importantes:

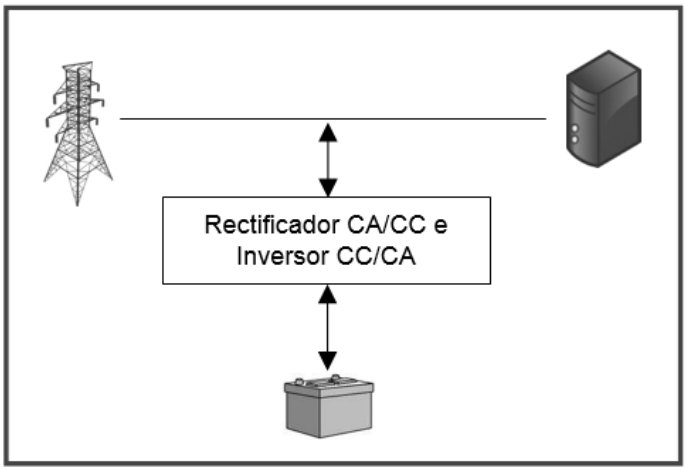
Off-line, Stand-by (espera) o Pasivos



Se monitorea la entrada de energía en forma permanente, cambiando la fuente de alimentación a batería por medio del Interruptor. Es capaz de detectar problemas en el suministro eléctrico de red en cuestión de milisegundos.

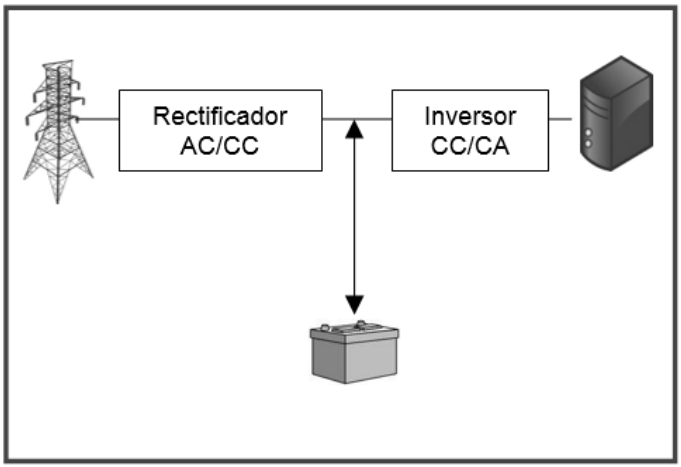
Operando en modo normal, la electricidad de la red alimenta los equipos, y una parte pequeña pasa por el cargador, convirtiendo de CA a CC para alimentar la batería. Si se interrumpe el suministro eléctrico de red, la batería provee la alimentación, y el inversor transforma de CC a CA, permitiendo que los equipos sigan funcionando sin interrupción. Se utiliza en instalaciones pequeñas (monofásica). Brinda una autonomía reducida.

On-line, Línea Interactiva o Activos



El inversor se encuentra conectado a red principal de energía debido a que siempre se está realizando una doble conversión en tiempo real y en forma constante. El conmutador que detecta la interrupción está conectado a la salida del inversor. La corriente pasa por el rectificador continuamente para cargar la batería y alimentando el inversor, el cual, a su vez, da la corriente alterna a la salida del UPS. Cuando se interrumpe el flujo eléctrico de la red, las baterías alimentan al inversor, por esta razón la salida no sufre ninguna interrupción por el corte (ni siquiera milisegundos). Es muy común para aplicaciones de mediana envergadura (con salida monofásica o trifásica).

On-line de Conversión Doble

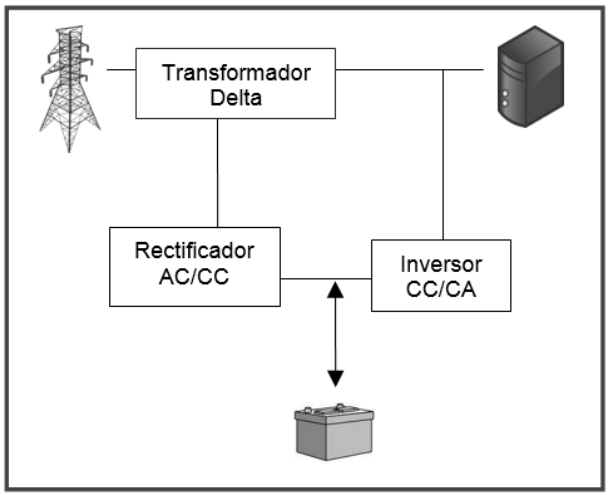


Es la más común dentro de los Data Centers, por su confiabilidad y calidad.

Posee un rectificador de conversión CA a CC a la salida de la red eléctrica, que alimenta a su vez, proveyendo carga a la batería. De esa salida, además brinda corriente continua al rectificador de inversión, que transforma la CC a CA para mantener el flujo constante de electricidad en los equipos críticos.

Tiene buen desempeño, pero alto desgaste de sus componentes. Se utiliza en Data Centers grandes.

On-line de Conversión Delta



Funciona de manera similar a la anterior, pero de forma optimizada, haciendo uso de una tecnología propietaria desarrollada en 1995 por APC[3]. Su ventaja es el aprovechamiento racional de la energía que utiliza para cargar la batería, ya que el transformador *delta* provee alimentación a la entrada del inversor, haciendo que utilice solo la diferencia la energía que proviene de la red y de la batería. De esta forma, se obtiene una mayor eficiencia y se alarga la vida útil de los componentes, ya que el desgaste interno es menor.

Haciendo un análisis de TCOa 10 años entre las UPS de Conversión Doble y Conversión Delta (tomando una configuración 2N de 300 kVA), se puede observar una diferencia significativa a favor de la de Conversión Delta, ya que la eficiencia es bastante mejor. Esto produce un ahorro en energía, enfriamiento y mantenimiento, que comparativamente será un 58% más económica en ese período.

[3]American Power Conversión Corporation es una empresa fundada en 1981 que fue adquirida por Schneider Electric, en el 2007, y está dedicada a producir distintos elementos para Data Centers (UPS, Racks, etcétera).

Tabla comparativa de las distintas UPS

Características	Stand-by	Línea Interactiva	Conversión Doble	Conversión Delta
Eficiencia (con carga al 100%)	No Aplica	98%	86% a 95%	97%
Rango potencia aplicación práctica kVA	< 0,5	0,5 a 5	5 a 5000	5 a 5000
Costo por kVA	Bajo	Medio	Medio	Medio
Uso de tensión	Baja	Baja o Alta	Alta	Alta
Beneficios	Bajo costo y tamaño reducido	Alta confiabilidad y eficiencia	Excelente confiabilidad	Excelente confiabilidad y eficiencia
Destinos	Hogareño (N)	Data Centers medianos (N+1)	Data Centers grandes (2N)	Data Centers grandes (2N)

Flywheel UPS

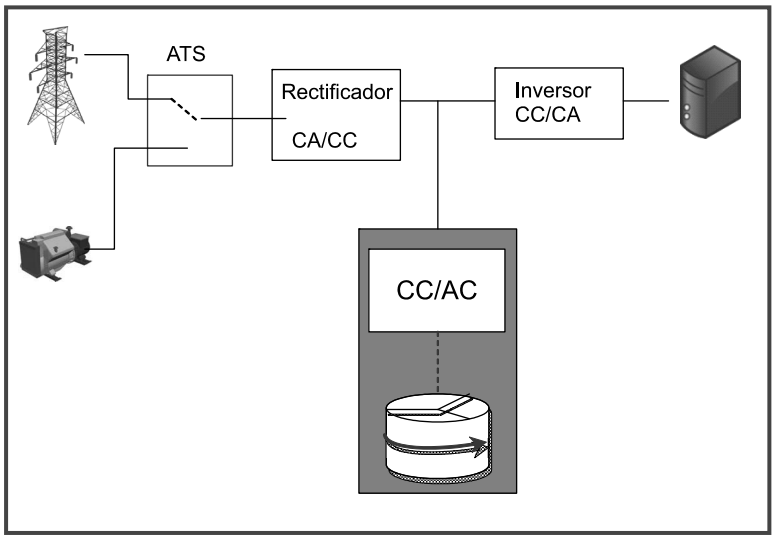
Los gastos de mantenimiento, refrigeración y utilización de las UPS consumen una parte importante del presupuesto de IT de los grandes Data Centers, pero existe una solución alternativa con un paradigma totalmente distinto del enfoque de la UPS tradicional. Esta nueva perspectiva está en creciendo en función de las ventas en el mercado (en 2003, acaparaban solo el 3%, pero para el 2007 ya se estima que poseían el 9,7% del mercado). Su principal ventaja competitiva es que permite ahorrar costos de manera significativa, y se la puede encontrar en el mercado en presentaciones desde 90 kVA o superiores.

Existe una condición primordial que se debe cumplir para implementar este nuevo modelo: tener un generador adecuado con todos los mantenimientos preventivos, de modo tal de ser cien por ciento confiables, ya que este nuevo modelo tiene una dependencia total con respecto al generador. Pero si se le realizan todos los controles y mantenimientos adecuados, no debería presentar problemas.

La UPS giratoria o Flywheel UPS está desarrollada sobre el concepto antiguo, que consiste en transformar la energía cinética en energía eléctrica.

La energía de la red pone en movimiento una rueda metálica muy pesada (de 300 kg o más), haciéndola girar a gran velocidad (entre 33 000 y 77000 RPM según el fabricante), y por medio de la levitación electromagnética al vacío no entra en contacto con otros elementos, evitando así el rozamiento que frenaría la rueda, permitiéndole girar a gran velocidad durante un tiempo prolongado (ya que no hay

fricción). Ese movimiento entregará corriente eléctrica cuando se interrumpa el suministro de red.



Si el suministro eléctrico se detiene, la rueda de gran masa que está girando a muchas revoluciones es capaz de proporcionar suficiente energía al Data Center durante unos segundos (entre 15 y 60 según la configuración).

Primero, la UPS espera durante dos segundos que se restaure el servicio eléctrico de red, si eso no sucede, da la orden al generador para que se inicie y comience a entregar energía estabilizada, que deberá producirse dentro de los siguientes seis segundos (para los generadores modernos es un tiempo aceptable). Si la rueda deja de girar y el generador no encendió por algún problema, todos los equipos se apagarán en menos de un minuto.

- Ventajas
  - Vida útil mayor a 20 años con ROI menor a tres años.
  - No utiliza baterías, produciendo grandes ahorros de energía, contaminación, enfriamiento, reemplazo y mantenimiento (sólo utiliza una pequeña batería para el arranque).
  - Ocupa menor superficie (por ejemplo, una UPS de 300 kVA ocupa solo 25% del espacio de una UPS de Conversión Doble, aunque puede llegar a pesar 2 500 kg)
  - Su eficiencia oscila entre el 95% y el 98%.
  - Su tiempo de carga es bajo: entre tres y ocho minutos, comparado con la UPS tradicional que puede llegar a tardar entre ocho y diez horas para completar la carga.

- La operatoria es silenciosa (entre 45 y 70 decibeles a un metro de distancia).
- Genera poca temperatura. Por ejemplo: una UPS de 300 kVA de 1.5 x 0.8 m y una altura menor a 2 m genera entre 5 kW/h y 7 kW/h de calor.

- Desventajas
  - Su inversión inicial es elevada.
  - Tiene poco tiempo de energía de resguardo, lo que genera una mayor dependencia del generador.

Criterios de selección

Al seleccionar y dimensionar la UPS se deberá tener mucho cuidado con las especificaciones técnicas, ya que muchas veces los fabricantes de UPS detallan la capacidad en VA (potencia aparente) que en realidad puede ser aproximadamente del 60% de la potencia real necesaria. Por ejemplo: una UPS de 1 kVA tiene una potencia real de 600 W, por lo que si necesito alimentar un servidor que tiene un consumo de 800 W, la UPS no podrá proveer la electricidad suficiente y el equipo se apagará.

- Los factores más importantes al momento de seleccionar la UPS son:
  - Calcular el costo del impacto por la interrupción del servicio para dimensionar qué tan importante es y hasta cuánto podremos invertir. De esto dependerán los requerimientos de disponibilidad, tipo de UPS, topología, etcétera. Y luego, analizar cuál es la solución más eficiente desde el punto de vista económico en función del presupuesto.
  - Colocar caminos redundantes entre el banco de baterías y la unidad de distribución.
  - Obtener las curvas de eficiencia de los fabricantes y considerar la eficiencia como factor clave para la toma de la decisión.
  - Comprender que la eficiencia de la UPS disminuye a medida que baja la carga. Por eso, es importante asegurarse de que los datos sobre la eficiencia suministrados por los fabricantes se expresen en función de la carga y no como valor único correspondiente al máximo de carga. Esas medidas se toman con distintas cargas, por lo general, del 25%, 50%, 75% y 100%.
  - Seleccionar una estructura modular que permita escalabilidad.
  - ¿Cuál es la vida útil de las baterías y el costo de reposición?
  - ¿Los equipos del Data Center poseen doble fuente de alimentación? ¿Es necesario tener un doble cableado para todos los equipos o sólo para algunos?

- Seleccionar la tecnología más eficiente de distribución eléctrica según la disponibilidad de la zona donde está el Data Center y los equipos ya existentes.

Recomendaciones para extender la vida útil de la UPS y reducir costos

- Estudiar la curva de eficiencia del fabricante (de 0% a 100%).
- Analizar la eficiencia en los procesos de conversión de AC a CC y de CC a AC, que generalmente son elementos por donde puede haber pérdidas de eficiencia. Es recomendable consultar con el proveedor si hay nuevas tecnologías disponibles que aumenten la eficiencia, ya que la reducción en costos puede ser muy significativa.
- Servicio preventivo de mantenimiento rutinario.
  - Verificación de señalizaciones de alarma.
  - Análisis térmico (si una UPS está 10°C por arriba del valor esperado se deben tomar medidas correctivas).
  - Inspección ocular de cables y conectores (detección de corrosión).
  - Verificación y medición de parámetros operativos del sistema y baterías.
  - Limpieza y verificación de filtros de aire, gabinetes, ventiladores.
  - Reajuste de conexiones y limpieza.
  - Elaboración de reporte de servicio con recomendaciones necesarias.
- Servicio preventivo con paro total.
  - Limpieza interna de los sistemas y reajuste de conexiones de control.
  - **Si se requiere mover una UPS que está montada en un Rack, se deberá vaciar totalmente la carga misma para evitar una descarga eléctrica accidental en caso de tocar alguna parte metálica.**
  - Revisión de condiciones de herrajes, cableados, motores, ventiladores, etcétera.
  - Revisión y estado de componentes de potencia, fusibles, diodos, bobinas transistores, detección de corrosión.
  - Medición de voltaje por celda del banco de baterías.
  - Pruebas de sincronía, transferencia, retransferencia, corte de entrada, prueba de autonomía del banco de baterías, etcétera.
  - Puesta en operación del sistema y en línea con la carga crítica.
  - Elaboración de reporte de servicio.
  - El tiempo estimado para la realización de lo antes descrito es de dos horas como máximo por sistema.

La vida útil de la UPS se estima en diez años y la vida útil de las baterías se estima entre cuatro o cinco años según el fabricante. Es recomendable reemplazar a las baterías **todas juntas**, ya que esto asegura que el esfuerzo conjunto para todas es igual y no hay diferencias entre baterías que tienen uno y otras que tienen tres años de uso, asegurando la *performance* y el manteniendo constante de la vida útil de los dispositivos, además de simplificar las tareas de mantenimiento y control.

Comparación de rendimiento

Las instalaciones donde los equipos funcionan a 220 V tienen un mejor rendimiento en comparación con aquellas en la que funcionan a 110 V, porque mejoran el aprovechamiento de la electricidad y de la UPS al máximo nivel. Por ejemplo: una UPS que funciona a 20 A y 110 V puede soportar cuatro servidores, pero la misma UPS que funciona a 20 A con 220 V puede soportar ocho servidores, porque tiene mayor potencia ocupando la misma superficie y, prácticamente, generando el mismo calor.

Generadores

Los generadores son sistemas de contingencia. En caso de interrupción del suministro eléctrico de red son capaces de seguir entregando electricidad al Data Center, y forman parte de la estrategia en el diseño para evaluar el tipo de UPS. Transforman la energía mecánica obtenida de la ignición de combustibles en energía eléctrica.

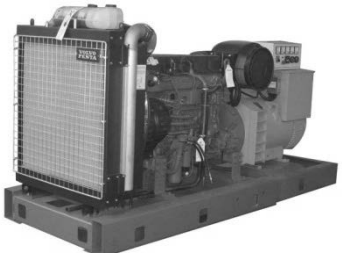
Estadísticamente, los cortes en el suministro eléctrico son responsables de:

- El 31% de las interrupciones en los Data Centers.
- El 45% de las pérdidas masivas de datos.
- El 33% de las fallas de hardware.

Los generadores son elementos extremadamente costosos, con cifras que arrancan en 300 000 dólares para generadores de potencia de hasta 2 000 kW, incluso algunos de mayor rendimiento pueden llegar a costar varios millones de dólares. Y a lo largo de su vida útil (estimada entre 20 y 30 años) esa cifra puede seguir creciendo en repuestos y tareas de mantenimiento. Además, según la ubicación geográfica donde se encuentre el Data Center puede ser bastante difícil conseguir el generador adecuado, aunque se disponga del dinero, ya que pueden existir demoras en el envío de país a país o demoras de instalación (por su complejidad). Más aun, por no ser elementos de consumo masivo y de alto valor individual, los vendedores o proveedores se manejan con un stock limitado.

Por ello la elección correcta forma parte fundamental de una buena estrategia de diseño del Data Center.

Elementos básicos del generador



- **Motor principal a combustible**: consiste en un motor de cuatro tiempos alimentado generalmente por diesel o gas (son lo más comunes).

  El tipo de combustible elegido dependerá de la locación y el acceso.

  En este cuadro comparativo se muestran las ventajas y las desventajas de cada uno de los tipos de generadores.

  — Diesel

  ✓Fácil de almacenar.

  ✓Pocos problemas si se almacena por mucho tiempo.

  ✓Amenaza de fuego reducida.

  ✓Mayor cantidad de horas de operación.

  ✗Daño ambiental.

  ✗Ignición dificultosa a bajas temperaturas.

  — Gas

  ✓Limpio y con menores emisiones tóxicas.

  ✓Menor costo de mantenimiento y menor riesgo.

  ✗Costo inicial elevado.

  ✗Tamaño limitado.

  ✗Pocos proveedores.

  ✗En épocas de emergencias es posible el corte de suministros.

  ✗Peligroso (fugas explosivas).

  — Gasolina o Combustible

  ✓Fácil de conseguir.

  ✓Inician más rápido que los motores diesel a bajas temperaturas.

  ✗Almacenamiento tiene riego de incendio alto.

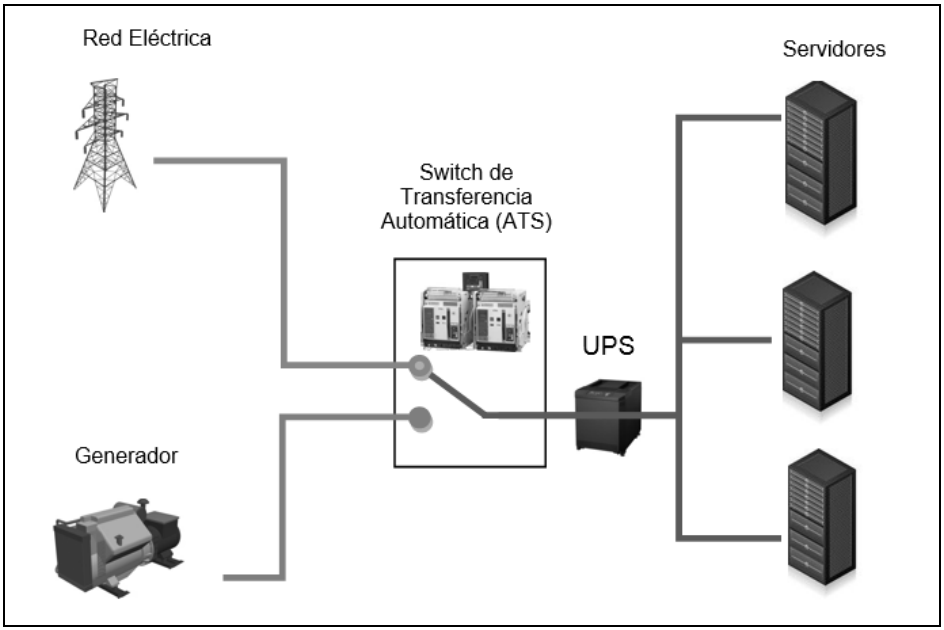
  ✗El almacenamiento de combustible es malo para el generador.

Fundamental: hacer los mantenimientos a la batería de arranque del generador. Estadísticamente los generadores que no arrancan correctamente son la principal causa de fallas eléctricas.
También, es necesario reemplazar los filtros de aire y combustible según corresponda.

- **Alternador**: es el encargado de convertir la energía mecánica en energía eléctrica. Básicamente transforma el movimiento rotatorio, generando una corriente alterna mediante inducción electromagnética como sucede en los automóviles. La electricidad que se utiliza para generar el campo electromagnético se crea dentro del propio alternador, lo que permite que este produzca grandes cantidades de electricidad sólo con la energía que brinda el motor principal.
- **Regulador de velocidad**: es el encargado de mantener las RPM (revoluciones por minuto) del motor principal y de estabilizar la frecuencia de salida. Posee un mecanismo hidráulico complejo y sistemas electrónicos. El regulador puede hacer que varíe la cantidad de electricidad que entrega según se requiera. A mayor RPM, mayor será la electricidad que proporcione.
- **En el caso de existir más de un generador, todos deben estar sincronizados para funcionar a la misma cantidad de RMP**. De esta forma, se genera un esfuerzo coordinado de mayor confiabilidad y se reducen los costos de mantenimiento. Ya sea en un sistema con múltiples unidades más pequeñas (idénticas) que se suman entre sí para obtener la carga máxima necesaria o en un sistema N+1, lo importante es que los generadores estén **sincronizados** para evitar una sobrecarga de la red eléctrica o el recalentamiento de un generador en particular.
- **Regulador de voltaje**: es un componente crítico colocado a la salida de los generadores, cuya función es otorgar el voltaje correcto al Data Center. Este elemento asegura la estabilidad del voltaje entregado al Data Center, previniendo picos inesperados que podrían llegar a dañar la infraestructura eléctrica.

Es normal que cuando funciona el generador se detecten fluctuaciones en la frecuencia debido a los ajustes que realiza el regulador de velocidad. Más adelante, en este capítulo, se detallarán cuáles son los métodos que permiten disminuir el impacto de dicho efecto. Por ello, es importante tener un sistema de monitoreo que muestre el funcionamiento de los parámetros principales del generador (RPM, Voltaje, temperatura, niveles de fluidos, alarma de fallas, etcétera) para que así el operador pueda tomar las decisiones correctas.

Esquema básico de instalación eléctrica



El Switch de Transferencia Automática (ATS) es el encargado de efectuar el cambio de origen de la fuente eléctrica en caso de interrupción del suministro de red. Su tiempo de respuesta es importante, pero todos los dispositivos del mercado responden en menos de un segundo. Al detectar la interrupción del suministro eléctrico, el generador comienza a funcionar. Según el uso, puede variar desde menos de 600 V hasta llegar a los 35 kV.

El tiempo ideal desde que se detecta el fallo hasta que el motor enciende y comienza a generar energía estabilizada es de diez a quince segundos, y puede ser aun menor a seis para los generadores más modernos. Pero, mientras sea inferior al minuto es aceptable también.

Elección del generador adecuado

Las preguntas que debemos resolver para elegir el generador son:

- ¿Cuál es el nivel de redundancia requerida?
- ¿Cuál es la carga total del Data Center en kW?
- ¿Cuál es el estimado de tiempo continuo de funcionamiento en el peor de los casos?
- ¿Cuál es el consumo por hora?

- ¿Qué tipo de combustibles hay disponibles en la zona donde está localizado el Data Center?
- ¿Cuáles son los costos de mantenimiento y repuestos?
- ¿Es la ubicación correcta para que no moleste a los vecinos?
- ¿Cuál es el lugar físico destinado a la instalación del generador y dónde estarán los depósitos de combustibles?
- ¿Existen regulaciones vigentes sobre las emisiones?

El mantenimiento del generador es clave, ya que es una tarea de suma importancia. En muchas ocasiones, una tarea importante queda relegada por otras de mayor urgencia, y por error se deja para más adelante. Esto es una equivocación bastante común, pero cuando se necesita el generador y por algún motivo no funciona, esto se transforma en un problema de dimensiones inesperadas, ya que se ha invertido mucho dinero en un mecanismo de contingencia que quizás solo deba funcionar en promedio 6 horas al año: pero cuando se lo necesita no responde como debería.

No sería agradable tener que explicarle al gerente de IT porqué se apagaron abruptamente 400 servidores, y justificar que el generador que costó 500 000 dólares, nunca antes usado, no arrancó, porque una batería que cuesta 50 dólares no se reemplazó debidamente.

- El generador debe estar **siempre** listo cuando se lo necesite.
- Al momento de realizar las pruebas, el generador debe tener la capacidad de funcionar entre 10 y 20 horas de corrido al menos una vez al año, ya que en caso de ser necesario utilizarlo puede requerir hasta 100 horas de uso continuo.
- Se debe realizar testeo térmico y de emisiones.
- Se debe verificar (testear) el generador a modo de prueba de manera esporádica.
- Conviene registrar todas las actividades para futuras referencias.
- Verificar el estado de los cables y conectores.
- Se debe efectuar la verificación de los filtros de aire para que la admisión de aire al generador sea suficiente, y que tenga ventilación suficiente para mantener la temperatura acorde con los requerimientos del fabricante.
- Hay que comprobar el estado y la tensión de las correas.
- Es necesario chequear los sensores, alarmas, controlar las baterías de arranque, monitoreo de temperatura, nivel de aceite y nivel de refrigerante.

Instalación del generador

La conexión a tierra del generador es trascendental tanto para la eliminación de fallas como para garantizar la eficacia de la energía generada, por esto, es obligatorio cumplir con los códigos eléctricos según la región correspondiente. Incluso no cumplir con las reglamentaciones de instalación puede tener penalizaciones económicas graves, como le ocurrió a Amazon, que fue multada con 261 638 dólares por el estado de Virgina (EE. UU.) por no cumplir con las regulaciones de instalación vigentes.

Además existen tres factores de importancia a tener en cuenta al momento de la instalación: las vibraciones, las emisiones por combustión y el ruido generado. Por ejemplo, en los Estados Unidos, la EPA (Agencia Federal de Protección del Medio Ambiente, Environmental Protection Agency) regula los niveles de estos parámetros, aunque según el estado puede variar. Otros países cuentan también con organismos ambientales similares que regulan las emisiones: el Ministerio de Medio Ambiente, Alimentación y Asuntos Rurales (DEFRA: Department for Environment, Food and Rural Affairs) del Reino Unido; el Ministerio del Medio Ambiente y Bosques (MoEF: Ministry of Environment and Forests), en la India.

La Asociación de Sistemas de Generación de Electricidad (EGSA, Electrical Generating Systems Association) es una organización mundial que brinda información sobre las emisiones y otros factores relacionados con los generadores.

También se deben tomar precauciones para evitar que las lluvias y condiciones de temperaturas extremas (altas y bajas) afecten directamente a los generadores.

Estos equipos se refrigeran con un sistema similar al del automóvil, que utiliza un ventilador para mover aire sobre el radiador y así mantener la temperatura del motor estable.

Instalación del tanque de combustible

El lugar donde se ubicará el tanque de almacenamiento de combustible para el generador es crítico debido al riesgo de inflamación, por lo que se deberán tener en cuenta los siguientes aspectos:

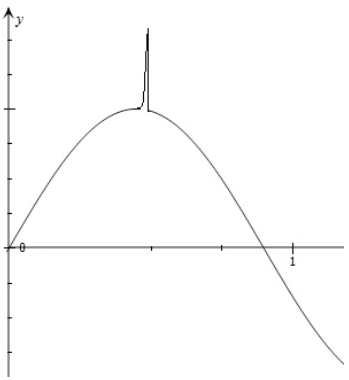
- **Ubicación:** por comodidad se coloca cerca del generador, y a su vez, el generador se coloca cerca del Data Center, lo que facilita la instalación de las cañerías, pero también genera el riesgo de tener un material inflamable cerca del edificio.
- **Capacidad del tanque:** deberá brindar una autonomía de al menos 60 horas, sobre la base del consumo del generador o los generadores que haya. Algunas certificaciones pueden llegar a exigir hasta 96 horas de operación continua.
- **Material del tanque:** pueden ser metálicos o plásticos.

- **Condiciones ambientales:** las temperaturas extremas son malas, tanto por ser demasiado altas (aumenta riesgos de incendio) como por ser demasiado bajas (riesgo de congelamiento).
- **Tiempo de almacenamiento:** el combustible que permanece por más de 12 meses dentro del tanque debe ser reemplazado, ya que con el paso del tiempo se generan sedimentos del combustible que pueden dañar el generador.

Problemas eléctricos frecuentes

Si bien es esperado que desde el proveedor del suministro eléctrico la calidad de la energía proporcionada sea constante según las normas establecidas, existen diversos tipos de problemas en el suministro eléctrico, que se pueden encontrar por razones internas o externas a las instalaciones del Data Center. Aquí se detallan los más comunes y sus posibles soluciones en cada caso.

Perturbaciones transitorias

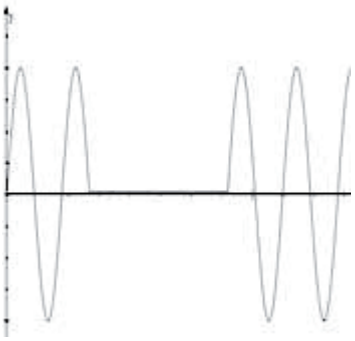


Las perturbaciones transitorias son eventos repentinos, de muy corta duración (nano segundos) que elevan o disminuyen la tensión (por ejemplo un rayo, una desconexión de una UPS grande o una descarga electromagnética).

Solución:

- instalar TASS (supresores de sobretensiones transitorios).
- mantener la humedad controlada.
- instalar UPS.

Interrupciones



Cuando se interrumpe el suministro de la red eléctrica.

Puede tener impacto negativo muy grande en los equipos. Por eso se toman medidas para contrarrestar dicha posibilidad.

Solución:

- instalar UPS y generador.

Incremento o decremento de tensión

Las posibles variaciones de la tensión pueden dividirse en cuatro grupos:

- Decremento de tensión (variable o sostenida en el tiempo).
- Incremento de tensión (variable o sostenida en el tiempo).

Ambos fenómenos son bastante similares, pero con comportamientos distintos:

El **decremento de tensión** podríamos decir que es el más inofensivo de los dos, ya que en el peor de los casos se apagarían los equipos (en caso de no contar con una UPS). Por ejemplo, es un fenómeno que podría ocurrir al instalar un equipo de gran consumo como es un aire acondicionado. Si nos encontramos con un decremento de tensión de larga duración, los problemas pueden ser mayores, ya que según qué tan fuerte sea el decremento, los equipos podrían llegar a apagarse (salvo tener una UPS preparada para soportar toda la carga).

Por otro lado, el **incremento de tensión** podría llegar a sobrecargar la fuente de alimentación, quemándola y dejándola fuera de servicio, razón por la cual habría que cambiarla. En general, es producido por fallas en los transformadores del proveedor de la red eléctrica.

Si es por un lapso de tiempo corto, el riesgo es moderado, pero si se sostiene en el tiempo, los riesgos son mucho mayores y podrían quemarse algunos equipos, dejándolos inactivos (salvo que tengamos en nuestra instalación un estabilizador de tensión).

Solución:

- instalar un estabilizador de tensión (con elevador de tensión) o UPS.

Distorsión de forma de onda

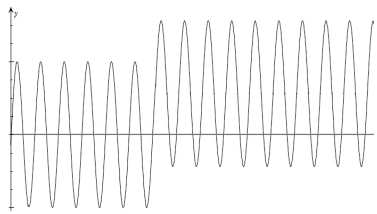
Son fenómenos en donde la forma de la onda resulta alterada por distintos factores externos. Generalmente, son de bajo impacto para los equipos, ya que la mayoría de las fuentes de alimentación pueden absorber este tipo de anomalías, como son:

Ruido: a la señal original se le suma otra tensión indeseada muy pequeña, alterando de manera constante la señal original, que es generalmente causada por frecuencias electromagnéticas como las producidas por motores, materiales o conectores eléctricos defectuosos, transmisores de radio cercanos.

Solución:

- revisar si la instalación a tierra es correcta.
- detectar la fuente del origen de la señal electromagnética.
- revisar el blindaje del cableado.

Desplazamiento de frecuencia (CC)



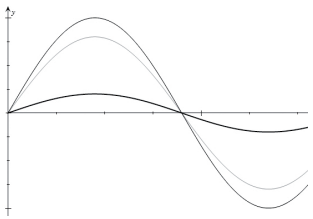
Lo generan los equipos de alimentación de corriente continua defectuosos, produciendo energía que tiene una señal inadecuada para los equipos del Data Center, pudiendo causar recalentamiento en los transformadores o producir interferencias. Pueden estar originadas por fallas en los rectificadores o en las fuentes de alimentación.

Solución:

- reemplazar el equipo defectuoso.

Distorsión armónica

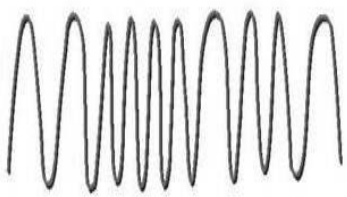
Se produce cuando a la señal original se le suma una señal adicional (de menor magnitud) en la misma frecuencia, por lo que se produce un efecto de adición entre las dos señales que resulta en una nueva señal total, distinta de la original. Generalmente causados por fallas en los transformadores o equipos de distribución eléctrica sobrecalentados.



Solución:

- si las fuentes de los equipos no pueden absorber el defecto se deberá revisar instalación eléctrica, instalar filtros de línea o UPS.

Variación de frecuencia



Son distorsiones en la frecuencia normal, poco usuales de presenciar en sistemas de alimentación eléctrica de red, pero suelen aparecer cuando se activan los generadores.

Las fuentes de alimentación de los equipos están preparadas para resistir este tipo fenómeno sin problemas si se producen en forma moderada.

Solución:

- revisar el regulador de voltaje del generador.

Resumen de los tipos de fenómenos eléctricos

Perturbación	Fenómeno	Origen	Efectos	Soluciones
Transitorios	Impulsiva	Rayo, una desconexión de una UPS grande o una descarga electromagnética	Pérdida de datos o daños a los equipos	TVSS, Humedad controlada, UPS
Interrupciones	Corte de energía	Interrupción suministro eléctrico del proveedor	Daños severos en equipos.	UPS y generador
Bajada de tensión	Bajada oscilatoria	Equipos de gran consumo que se encienden	En bajas pérdidas las fuentes pueden absorber la falla	Rectificadores de tensión y UPS
	Sub tensión	Fallas en el transformador del proveedor eléctrico.	A cierto límite pueden apagarse los equipos	Rectificadores de tensión y UPS
Subida de tensión	Subida oscilatoria	Equipos de gran consumo que se encienden	Con incrementos moderados las fuentes pueden absorber la falla	Rectificadores de tensión y UPS
	Sobre tensión	Fallas en el transformador del proveedor eléctrico.	Daños a los equipos, quema de fuentes o hasta incluso incendio	Rectificadores de tensión y UPS

Distorsión de forma de onda	Ruido	Frecuencias electromagnéticas (motores)	Posible pérdida de datos	Blindaje de cableado y eliminación del origen
	Desplazamiento de frecuencia	Fallas en los rectificadores o en las fuentes de alimentación.	Recalentamiento de transformadores o producir interferencias	Reemplazar el equipo defectuoso
	Distorsión armónica	Falla en transformadores	Cambio en la frecuencia de onda	Fuentes con factor de corrección
	Variación de frecuencia	Fallas en el generador (regulador de voltaje)	Sin impacto a los equipos informáticos.	Corregir fallos en regulador de voltaje del generador

Control ambiental

5

"La ciencia es la expresión de una necesidad inherente al ser humano y, en todo caso, está ligada a la función superior de su naturaleza inteligente: la capacidad de crear".

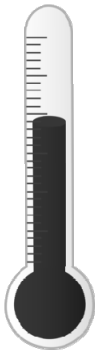
-- René Gerónimo Favaloro (1923-2000) Médico-cardiólogo argentino

El establecimiento y ejecución adecuada de una política definida sobre el control ambiental contribuye a tener un Data Center robusto, confiable y durable.

Temperatura

Por principios básicos de la física, el calor se transfiere en el sentido de la zona caliente hacia la fría cuando existe diferencia de temperatura. Los métodos de transferencia son tres:

- Convección: se da entre líquidos o gases, si existe una diferencia de temperatura en el interior de un líquido o un gas se producirá un movimiento del fluido, de calor a frío. También se lo denomina convección natural o convección forzada. Es el método que usan los *coolers* para refrigerar los microprocesadores dentro de los servidores.
- Radiación: término que se aplica genéricamente a toda clase de fenómenos relacionados con la emisión de ondas electromagnéticas como las que ocurren dentro de una cocina de microondas doméstica.
- Conducción: se da entre sólidos. Si colocamos una barra metálica sobre el fuego la podremos sostener hasta que la transferencia alcance el otro extremo y comience a quemarnos. Según las propiedades características del metal, la velocidad de transferencia de calor puede variar. Los microprocesadores de los satélites no tripulados que orbitan alrededor de la Tierra no se pueden refrigerar por convección, ya que no hay aire; la solución es utilizar disipadores apoyados sobre los procesadores para que absorban el calor por conducción.



Dentro del Data Center, el mantener una temperatura estabilizada y vigilada es una pauta fundamental del control ambiental.

El rango de temperatura **óptimo** para un Data Center es entre **17°C** y **21°C**. Es necesario aclarar que esa temperatura no es de carácter obligatorio e inamovible, sino que existe también un margen **aceptable** de operación que sería de**15°C** y **25°C**.

Cualquier temperatura mayor a 25 °C deberá ser corregida de manera inmediata, ya que implica poner en riesgo el equipamiento del Data Center.

Este rango de temperatura operacional es el indicado por los fabricantes de circuitos integrados para lograr un funcionamiento ideal en rendimiento y durabilidad, devenido de la Ley de Arrhenius[1] o también conocida como la *Regla de los 10 grados*. Esta regla dice que la vida de un componente o material se reduce a la mitad por cada 10ºC de aumento en la temperatura; aplicado inversamente: por 10ºC de disminución de temperatura, la vida útil de un semiconductor se duplicará.

En los grandes Data Centers, la temperatura es difícil de medir, ya que no existe un único punto de referencia para tomar la muestra. Por ello se debe realizar por pasillos, y hasta en algunos casos, se puede llegar a tomar la temperatura en varios Racks.

Actualmente en el mundo de IT, existe una discusión sobre cuál es la temperatura ideal para operar un Data Center debido a la publicación de las mejores prácticas recomendadas por el reconocido organismo ASHRAE[2] en 2011, donde la entidad sugiere un rango de operación permitido más amplio según el tipo de Data Center, es decir, más elevado que lo afirmado en su previa publicación en 2008, y más aún comparada contra la versión del 2004.

En 2004 la recomendación de operación era entre 20°C y 25°C; en la publicación del año 2008, el rango recomendado se amplió a 18°C y 27°C. En el año 2011, el rango recomendado se mantuvo, pero se amplió el rango permitido de 5°C a 40°C (cabe aclarar que esto no es para todos los tipos de Data Centers, sino que varía según su clasificación).

El principal impulsor para ampliar los límites provino de la necesidad de la industria de tener mayor flexibilidad, y al mismo tiempo, de reducir costos en enfriamiento, para lo cual se debe tener un claro conocimiento de la edad de los servidores y su política de renovación. No es lo mismo renovar los equipos cada

[1] Svante August Arrhenius (1859-1927) fue un científico físico-químico sueco, galardonado con el Premio Nobel de Química, en 1903.

2 ASHRAE: American Society of Heating, Refrigerating and Air Conditioning Engineers.

tres, cinco o siete años, si bien cuando se compran los equipos nadie lo hace pensando que van durar 10 años; en la práctica termina siendo mucho más habitual de lo que creemos, ya sea por razones presupuestarias o dificultades de migración.

Si sabemos que nuestros equipos se renuevan siempre cada tres años probablemente no tengamos problemas operando nuestro Data Center a 27 °C. En cambio, si sabemos que la vida útil de nuestros servidores va a ser mucho más extendida, deberíamos pensar en un rango de operación más bajo para así prolongar la duración de los equipos. Como se citó anteriormente, según la *Regla de los 10 grados*, a menor temperatura, mayor es la durabilidad de los componentes.

Por otra parte la norma TIA/EIA-942 recomienda como rango aceptable de temperatura entre 20°C y 25°C.

- ¿Qué rango de temperatura recomiendan los principales fabricantes de servidores?
  - IBM: 22°C
  - Dell: 23°C
  - HP: 22°C

- ¿A qué temperatura operan los Data Centers de las grandes empresas?
  - Google: 26°C **(*)**
  - Sun: 27°C **(*)**
  - Cisco: 25°C **(*)**
  - Facebook: 22°C **(*)**

(*)Información disponible en la sección "Video Tour" de la página `http://www.datacenterknowledge.com/`

Humedad

La amenaza menos visible de los equipos dentro del Data Center es la humedad, más aún, algunas personas llegan a omitirla dentro de sus consideraciones al momento de monitorear.

La humedad ambiental es la cantidad de vapor de agua presente en el aire. Se puede expresar de dos formas: mediante la humedad absoluta, y de forma relativa o grado de humedad (también conocido por las siglas HR). La humedad relativa es la relación porcentual entre la cantidad de vapor de agua real que contiene el aire y la que necesitaría contener para saturarse a la misma temperatura. Por ejemplo, una humedad relativa del 60% quiere decir que de la totalidad de vapor de agua (el 100%) que podría contener el aire a esta temperatura, solo tiene el 60% de vapor.

Otro término importante es el punto de condensación o punto de rocío, representado por la temperatura a la cual el agua que está en el aire cambia de estado de gaseoso a líquido, es decir, cuando la HR = 100%. Entonces, el aire se considera saturado.

A medida que aumenta la temperatura del aire, aumenta la capacidad para retener agua, lo cual es otro buen motivo para controlar la temperatura. Esto es un efecto secundario del consumo de aire frío por parte de los equipos informáticos. Cuando el aire frío pasa desde el frente de los servidores, sale con mayor temperatura y con mayor capacidad de retener agua.

Característica	Ingreso al servidor	Salida del servidor
Temperatura del aire	22°C	37°C
Humedad Relativa	50%	22%
Punto de condensación	**12°C**	**12°C**

El aire que ingresa por el frente del servidor para refrigerarlo tiene propiedades distintas cuando sale por la parte trasera. A mayor temperatura, menor HR e igual punto de condensación.

Existen dos posibles amenazas relacionadas con la humedad relativa dentro del Data Center:

- **Descargas electroestáticas:** dentro de un Data Center, las posibilidades de descargas electroestáticas[3], también conocidas como ESD (*electrostatic discharge*) se producen cuando la humedad baja. Asimismo, esas posibilidades aumentan aún más si la temperatura es baja. Las descargas electroestáticas pueden ser apenas perceptibles para las personas, pero no causan ningún tipo de daño. En cambio, una descarga de 10 Volts, ya es capaz de dañar un equipo.
- **Corrosión:** ocurre cuando un elemento metálico es expuesto al agua, ya sea porque se moja o se generan pequeñas gotas causadas por la condensación de agua en el aire. Por ejemplo; en un ambiente con una humedad alta. Los elementos dentro de los servidores se pueden dañar y sufrir una pérdida de datos.

[3]Corriente rápida producida por dos objetos que tienen carga estática. Cuando alguno de ellos se acerca lo suficiente para producir arcos o descargas, se genera una electricidad estática que puede destruir un dispositivo electrónico semiconductor.

La clave es encontrar un equilibrio justo para tener lograr tener la humedad en un rango óptimo donde se eviten las descargas estéticas y de condensación. Por ello, el rango más adecuado de humedad es entre el 40% y el 55% (también es el rango recomendado por la norma TIA/EIA 942).

Por arriba del 55% podría haber síntomas de corrosión, y por debajo del 40% comenzarían a aumentar los riesgos de descargas estáticas.

Como medida adicional de protección se pueden instalar supresores de sobretensiones transitorias o TVSS (Transient Voltage Surge Supressors) definidos por las normas eléctricas internacionales con el fin de proteger las instalaciones eléctricas de incrementos o picos de voltaje generados por fenómenos de carácter transitorios (lapso muy reducido de tiempo). Estos fenómenos inesperados pueden causar serios problemas en las instalaciones y en los equipos sensibles. Por esta razón, su importancia clave dentro del sistema de protecciones.

La sobrecarga puede tener dos fuentes de origen:

- Interno: asociados con las sobretensiones relacionadas con maniobra y conmutación entre circuitos dentro de la propia instalación. Prácticamente todas las conmutaciones en las redes del tipo industrial, y particularmente las potencias elevadas, producen sobretensiones.
- Externo: causado principalmente por descargas eléctricas provenientes de la atmósfera como pueden ser los rayos.

La norma IEEE C62.41 determina tres categorías de supresores, los cuales varían su tipo de acuerdo al lugar a donde se instalarán:

- Supresores Clase A: sirven como protección directa de las cargas (salidas de tomacorriente, toma múltiple, etcétera).
- Supresores Clase B: se instalan como protección de alimentadores de gran potencia y circuitos ramales cortos (en tableros de distribución secundarios).
- Supresores Clase C: aquellos que se instalan como protección primaria en la cabecera de la instalación contra sobretensiones externas. Son el punto de entrada entre el transformador y el primer medio de desconexión (en tableros de distribución principales a la salida del transformador).

Otras alternativas para prevenir descargas electroestáticas:

- Conexión a tierra: la conexión a tierra es un medio de drenar las cargas electrostáticas presentes en un medio.
- Aislamiento: el aislamiento consiste en envolver con material aislante los equipos IT durante el almacenamiento o transporte, ya que las descargas electrostáticas no pueden penetrar en los empaques.

- **Prevención:** es conveniente tener en cuenta los siguientes consejos para prevenir las ESD:
  - Revisar periódicamente la conexión a tierra común y la conexión a tierra de los equipos.
  - Mantener los puestos de trabajos limpios y libres de material innecesario (en especial de plástico).
  - Instalar humificadores: son dispositivos que tiene sensores, los cuales envían señales para comenzar a funcionar cuando el umbral para el cual están configurados es alcanzado. Existen muchos tipos de humificadores con diferentes ventajas y desventajas en cuanto al costo inicial, de operación y mantenimiento que tendrán que ser analizados. Aquí solo se detallan los cuatro tipos más comunes:
    - Ultrasónicos (adiabáticos): generan vapor mediante ondas ultrasónicas. Poseen discos sumergidos en agua que vibran con 1.65 MHz, rompiendo la molécula del agua y produciendo vapor frío que se inyecta en el aire. Se produce un enfriamiento adiabático de humidificación (de allí su nombre). En los equipos centralizados se integran directamente con el aire acondicionado para un correcto funcionamiento. El consumo eléctrico de estos sistemas es bajo.
    - Infrarrojos: genera vapor mediante una lámpara de cuarzo que calienta el agua aumentando la humedad relativa en el aire.
    - Vapor: se genera vapor cuando se electrifican los electrodos internos y entran en contacto con el agua, que se hierve generando vapor, aumentando la HR del aire.
    - Centrífugos: se colocan pequeñas gotas de agua sobre discos que giran a gran velocidad, usando la fuerza centrífuga para atomizar el agua en ambiente.

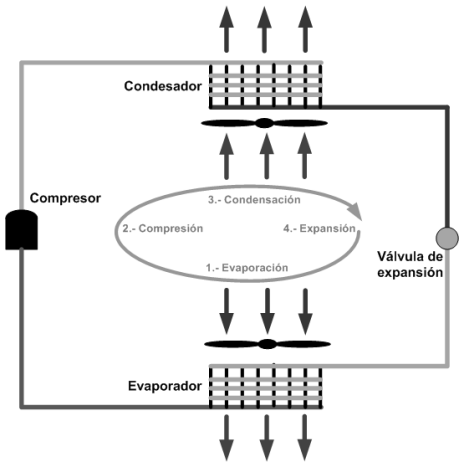
Como solución final al problema, en el mercado existen humificadores ultrasónicos que muestrean la humedad relativa del ambiente y automáticamente regulan la humedad para mantenerla dentro del rango deseado.

- **Mediciones:** La humedad relativa y la temperatura deben tomarse en el frente donde ingresa el aire frío al equipo. Para medir las condiciones ambientales del Rack se debe colocar el instrumento de medición dentro del primer tercio del mismo comenzando de arriba, 5 cm de distancia del frente del servidor.

Funcionamiento básico de un aire acondicionado

Un sistema de refrigeración es un circuito cerrado donde hay un fluido con propiedades termodinámicas específicas al que se le aplica un proceso de cuatro etapas por medio de las cuales se permite ingresar aire frío y eliminar el aire caliente de la zona donde se instala. Las etapas son: *Evaporación → Compresión → Condensación → Expansión*. Ellas funcionan de forma cíclica para disminuir la temperatura del aire.

Según la *Ley ideal de los gases*[4], cuando un gas se comprime, genera calor. Cuando se expande, hace lo inverso, cambiando de estado, de líquido a gaseoso.



Las fases de un mecanismo básico de refrigeración son:

Etapa 1: Evaporación

El aire caliente del Data Center se envía mediante ventiladores al evaporador, donde comienza el intercambio de calor. El fluido refrigerante que se encuentra aproximadamente a 7°C necesita absorber calor para poder evaporarse (convirtiéndose de líquido a gas). El evaporador utiliza un líquido refrigerante (generalmente R-22[5]) para enviar aire frío al Data Center. En este momento, el refrigerante se transforma en un gas caliente.

Etapa 2: Compresión

El fluido refrigerante en estado gaseoso y caliente es aspirado por el compresor, pero para poder disminuirle la temperatura, primero se le debe aumentar la presión,

[4] Formulada por Robert Boyle y Edme Mariotte, en 1676, define que el volumen y la presión de un gas a determinada temperatura es siempre constante (V*P)/T=cte, es decir, que el volumen es inversamente proporcional a la presión.

[5] R-22 o HCFC-22 (Monoclorodifluorometano). Se encuentra en proceso de desaparición porque daña la capa de Ozono. Los posibles reemplazos son R427A, R410A, el R407C y el R134a.

comprimiéndolo hasta alcanzar los 200 PSI[6] (o 14 Bares), dicha compresión también eleva la temperatura del gas a 52°C.

Etapa 3: Condensación

El fluido en estado gaseoso entra al condensador a alta presión y temperatura. Por medio de un ventilador comienza la cesión de calor del fluido al aire que atraviesa el intercambiador (formado por pequeños tubos metálicos, similar al radiador de un automóvil), expulsando aire caliente hacia el exterior. Además, en esta etapa se produce la condensación del fluido refrigerante que disminuye su temperatura.

Etapa 4: Expansión

El fluido refrigerante que aún está a una temperatura y presión elevada pasa por la válvula de expansión termostática, donde se produce una caída brusca de presión y temperatura. El fluido sale de la válvula en estado líquido a presión baja y a una temperatura de 7ºC.

Control

El control podría considerarse como una quinta fase continua que ocurre en todas las etapas, en la que se regula la temperatura según los parámetros establecidos. Según el equipo puede tener más de un sensor que regule la temperatura de funcionamiento.

El fluido a la salida del evaporador y a la entrada del compresor debe estar en estado gaseoso para evitar posibles deterioros en el compresor. En los circuitos equipados con una válvula de expansión termostática, el control se realiza a la salida del evaporador mediante el recalentamiento o diferencia entre la temperatura a la salida del evaporador y la temperatura de evaporación. Dicho valor debe estar comprendido entre los 2ºC y los 10ºC. En caso de encontrarse fuera de estos márgenes, la válvula se abre más o menos para permitir la entrada de un caudal mayor o menor al evaporador; por lo tanto, resulta imprescindible no variar el tamaño de dicha válvula.

Tipos de unidades de aire acondicionado

Básicamente, existen dos grandes grupos de equipos utilizados para refrigeración:

[6] Unidad medición de presión (*pounds per square inch*) libra-fuerza por pulgada cuadrada. 1 psi = 0.0698 bares.

Domésticos

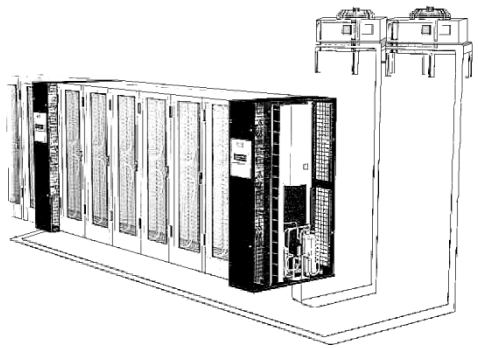
Son los que se utilizan en los hogares (también llamados *split*). Tienen una capacidad de enfriamiento relativamente baja, ya que están diseñados para cubrir áreas pequeñas; su finalidad es el confort, por lo cual no suelen ser muy precisos ni están preparados para funcionar durante períodos de tiempo prolongados.

Profesionales

Utilizados en grandes edificios que requieren bajar la temperatura en espacios muy grandes con gran nivel de precisión y confiabilidad. Diseñados para funcionar 24 x 7 los 365 días del año, salvo en casos de mantenimiento planificado. Además poseen mayor capacidad de enfriamiento con menores costos operativos. A continuación, se describen los diferentes equipos de enfriamiento que se usan en los Data Centers.

Aire acondicionado portátil

Son equipos móviles de baja capacidad que se colocan en el interior del Data Center para cubrir una demanda repentina o en una determinada zona puntual. Son simples de instalar, ya que se colocan cerca de la pared exterior, algunos modelos ni siquiera requieren colocación. Resultan poco prácticos en un Data Center de uso permanente, ya que utilizan situaciones de espacio reducido o para mitigar alguna situación crítica, como los *hot spots* o puntos calientes. Existe riesgo de derrames de líquidos por condensación.



Refrigeración por aire o expansión directa (DX)

Consiste en un sistema integrado por dos módulos. El exterior se encargará de eliminar el calor por medio de tuberías y se conectará con el módulo interior (CRAC, Computer Room Air Conditioning), ubicado dentro del Data Center (que posee reguladores de humedad, ventiladores, válvulas, filtros entre otros componentes) y distribuirá el aire frío a los equipos. Básicamente, funcionan como el resultado directo de la expansión y compresión del refrigerante vaporoso que cambia de estado líquido a gaseoso según la etapa.

Cuando se aplica la presión al gas, su temperatura aumenta y viceversa. Se utilizan en ambientes chicos o medianos, y su mantenimiento es sencillo.

Los equipos exteriores son grandes, pudiendo pesar más de una tonelada. En caso de que se coloquen sobre el techo, se debe asegurar que la loza esté preparada para soportar la carga de dicho equipo.

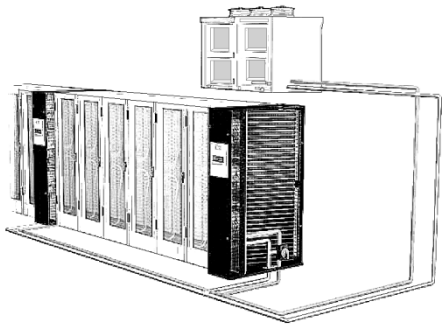
Es recomendable que el compresor se encuentre en el módulo exterior, ya que facilita el mantenimiento. Además la instalación de cañerías no debe tener pérdidas de presión, por lo que no es recomendable que abarquen largas distancias.

Para proveer un mejor rendimiento, algunos fabricantes agregan un sistema de refrigeración adicional que dispersa pequeñas finas gotas de agua como si fuera un *spray* sobre el condensador. Esto mejora la eficiencia de expulsión de calor, potenciando la capacidad de enfriamiento y reduciendo el consumo eléctrico.

Refrigeración por Glicol

Es también un sistema de expansión directa que en lugar de utilizar gas, se lo reemplaza por una solución sintética anticongelante llamada Glicol o Glycol en inglés, es similar a la utilizada en los radiadores de los coches. Con dicho producto se obtienen mejores resultados, ya que hay menor corrosión, mayores costos en insumos, menor frecuencia de mantenimiento, logrando un mejor nivel de recuperación de temperatura.

Si las condiciones exteriores son favorables (estaciones invernales o climas fríos) es posible mejorar aun más el rendimiento aprovechando el clima exterior, haciendo circular el líquido por una serpentina que disminuya la temperatura del fluido de manera natural, disminuyendo así los costos operativos.



Refrigeración por agua

Este mecanismo posee una unidad de refrigeración en el interior del Data Center (CRAH, Computer Room Air Handler), y una bomba que toma el agua de un depósito exterior para refrigerar el aire por medio del módulo interior. El agua del circuito se reutiliza, tomando agua a menor temperatura y retornado el agua para ser utilizada (a mayor temperatura).

Si las condiciones exteriores en invierno son muy extremas, el tanque deberá estar preparado para que el agua allí contenida no se congele; en verano, debe prevenirse la evaporación.

La instalación de cañerías es muy crítica, ya que se pueden producir filtraciones dentro del Data Center con consecuencias peligrosas, pero permite distancias más largas que los sistemas exteriores e interiores.

Refrigeración por agua helada (Chilled Water)

Similar al sistema de refrigeración por agua, pero en este caso, existe en el módulo exterior. Posee un enfriador que disminuye la temperatura del agua a 7°C, haciendo que el agua llegue al módulo interior a menor temperatura, luego aire caliente pasa por las cañerías y se enfría por medio de los radiadores. Se utiliza en Data Centers grandes o donde la densidad de enfriamiento requerida es grande. Las cañerías pueden recorrer mayores distancias. Se recomienda para instalaciones de alta densidad que requieran al menos 100 kW (sino resulta demasiado costoso). Si bien es el método más eficiente de disipación de calor, su principal desventaja es que las cañerías con agua deben ingresar a la superficie del Data Center donde se encuentran los servidores, lo que genera un riesgo que debe ser tenido muy en cuenta.

Refrigeración Libre o Free Cooling

Es una solución de refrigeración simple, que aprovecha el aire fresco del exterior conduciéndolo hacia el interior del Data Center por medio de ventiladores, y generando un ahorro muy significativo que puede llegar al 75%, dependiendo de las condiciones climáticas externas.

Solo puede ser utilizado en lugares donde las temperaturas exteriores sean menores a las establecidas para los pasillos fríos. Por citar un ejemplo: en Berlín el 90% de los días de año, la temperatura es inferior a los 19°C, y más aún en los países nórdicos.

En lugares donde el Data Center está ubicado en zonas donde el polvo y la polución del aire no se pueden eliminar con filtros, no se puede utilizar este método de enfriamiento.

La humedad debe ser regulada con humificadores. Algunos modelos ofrecen un módulo adicional de enfriamiento mecánico para cuando la temperatura del aire exterior no es utilizable para disminuir la temperatura del Data Center (agua helada o expansión directa).

Es importante destacar que el flujo de aire que ingresa por este mecanismo debe ser regulado, ya que si es demasiado fuerte puede perjudicar a los sistemas de extinción de incendios, dispersando la concentración de los agentes de eliminación de fuego que está instalado sobre los equipos.

Refrigeración por aceite (experimental)

Es una tecnología nueva que se encuentra en fase de ensayo desarrollada por *Green Revolution Cooling* (www.grcooling.com). Propone un modelo donde los equipos son sumergidos completamente en un aceite mineral, no tóxico y tampoco conductivo a fin de disipar el calor, similar al utilizado en grandes transformadores eléctricos.

Su principal ventaja es la gran reducción en costos de enfriamiento (entre el 90% y el 95%), y entre el 10% y el 20% en consumos del servidor, ya que se eliminan los ventiladores internos. Una desventaja es que requiere una preparación especial de los equipos, eliminando los discos o sellándolos, pero puede ser útil para ciertas configuraciones especiales. La iniciativa cuenta con el aval de Intel que ha participado en las etapas de prueba, y luego de evaluar los resultados de los servidores que estuvieron sumergidos y funcionando por meses, no se encontraron daños en ellos.

Resumen comparativo de tipos de sistemas de refrigeración

Categoría	Tipos de Aires acondicionados					
	Portátil	**Expansión Directa (DX)**	**Expansión Directa Glicol (DX)**	**Refrigeración por agua**	**Refrigeración por agua helada**	**Libre**
Costo inicial	Bajo	Reducido	Medio	Alto	Alto	Alto
Costo operación y mantenimiento	Bajo	Media	Medio (un poco menor que DX)	Alto	Alto	Medio
Vida útil	Baja	Media	Larga	Muy larga	Muy larga	Muy larga
Capacidad de enfriamiento	Baja	Media	Media	Alta	Muy alta	Alta o Muy alta
Relación enfriamiento/ energía consumida	Mala	Aceptable	Buena	Muy buena	Muy buena	Excelente
Tamaño Data Centers	Chicos	Medios	Medios	Grandes	Muy Grandes	Grandes o Muy grandes
Introduce líquido al área del Data Center	No	No	Si	Si	Si	No
Económicamente viable para Data Centers que requieran	menor 4 kW/h	7 a 200 kW/h	30 a 1000 kW/h	30 kW/h o más	200 kW/h o más	1000 kW/h o más

Los equipos de refrigeración profesionales están diseñados para mantener la temperatura constante con un margen de error de entre ±0.56-1°C y la humedad entre ±3-5%.

Estimación calórica

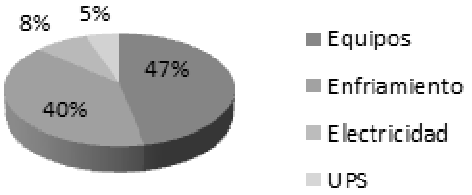
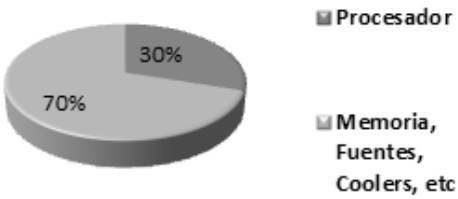
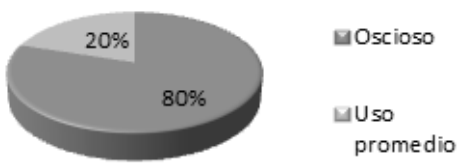
Prácticamente, el 100% de la electricidad que ingresa al Data Center se transforma en calor de alguna u otra forma, ya que todos los elementos que allí se almacenan generan calor: servidores, equipos de enfriamiento, transformadores, UPS, ventiladores, iluminación, sensores, etcétera. Como se mencionó en el capítulo 3, el incremento de la cantidad de CPU tiene una tendencia que va en aumento. Esto se puede resumir en más calor y más consumo eléctrico, en un espacio más reducido.

Los fabricantes de hardware buscan aprovechar al máximo la tecnología buscando procesadores más potentes. Antiguamente, los procesadores poseían solo un núcleo interno, y todas las operaciones se realizaban allí. Pero con la optimización y el procesamiento paralelo, los procesadores, un solo procesador físico es capaz de tener, dos, cuatro, seis y hasta ocho núcleos (*cores*), que los hacen mucho más potentes, pudiendo hacer operaciones de multiprocesamiento en paralelo, mejorando la capacidad de cálculo notablemente, y también generando muchísimo más calor.

Muchas veces los equipos físicos tienen capacidad ociosa, pero por ello no dejan de consumir electricidad y generar calor, lo cual constituye un desaprovechamiento. Esto ha motivado cambios en la industria de IT, como la virtualización, que se desarrollará en el capítulo 9.

En el siguiente cuadro, se muestra el consumo promedio dentro del Data Center y sus componentes principales.

Consumo eléctrico promedio dentro del Data Center y su utilización

Data Center	Detalles
	La mayor parte del consumo eléctrico es debido a los equipos dentro del Data Center, aunque cabe destacar que el enfriamiento se lleva una parte muy importante. Según el tipo de UPS y la eficiencia puede alcanzar hasta un 15% (según la topología seleccionada)
Servidores	**Detalles**
	En promedio el procesador utiliza no menos del 30% de la electricidad consumida total, aunque también puede ser mayor según la cantidad de núcleos. Así mismo el calor generado va en aumento.
Utilización real (Procesamiento)	**Detalles**
	Tomando el uso promedio general de un servidor, en la mayoría de las veces se ve un gran desaprovechamiento de la capacidad de procesamiento real disponible, este es uno de los principales motivadores de las técnicas de virtualización.

Los requerimientos de refrigeración o generación de calor muchas veces vienen expresados por los fabricantes de quipos en BTU[7] (equivale al calor necesario que se necesita para elevar en un grado Fahrenheit una libra de agua = 0.45 kg), que si bien es una unidad que está en desuso por ser poco práctica, aún continúa vigente.

Podemos encontrar material de referencia expresado en: grados Centígrados (°C) propuesto por el Sistema Métrico Internacional, o también expresado en grados Fahrenheit (°F) usado por el sistema anglosajón. Si se precisa hacer una conversión de °F a °C la fórmula que se debe aplicar es:

$$C° = \frac{F° - 32}{1{,}8}$$

Para los cálculos de enfriamiento también se utilizan otras unidades de conversión, ya que algunas tuvieron su origen a principio del siglo pasado, pero aún se siguen utilizando, como la siguiente equivalencia:

12.000 BTU/h = 3.517 W = 1 Tonelada de refrigeración[8] = 3.000 frigorías/h

Aunque las frigorías no son unidades aceptadas en el Sistema Técnico, muchos equipos (en especial los domésticos) expresan su capacidad de enfriamiento en estas unidades que representan la capacidad de reducir 1°C la temperatura a un kilogramo de agua a 15.5°C.

Equivalencias para convertir unidades:

- BTU/h x 0,293 = Watts
- Watts x 3,41 = BTU/h
- Toneladas x 3530 = Watts
- Watts x 0,000284 = Toneladas

Uno de los primeros pasos que se debe seguir cuando se releva información sobre el Data Center, ya existente o próximo a construir, es la definición del consumo de Kw/Rack actual, y el estimado para los próximos años. De esa forma, se determinará la **densidad** de calor generado por Rack medido en Kw, lo cual no es una tarea sencilla ya que no todos los Rack tiene el mismo consumo, por ejemplo los equipos te comunicaciones, red, telefonía generan muy poco calor. Por el contrario, los servidores, que tienen muchos procesadores en un espacio reducido generarán más calor. Por eso, hay que identificar los distintos consumos por Rack.

[7] Unidad de energía británica designada por las siglas de British Termal Unit.

[8] Es el calor que absorbe una tonelada de hielo al derretirse en 24 h.

Luego de tener una clara definición de cuánto calor genera cada Rack,hay que establecer la estrategia de refrigeración. En particular, al momento de la ubicación, conviene definir diferentes tipos de zonas o identificar posibles riesgos. Una vez efectuado esto, también es necesario saber la densidad de calor generado kW/m^2 y la densidad promedio kW sobre la superficie total del Data Center. Esa información nos ayudará a definir la estrategia de refrigeración que elegiremos.

Además del cálculo del consumo de los Racks, se deberá tener en consideración el calor generado por la UPS, la iluminación, la cantidad ventanas y las personas dentro de la sala (aunque es recomendado que no las haya).

La tendencia de refrigeración evoluciona con el paso del tiempo debido al cambio de tecnologías que ofrecen nuevos dispositivos de refrigeración. Éstos tienen mayor capacidad y menor tamaño, o incluso podrían reducir los costos, haciendo a los Data Centers más versátiles y dinámicos.

En los Data Centers actuales es común encontrar Racks que tiene un consumo de 20 kW o más. Esta es una tendencia en aumento a partir del año 2004 con la aparición de servidores de 1U y los servidores Blade[9] (foto). La concentración de procesadores y servidores de alto rendimiento en espacios reducidos es una tendencia que continua en aumento. El peor escenario posible sería un Rack completo con servidores de 1U o con varios servidores Blade que pueden llegar a generar entre 30 a 50 kW/Rack.

Clasificación según el consumo promedio por Rack:

Densidad baja (tradicional)→1 a 3 kW

Densidad moderada (promedio actual)→3 a 8 kW (hasta 2 servidores Blade)

Densidad media (tendencia)→9 a 14 kW (hasta 3 servidores Blade)

Densidad alta→15 a 20 kW (hasta 4 servidores Blade)

Densidad extrema→más de 20 kW

Por ejemplo, para hacer el cálculo de generación de calor de un Rack, suponemos un Rack de 42U, donde entran 21 servidores de 2U cada uno,

[9]Está formado por un chasis que aloja entre 7 y 14 servidores individuales (hojas) en un espacio que varía de 4U a 9U según el modelo (Dell, IBM, HP, y otros). Provee gran capacidad de procesamiento en un espacio reducido, ya que comparte algunos componentes, como por ejemplo, la fuente de alimentación, placas de red, etcétera.

suponiendo que todos son del mismo modelo y tienen un consumo promedio de 575 W, el consumo total del Rack será = 12.8 kW. Los cuales generan 41.212 BTU/h de calor.

Una de las tareas más complejas es calcular la capacidad de enfriamiento necesaria para un Data Center, porque no existe una fórmula para tal fin, sino que es un proceso artesanal que depende principalmente de la planificación. Algunos diseñadores de Data Centers establecen una regla mínima de 12.000 BTU/h o 3.517 W por cada 37 m^2, y de allí para arriba según el consumo kW/m^2, además de todos los componentes adicionales ya mencionados que generan calor. La empresa APC propone en su artículo "Cálculo de los requisitos totales de refrigeración para centros de datos" un método de estimación bastante bueno en función a algunas variables que son fáciles de medir, pero no se puede tomar como la solución al problema, que es mucho más complejo, como se explicará más adelante en este capítulo. La capacidad de enfriamiento puede ser superior a la requerida, pero si no llega a los equipos de manera adecuada es un desperdicio de recursos.

Si bien cuando se eleva la temperatura del Data Center, el hardware sigue funcionando, la *performance* disminuye. Por ejemplo, el acceso a la información almacenada en los discos (que son dispositivos mecánicos de alta precisión) se ve afectado por la dilatación que sufren los materiales que operan a gran velocidad.

El calor debe ser removido de los servidores para que no sufran daños. ¿Se imaginan el calor que genera una heladera doméstica con la puerta cerrada con 300 lámparas de 100 Watts encendidas?

Existen dos estrategias para hacer un uso inteligente en la distribución de los Rack a fin de optimizar la utilización de refrigeración dentro del Data Center:

- **Distribución equilibrada:** consiste en tener un consumo similar en todos los Racks, ubicando los equipos deliberadamente de manera tal que el consumo del Rack esté distribuido equitativamente con el promedio general. De esa forma, se garantiza que el promedio de kW/Rack es uniforme en toda la superficie del Data Center. Aunque ésta no es una práctica recomendada, porque puede ser complejo y riesgoso hacer movimientos constantes de equipos para mantener el balance.
- **Distribución zonal:** en este caso, se agrupan los Racks que tiene mayor consumo y se los coloca todos juntos, de manera de establecer una metodología de enfriamiento especial en esa área específica que tiene mayor densidad, aumentando la capacidad de refrigeración y asegurando la temperatura correcta. Por ejemplo: tenemos un Data Center con refrigeración equilibrada en toda la superficie, con cuatro filas de 10 Racks en cada una, a un promedio de consumo de 4 kW/Rack, en donde deben instalar 20 nuevos servidores Blade. Lo correcto sería agrupar todos esos nuevos servidores en la misma fila, en Racks consecutivos e instalar una nueva unidad de refrigeración por fila de alta capacidad en ese pasillo.

- Para los equipos de comunicaciones que tienen muy baja densidad (<3 kW/Rack) se debería aplicar la misma estrategia de mantenerlos agrupados, por funcionalidad y por distribución calórica. Algunos Data Centers tienen salas dedicadas exclusivamente a tal función.

La peor opción sería tener varios Racks de densidad extrema distribuidos en diferentes puntos dispersos dentro del Data Center, que tiene una densidad promedio por Rack baja. Esto resultaría muy complejo para mantener una temperatura correcta en esos Racks, produciendo los que se conoce como *hot spots* o puntos calientes.

A los equipos de refrigeración les puede tomar entre 15 y 30 minutos en restablecer la temperatura. Quizás esto no parezca mucho tiempo, pero tal vez sí lo sea.

En el 2011, Computer Site Engineering Inc. realizó una simulación muy interesante en un Data Center de 2 800 m2 para analizar cuántos grados y a qué velocidad cambiaba la temperatura si se apagaba un aire acondicionando y la ventilación durante 10 minutos. Los resultados fueron los siguientes:

- Considerando una densidad 0.6 kW/Rack, pasó de 9° a 30.8°C en 14 minutos.
- Considerando una densidad 1.2 kW/Rack, pasó de 14° a 35.5°C en 10 minutos.
- La humedad relativa bajó de 25% a 19% en 10 minutos.
- A mayor densidad, más drásticos son los cambios de temperatura cuando fallan los sistemas de enfriamiento.

Estrategias de refrigeración

Dentro de un Data Center, no todo es la capacidad de enfriamiento, sino que existen distintas formas de organización que pueden maximizar el rendimiento, reducir costos y optimizar el funcionamiento de los equipos según las necesidades. Aquí se detallan las más comunes:

Orientada por sala (Room) – (densidad baja)

Fue la primera estrategia utilizada en los Data Centres, iniciada en los setenta y se mantuvo por mucho tiempo como el diseño estándar, donde siempre se requería una instalación de piso técnico por donde se colocaban los cables y por donde circulaba el aire frío. Es normalmente usado para Data Centres de entre 300 y 800 $m^{2.}$

- Ventajas
  - Es la mejor opción económica para Data Centers con un consumo menor a 2kW por Rack. Por ejemplo: donde hay muchos equipos de comunicaciones que generan poco calor, aunque es una tendencia en desuso.
  - Brinda una temperatura homogénea en toda la sala.
- Desventajas
  - No es eficiente para Data Centers con densidad mayor a 2kW por Rack.
  - Es poco ágil, ya que resulta difícil de adaptar.
  - Es sensible a la arquitectura (altura del techo, forma de la sala, ubicación de los Racks, etcétera).
  - Requiere un estudio de CFD[10] (Computational Fluid Dynamics), que resulta costoso.
  - La circulación del aire no es utilizada de manera eficiente, ya que se mezcla el aire frío y caliente.

Orientada por fila (Row) – (densidad media)

El enfriamiento se orienta por cada fila. Hay al menos un dispositivo de control ambiental (CRAC) por cada fila, ubicado en la punta o en el medio. La distancia que recorre el aire frio desde la unidad CRAC hasta el equipo es menor, eso mejora el rendimiento, ya que reduce la ventilación requerida. Actualmente es la estrategia más utilizada y eficiente para los nuevos Data Centers.

- Ventajas
  - No requiere piso técnico.
  - Permite ajustar la temperatura adecuadamente por cada fila específicamente.
  - Permite ajustar las necesidades por fila en caso de que requieran distintos niveles de redundancia.
  - Hay una menor distancia entre la unidad de enfriamiento y el equipo destino.
  - Es adaptable, modular, previsible, lo cual permite una instalación rápida.
  - Permite una densidad por Rack variable, desde 3 kW hasta 25 kW.

[10] Es un método analítico gráfico en el cual a través de imágenes térmicas se verifica la forma en que fluye el aire a distintas temperaturas y su distribución dentro de la sala.

- Desventajas
  - Desperdicia el espacio crítico en la zona de los Racks para proveer enfriamiento.

La refrigeración por fila puede ser de tres tipos:

- **Aire inyectado desde el piso:** mediante las rejillas del piso técnico ubicadas en el frente de los Racks, se suministra aire frío con la presión adecuada para refrigerar a todos los dispositivos que se alojan allí.
- **Refrigeración en la fila:** consiste en un equipo de refrigeración ubicado entre los Racks, en la mitad o en la cabecera de una fila, que provee enfriamiento a esa fila en particular, hacia los laterales, con un flujo de recirculación corto. Su desventaja es el desaprovechamiento del espacio para colocar equipos en ese sector.
- **Refrigeración por encima de los Rack**: consiste en tener un sistema de tuberías y ventiladores superiores, colocados en forma superior direccional, que apunta hacia el frente de los Racks donde están los equipos, proporcionando el flujo de aire frío necesario. De esa manera, logra mantener la temperatura adecuada en el interior del Rack sin necesidad de tener un piso técnico.

Orientada por Rack – (densidad alta)

Se aplica en situaciones donde se requiere mantener la temperatura en Racks que tienen densidad muy alta, ya que la unidad de enfriamiento se coloca directamente en ese Rack en particular, por lo cual se reduce la ventilación requerida.

Estos dispositivos pueden ser colocados en la parte inferior, en la parte superior o en los laterales del Rack. Son conocidos como side-to-side que refrigeran los equipos desde los costados (para que se puedan colocar requiere una planificación especial y Racks más anchos a los estándares de 19”).

- Ventajas
  - Modular, adaptable, es rápido de implementar (ya que existen equipos que se montan sobre el mismo Rack y no requieren piso técnico).
  - Permite la máxima densidad posible, hasta 50 kw por Rack.

- Permite ajustar las necesidades que requieran distintos niveles de redundancia.

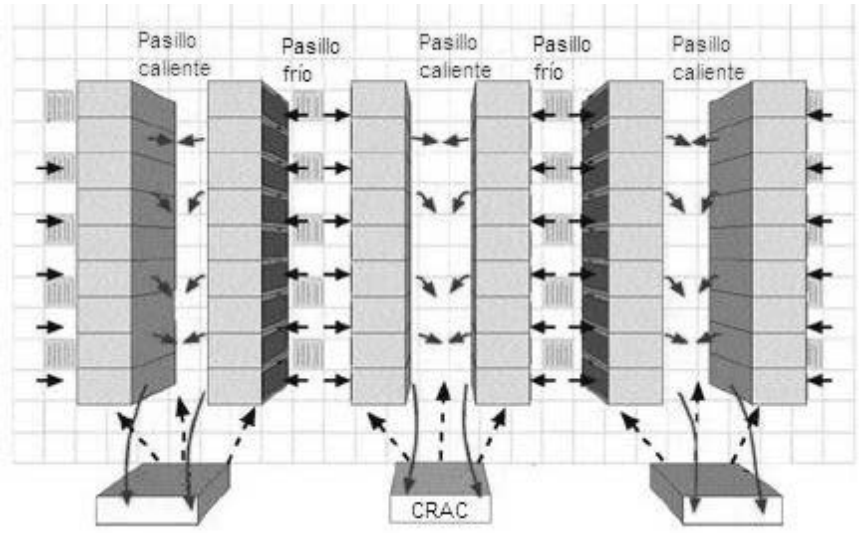
- Desventajas
  - Costo elevado (compra inicial, instalación y mantenimiento).
  - No se puede compartir con otros Racks la capacidad de enfriamiento excedente.
  - Se debe asegurar que la salida del aire caliente no afecte a otros Racks ubicados a continuación.

Hibrida – (Densidad variable)

En los Data Centers medianos y grandes es posible que existan distintas zonas que requieran mayor o menor enfriamiento según la densidad y concentración de equipos. Esta es una estrategia inteligente y ágil, ya que optimiza los recursos sobre la base del consumo necesario y sin desperdiciar. Está preparado para equipos que requieran una mayor densidad de consumo a futuro.

Diseño de pasillos

El diseño y la ubicación de los Racks dentro del área del Data Center es vital para lograr una optimización de eficiencia en la refrigeración.



Los Racks deben estar todos alineados formando pasillos opuestos unos con otros, enfrentando la parte delantera de una fila con la parte delantera de la otra. De esa forma, quedan diseñados pasillos intercalados: uno frío y uno caliente,

alternadamente. El pasillo por donde sale el aire caliente de los Racks deberá estar en forma opuesta a la siguiente fila. Los equipos toman el aire frio por la parte frontal y expulsan el aire caliente por la parte trasera.

Este diseño fue propuesto por el Dr. Robert Sullivan, en 1993, y hoy en día es prácticamente un diseño universal. Esa instalación permite una optimización de los métodos de refrigeración y puede ser potenciado aún más si los pasillos se aíslan para limitar la recirculación del aire.

Sobre la base de las recomendaciones de la norma TIA/EIA-942, los pasillos fríos deben tener 1,20 m de ancho (hasta 0,9 es aceptado), y deberán tener una temperatura no mayor a los 25°C. Por otra parte, los pasillos calientes deben tener 0,9 m de ancho (hasta 0,6 es aceptado), funcionando a una temperatura que puede oscilar entre 36°C y 47°C, dependiendo de la carga y el uso de los Racks en ese pasillo.

En el gráfico, se muestra la disposición de los pasillos. El pasillo frío se encuentra refrigerado por el aire que ingresa por el frente de los Racks a través de las rejillas de ventilación inferiores, y luego el aire caliente es expulsado por la parte trasera de los Racks, para reingresar a las unidades de enfriamiento, también conocidas como CRAC (Computer Room Air Conditioning).

En estos dispositivos, monitorean y mantienen controlada tanto la temperatura como la humedad dentro del Data Center. Poseen una entrada por donde ingresa el aire caliente y una salida por donde expulsa el aire frío. Las unidades de enfriamiento deben estar coordinadas entre sí de forma tal que funcionen de modo sincronizado, haciendo un esfuerzo cooperativo, y donde la distribución de la carga es equitativa, maximizando así la vida útil de los componentes y balanceando la energía consumida.

Si estamos armado un Data Center desde cero, la mejor estrategia de optimización de espacio es inversa a la lógica convencional de diseñar primero las paredes, las columnas y puertas en un espacio vacío que luego será amoblado con cientos de equipos computacionales. Es decir, lo que se debería hacer en primer lugar, es diseñar la disposición de los Racks, ubicación de pasillos (fríos y calientes), equipos de refrigeración, etcétera. Una vez dispuesto el diseño de la distribución de todos los elementos, es el momento de colocar las paredes, puertas y columnas en el plano. De esta forma, se logrará un máximo aprovechamiento del espacio físico, evitando así espacios muertos inutilizables.

Para tener un mejor rendimiento en los equipos de aire acondicionado, hay que disminuir el consumo eléctrico y mantener la temperatura controlada. Se recomienda hacer una aislación completa entre los pasillos, ya sea al comienzo o al final de los Racks, colocando puertas para poder acceder al pasillo aislado. Dicha separación de pasillos impide que el aire se mezcle, mejorando la temperatura y disminuyendo el consumo.

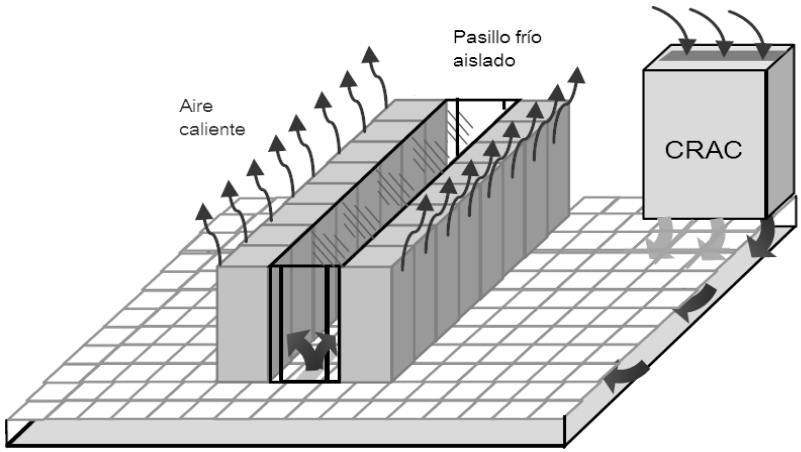
Circulación del aire

Existen distintos métodos de distribución del aire, dependiendo de si existe o no piso técnico o según el consumo de kW/Rack.

Los intercambios de aire entre el Data Center y el exterior son perjudiciales para el mantenimiento de la temperatura adecuada. Por eso, siempre se debe minimizar el acceso al área donde están los equipos.

Además se debe tener en cuenta la distancia la salida de aire frío y la toma de aire caliente con respecto a la unidad de enfriamiento.

Método de circulación de aire puede ser:



- **Por piso técnico:** el aire frío generado por un equipo instalado en la cabecera de la hilera de Racks ingresa por debajo del piso técnico a través de las rejillas perforadas refrigerando cada Rack. La salida de aire caliente por detrás no tiene ningún método de contención y se reabsorbe por la unidad de enfriamiento. Se usa en instalaciones chicas con consumos menores a 8 kW/Rack.
- **Por piso técnico con pasillos fríos cerrados:** similar al anterior, pero con la diferencia que el pasillo frío se encuentra totalmente sellado. El aire caliente que sale de los Racks reingresa a la unidad de enfriamiento. Se usa en instalaciones medianas con consumos menores a 20 kW/Rack. La aislación de pasillos puede hacerse tanto en el pasillo frío o en el caliente, ambos con resultados similares. Esto contribuye de manera importante en la reducción del consumo eléctrico pudiendo proveer disminuciones de entre un 20% y 25%.

- **Climatizadores intercalados entre Racks y pasillos fríos capsulados:** similar al anterior, con el pasillo frío totalmente sellado, pero en este caso la unidad de enfriamiento se encuentra entre los Racks a la mitad de la hilera. El circuito de circulación de aire es más corto que en los casos anteriores, permitiendo un mejor aprovechamiento del aire frío. Es utilizado en instalaciones medianas a grandes con consumos menores a 25 kW/Rack.
- **Sistemas de enfriamiento integrados directamente en el Rack:** utiliza una unidad de enfriamiento instalada en ese Rack. Tiene el circuito de circulación de aire más corto. Se utiliza en instalaciones que tengan un consumo de 25 a 50 kW/Rack

En caso de que no se cuente con piso técnico, y se envíe el aire frío utilizando una distribución superior, los métodos de circulación de aire descritos se aplicarán de igual forma.

Ventilación

Para mejorar el flujo de aire, de manera de poder alcanzar todos los sectores del Data Center y lograr un buen aprovechamiento de los recursos eléctricos es recomendable utilizar en los climatizadores ventiladores **EC** Electrónicamente Conmutado y válvulas de expansión electrónicas. El ahorro energético en esta aplicación está en el orden del 5%, haciendo la comparación con un sistema idéntico enfriado por aire, ya que el flujo de aire se puede regular cambiando la velocidad de funcionamiento del ventilador sobre la base de las necesidades en tiempo real, logrando así una elevada eficiencia a un bajo consumo eléctrico. Por ser un ventilador centrífugo con transmisión directa, las vibraciones son prácticamente nulas.

- Ventajas
  - El ahorro energético.
  - Al hacer funcionar climatizador *stand-by* se incrementa la capacidad frigorífica neta.
  - Tiene una fácil adaptación a los cambios de condición de la sala.
  - Posee un bajo nivel sonoro y ruido eléctrico.
  - Tiene un tamaño reducido.
  - No requiere mantenimiento.

Regulación presión piso técnico y velocidad de descarga

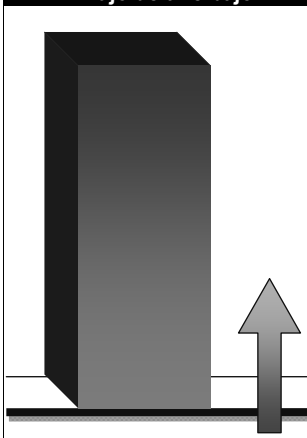
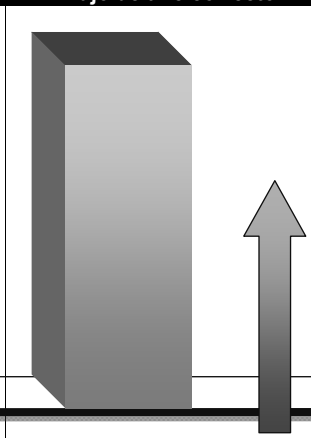
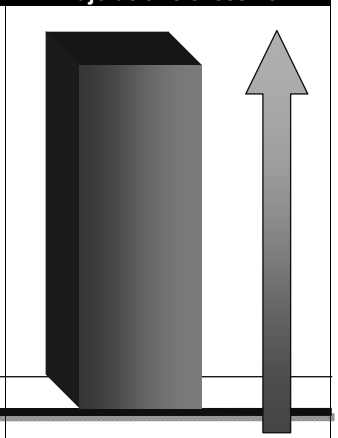
Para asegurar la correcta refrigeración de los equipos, una de las claves está en descargar la cantidad justa de aire frío, dirigida hacia la fuente de calor, mediante rejillas en el piso técnico o por ventilación superior.

En el caso del piso técnico, se produce un cambio de presión dentro del piso falso, comparado con la presión externa. En función de este diferencial, aumenta o

disminuye la velocidad de giro de los ventiladores EC de los climatizadores. En caso de tener un solo un pasillo frío encapsulado, se mide el diferencial de presión del interior del pasillo con la sala, usando esta señal para regular la velocidad de giro de los ventiladores.

En el piso del pasillo encapsulado están los elementos de control de caudal de aire frío, en función de la temperatura dentro de los Rack. La presión en el interior del pasillo encapsulado no debe superar un valor máximo para no exigir a los ventiladores en el interior de los servidores. En caso de tener múltiples pasillos encapsulados, se instala una regulación por pasillo y una de presión general del piso falso. Al reducir el caudal de aire a la mitad, el consumo eléctrico es mucho menor. A mayor velocidad de circulación del aire, menor presión estática en las placas perforadas más cercanas a la unidad CRAC.

Dicho control asegura que el aire sea el justo y necesario, permitiendo un ahorro significativo en el consumo eléctrico de los ventiladores. A continuación, se pueden ver las diferencias que existen entre un flujo correcto de aire y otros incorrectos.

Flujo de aire bajo	Flujo de aire correcto	Flujo de aire excesivo
		
El flujo de aire que ingresa por debajo del piso técnico es **insuficiente,** impidiendo que alcance a refrigerar la parte superior del Rack	El flujo de aire es el **correcto**, permitiendo refrigerar de manera uniforme a todos los equipos del Rack.	El flujo de aire es **excesivo**, haciendo que el aire frío suba de manera ineficiente, sin que refrigere la parte trasera del Rack.

El control de presión en pasillo frío encapsulado asegura que el aire fluya correctamente y se mantenga separado el frío del caliente, asegurando que el aire caliente reingrese a la unidad de enfriamiento sin pérdidas.

De ser posible es recomendado mover la refrigeración más cerca de la carga, lo que permitirá ahorrar en potencia total de ventilación y proporcionará un tiempo de reacción más rápido si varían las cargas de los equipos en los Racks.

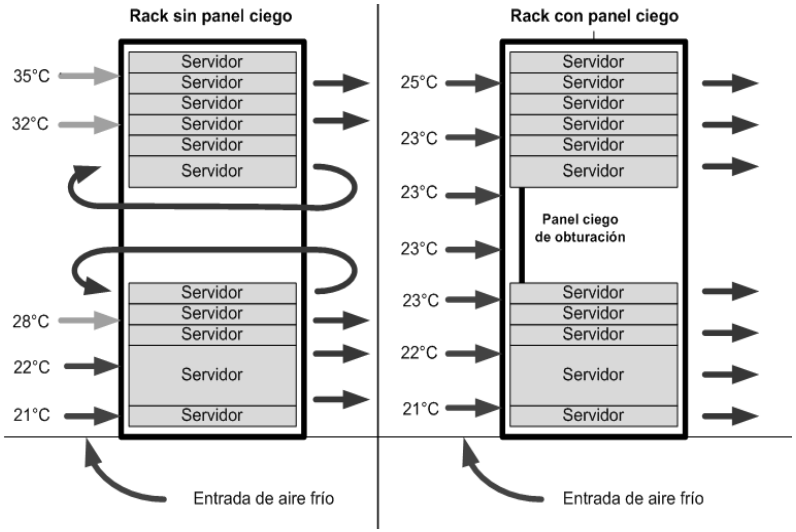
No siempre que se detectan problemas de temperaturas la solución es bajar la temperatura del CRAC. El problema también puede ser la presión de aire, por lo tanto aumentar o recudir la velocidad de circulación del aire frío puede ser la solución óptima.

En los diseños donde el aire frío ingresa por debajo del piso técnico, el pasillo frío debe estar libre de obstrucciones, permitiendo una circulación libre. Por lo tanto, los cables de alimentación y comunicaciones deberán pasar por debajo del pasillo caliente.

La eliminación del aire caliente puede estar provista por canalizaciones especiales ubicadas en el techo, que pueden ser selladas o no, ya que el aire caliente siempre tiende a subir a fin de permitir la expulsión de ese aire caliente hacia el exterior o para volver a introducirlo en la unidad CRAC. Si la temperatura de salida del aire caliente aumenta al reingresar a la unidad CRAC, el esfuerzo para enfriarlo será mayor, y viceversa.

Por otro lado, existe un problema frecuente en los Data Centers, ya que muchas veces se mueven equipos de un Rack a otro, dejando espacios libres y no se toman medidas para evitar la recirculación de aire caliente hacia el frente del Rack.

Instalado paneles ciegos (o también llamados de obturación) se impide que el aire caliente recircule hacia la parte delantera del Rack donde se encuentra la toma de aire frío para los equipos, haciendo un buen aprovechamiento de la capacidad de refrigeración.



La clave es encontrar un equilibrio justo para tener la humedad en un rango óptimo. Los paneles ciegos en los Racks ayudan a disminuir la circulación del aire, manteniendo los pasillos fríos y calientes separados.

Sensores de temperatura, humedad y mantenimiento

Como se describió en este capítulo mantener la temperatura y humedad dentro de los parámetros establecidos es de suma importancia. En ese sentido, es clave contar con herramientas de monitoreo continuo que adviertan situaciones anómalas, para así tomar las acciones necesarias que eviten mayores inconvenientes. Para ello existen sensores con capacidad de monitorear ambas variables que envían una alerta a través de la red, ya sea a una consola central, alertas por correo electrónico o SMS.

- **Sensores de sala:** monitorean la temperatura general del Data Center. Es importante que estén ubicados en una zona donde la muestra que se tome sea referencial de la temperatura global de la sala.
- **Sensores de Rack:** detectan la temperatura de un Rack específico (ya sea por la importancia de los equipos allí contenidos o como muestra aleatoria de una fila). Dentro del Rack el sensor debe estar a 2/3 de la altura total, comenzado desde abajo para tener una muestra general.
- **Sensores de piso:** ideales para detectar fuga de líquidos. Se recomienda colocarlos debajo del piso técnico cerca de la zona donde se encuentran los equipos de refrigeración.

- **Sensor de temperatura para aire acondicionado:** se colocan debajo de la salida de aire como referencia de funcionamiento. Si bien los equipos tienen sus propios sensores, es una buena práctica tener un doble control sobre el punto de salida. Esto es crítico, porque permite detectar la falla de manera temprana.

El mantenimiento de los aire acondicionados es clave para evitar problemas a largo plazo y que la vida útil del equipo sea la establecida en el momento de la compra inicial, por eso deben hacerse con la regularidad estipulada por el fabricante, así como también el reemplazo de los filtros de aire.

Seguridad y prevención de incendios

6

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados".

-- Gene Spafford (1956) Experto estadounidense en Seguridad Informática

Proteger los activos del Data Center es una responsabilidad básica y obligatoria que debe ser considerada desde el momento inicial del diseño.

Seguridad física

El acceso a las personas deberá estar regulado y limitado sólo a aquellas que necesitan ingresar para realizar tareas de mantenimiento que no puedan ser llevadas a cabo de manera remota, y también se debe evitar el ingreso de personas malintencionadas. Las personas con acceso autorizado deberán comprender la importancia del equipamiento allí almacenado para evitar así interrupciones causadas por falta de entrenamiento o fallas humanas.

La situación de entrar a un Data Center para hacer una verificación, porque un servidor no respondía y encontrarse que el enchufe donde debía estar conectado el servidor está ocupado por una aspiradora o un taladro, es una situación que ningún administrador de sistemas debe atravesar, pero que lamentablemente puede llegar a ocurrir si no se toman las medidas adecuadas.

Existen innumerables dispositivos de seguridad física, como: tarjetas identificadoras, sistemas de seguridad biométricos, cámara de seguridad, personal de seguridad, etcétera. Además es posible tener distintos niveles de seguridad según el tipo de dispositivo que se desee proteger.

Según datos brindados por el Uptime Institute, **los errores humanos son la principal causa de interrupciones dentro de los Data Centers, siendo responsable del 60% de los incidentes**, ya sean por distracciones, errores de comunicación, errores de etiquetado o fallas en los procedimientos. Por eso, las restricciones de acceso sólo a las personas autorizadas disminuyen la posibilidad de que se produzcan este tipo de acontecimientos indeseados.

¿Qué se necesita proteger y de qué manera?

Respondiendo a dos preguntas básicas se podrá saber qué nivel de acceso deberá otorgarle a cada persona según sus funciones:

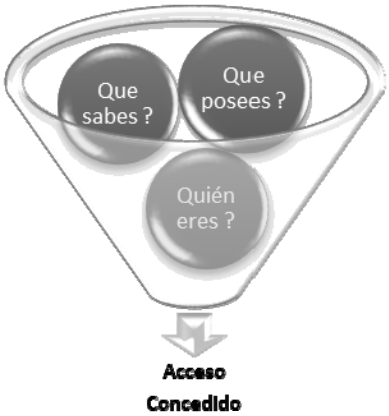
- ¿Quién eres?
  Personal interno, proveedor
  ¿Cuál es su rol?
- ¿Qué estás haciendo aquí?
  ¿Para que necesitas estar aquí?
  ¿Estás desarrollando una tarea habitual correspondiente a tu rol?
  ¿Eres un proveedor externo?

Métodos y dispositivos de identificación

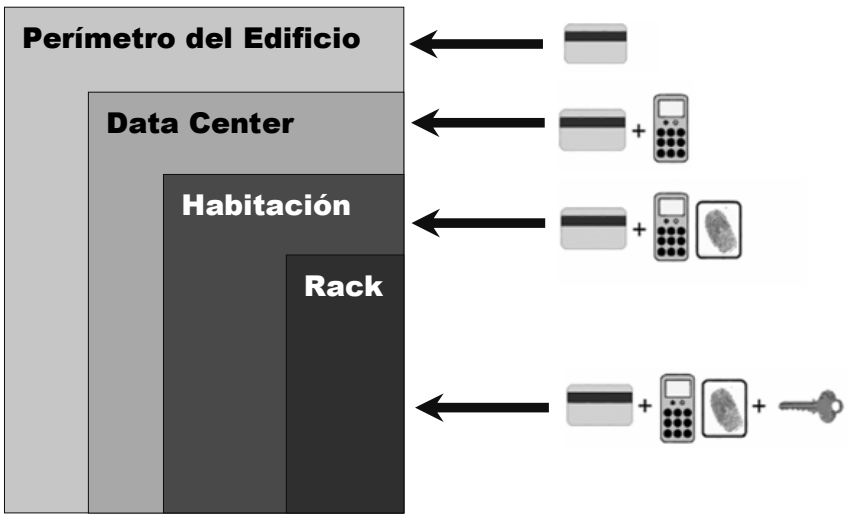
Los métodos de acceso están relacionados con los dispositivos de identificación sobre la base del nivel de seguridad. Se utilizan tres criterios básicos:

- **Qué posees:** algo que llevas o tienes en tu poder. Por ejemplo: tarjetas electrónicas, tarjetas magnéticas, tarjetas de códigos de barra (estas últimas son poco confiables, porque pueden ser copiadas fácilmente, pero son baratas) o cualquier otro dispositivo transportable.
- **Seguridad baja:** no hay garantía que lo usará la persona correcta. Se puede perder, copiar o robar.
- **Qué sabes**: como por ejemplo una contraseña. Es más seguro que algo que posees, pero el problema de las claves es que mientras más larga sea, más segura será porque será más difícil de hackear. Pero aun así, al ser muy largas o teniendo un intervalo de solicitud de cambio muy frecuente, las personas tienden a escribirlas, haciendo que se vuelvan inseguras.
- **Seguridad media:** no hay garantía de que lo usará la persona correcta, porque las claves pueden ser robadas, escritas en papel o compartidas.

- **Quién eres**: se refiere a una identificación física relacionada con alguna característica única de la persona, también es conocida como identificación biométrica, como: huella dactilar, manos, iris, cara, retina, escritura manual, voz, etcétera.
- **Seguridad alta:** es el método más seguro, ya que requiere una característica física única de la persona que fue previamente autorizada. Una desventaja de este método es que el sistema rechaza a veces a personas que están autorizadas a causa de los problemas en el lector, y entonces se debe repetir la operación más de una vez. Es importante destacar que este tipo de sistemas **no son infalibles** pese a que su costo no es bajo.



La combinación de estos tres métodos es la manera ideal y más eficaz de profundizar la seguridad, haciendo uso de niveles concéntricos según el área a donde deba acceder la persona. A medida que accedemos a una zona más oscura (ver gráfico), el nivel de seguridad es más elevado, ya que los requerimientos para acceder son más restrictivos. Esto sucede porque los controles son incrementales, es decir, que para acceder al Rack será necesario contar con una tarjeta electrónica, más una clave de seguridad que será digitada por teclado al momento de ingresar al Data Center, más una identificación biométrica que puede ser la huella digital para acceder al área. Y finalmente, deberá poseer en su poder la llave del Rack para llegar al servidor.



Identificar estas aéreas y clasificarlas según el nivel de seguridad que necesitan es parte de un buen diseño. **El color más oscuro representa un mayor nivel de protección.**

Cámara o CCTV (Circuito Cerrado de Televisión)

La colocación de cámaras dentro del Data Center puede ser muy útil para identificar actos de vandalismo, si bien es cierto que son medidas reactivas en lugar de preventivas (ya que no evitan los incidentes) permiten revisar las grabaciones luego de que ocurrieron los hechos. Aunque pueden ser elementos de disuasión en algunos casos.

Las cámaras deben estar ubicadas de manera que permitan identificar a las personas, cubriendo la mayor superficie de visionado posible, como así también puertas y zonas críticas. Las cámaras pueden ser fijas, móviles automáticas rotatorias o controladas remotamente.

Una vez que el CCTV está instalado, se debe establecer una política clara sobre cómo se van a manejar las filmaciones. Esta política debería responder las siguientes preguntas:

- ¿Cómo se van a catalogar y ordenar las cintas?
- ¿Se almacenarán dentro o fuera del Data Center?
- ¿Quiénes tendrán acceso a ellas?
- ¿Cuál es el procedimiento para acceder a una grabación?
- ¿Por cuánto tiempo se mantendrán las cintas almacenadas antes de ser eliminadas?

Personal de seguridad

El personal de seguridad debe ser calificado y entrenado para brindar la mejor protección. Deberá tener procedimientos claros a los cuales deberá apegarse. Por ejemplo, deberá tener una política de acompañamiento en caso de visita de alguna persona técnica para realizar una tarea de mantenimiento en un área crítica. Una de sus habilidades será responder con inteligencia y rapidez ante eventos no esperados.

Más allá de los sensores tradicionales, existen otros especialmente diseñados para alertar al personal de seguridad, como: sensores láser barrera, sensor de pisada, sensores de contacto o sensores de vibraciones.

Los visitantes deben quedar registrados al ingresar y al salir, con nombre, fecha, hora y motivo.

La tentación de sortear un procedimiento de seguridad a una cara conocida puede tener consecuencias catastróficas, sobretodo en casos de sabotaje.

La protección del robo de información debe ser también una política de seguridad. Por ello debe documentase qué elementos de transferencia de información pueden ingresar o salir del Data Center y quiénes son las personas autorizadas para ello.

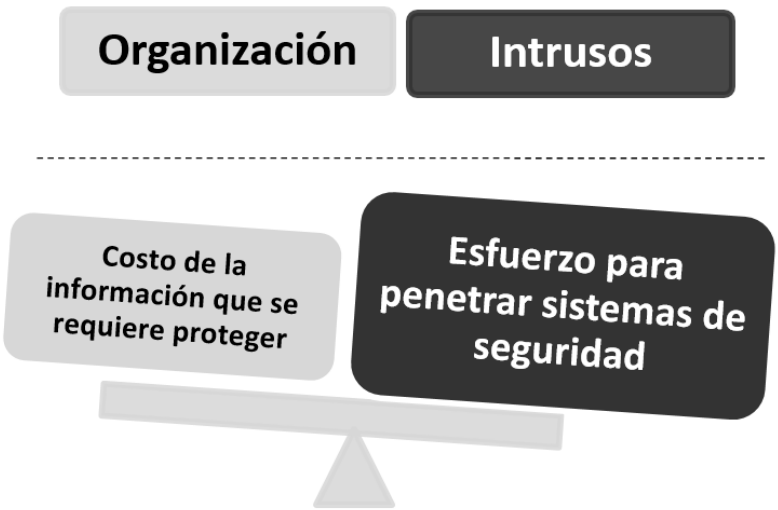
Considere que las personas que tienen acceso físico directo a los servidores, pueden copiar en un pequeño dispositivo donde caben cientos de Gigabytes de información que pueden ser traducidos en millones de dólares.

Balance entre el riesgo y el costo

Los costos de la instalación inicial del equipamiento de seguridad pueden ser muy elevados si el diseño es exagerado para las necesidades. Adicionalmente se agregan los costos de mantenimiento y los sueldos del personal de seguridad. Esos costos deben estar en equilibrio con el valor de la información que deseo proteger.

Los especialistas en seguridad informática utilizan una fórmula muy simple y efectiva para definir qué medios arbitrarán para proteger la información de ataques informáticos.

Costo económico para vulnerar el sistema > Costo de la información protegida



Si necesitamos proteger la información de un servidor que almacena los diseños y planos de un microprocesador de alta tecnología para los cuales se invirtió 1 millón de dólares en su desarrollo, la estrategia de protección de la seguridad deberá considerar que aquellas personas que intenten violentar el

sistema deban tener que incurrir en un gasto tan elevado que no les compense el ataque, ya que será más redituable producir la información que robarla.

Esta misma analogía se puede aplicar a la seguridad de los Data Centers y a cuanto se debe invertir para la protección física y lógica de los datos.

Seguridad extrema

Existen ambientes donde la seguridad tiene una gran preponderancia en relación a los equipos allí alojados, donde podrían existir diseños de puertas doble o llamado "mantrap" en el cual, la segunda puerta no se puede abrir hasta que la primera puerta no esté cerrada, asegurando que solo ingrese una persona a la vez que posea ese doble acceso requerido.

Un ejemplo de Data Center con medidas de seguridad extremas es el que se finalizó de construir en septiembre de 2013 la agencia estadounidense NSA (National Security Agency) en Bluffdale, Utah, destinado a almacenar el sistema de espionaje más complejo del mundo, capaz de analizar: búsquedas de ciertas palabras claves, correos electrónicos, llamadas telefónicas, datos bancarios, fotos, etcétera.

La revista Wired publicada en abril de 2012 reveló que el programa tiene un presupuesto estimado en 2 000 millones de dólares para una superficie aproximada de 9.000 m2 que albergará cientos de Racks, además contará con otro espacio mucho más grande para oficinas administrativas y técnicas, lo que lo convierte también es uno de los más costosos. Sólo para el programa antiterrorista perimetral se destinaron 10 millones de dólares, que incluye una valla diseñada para detener un vehículo de hasta 6 toneladas circulando a 80 km/h.

Además, posee su propia subestación eléctrica para una demanda de 65 MW, combustible para operar los generadores por tres días consecutivos y un sistema de enfriamiento capaz de proporcionar 60 000 toneladas de enfriamiento con tanques de agua que pueden acumular más de 6 millones de litros de agua.

Por ello es importante definir el problema de seguridad para cada Data Center y aplicar la tecnología adecuada para resolverlo.

Seguridad Lógica

Si bien la seguridad lógica no forma parte de las tareas de la administración de un Data Center nunca debe ser puesta de lado cuando se analizan las soluciones de seguridad física, ya que las amenazas digitales constituyen una de las principales preocupaciones dentro del área de IT: **la confidencialidad, integridad y disponibilidad de la información**.

Entre las amenazas digitales se encuentran los hackers, los virus, los cuellos de botella en las redes y otros ataques accidentales o maliciosos a la seguridad o el flujo de datos.

El fuego y su clasificación

Conocer bien la clasificación del fuego según el origen del material que lo genera, nos ayuda a elegir el procedimiento más apropiado para apagarlo.

Premisa básica: para que el fuego se produzca debe haber una combinación de tres elementos al mismo tiempo: calor, oxígeno y algún tipo de combustible. Si logramos evitar o extinguir alguno de estos tres elementos, el fuego se apaga.

Clasificación del fuego según el origen del material de combustión

Fuego Clase A: son los que se producen al arder los combustibles sólidos comunes como maderas, papeles, corcho, tejidos, fibras, plásticos, etcétera. Se queman en la superficie y en profundidades. Dejan residuos.

Fuego Clase B: son fuegos de líquidos inflamables, como combustible, alcohol, solventes, pinturas, barnices, etcétera. Se queman solamente en la superficie. No dejan residuos. También se incluyen los gases inflamables como el propano y butano. Los fuego clase B no incluyen fuegos que involucren grasa ni aceite de cocinar.

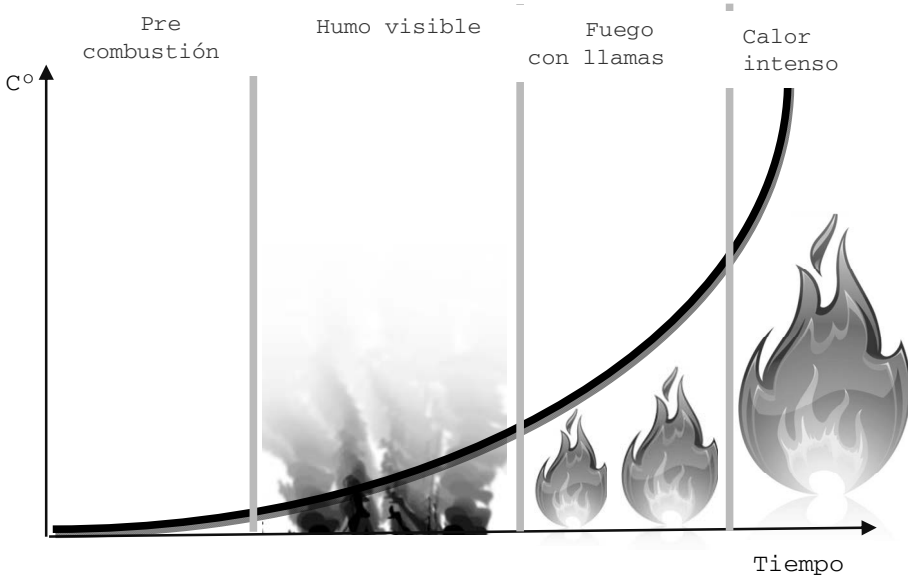
Fuego Clase C: son fuegos que involucran equipos eléctricos energizados como motores eléctricos, servidores, transformadores y aparatos eléctricos. Es uno de los más comunes dentro del Data Center

Fuego Clase D: llamados también fuegos metálicos, son los ocasionados por metales inflamables como sodio, magnesio, aluminio, potasio, circonio, titanio, etcétera, que se alimentan del fuego, y solo pueden combatirse con líquidos especiales.

Fuego Clase K: son fuegos derivados de grasas y aceites de cocina como mantecas vegetales y minerales. No existen dentro del Data Center.

Etapas del fuego

- **Pre combustión:** aquí se origina el fuego, aun cuando no es visible al ojo humano, pero puede ser detectado por algunos sensores de alta sensibilidad.
- **Humo visible:** se comienzan a ver algunos indicios de humo. Se detecta por la presencia de humo en el aire mediante la absorción o difusión de la luz.
- **Fuego con llamas:** ya comenzó el fuego y aparecen las llamas.
- **Calor intenso**: luego de varios minutos de combustión, las llamas comienzan a tomar temperatura elevada, y en este punto, el incendio se hace realmente difícil de controlar.



Reducir riesgos es la salvación

La agencia estadounidense NFPA (Asociación Nacional de Protección contra el Fuego, Nacional FIRE Protection Association) proporciona orientación para la protección contra incendios y la continuidad del negocio.

Debido a que la protección contra incendios es una parte integral de la continuidad del negocio, la NFPA en el año 2009 desarrolló la norma NFPA 75 que es una actualización de la Norma NFPA 72. En dicho documento, se detallan las mejores prácticas para la protección de equipos electrónicos y procesadores de

datos, y donde se presenta un enfoque lógico de la protección contra incendios y la continuidad del negocio basado en el riesgo que estos elementos representan.

Desde el punto de vista del negocio, el factor de riesgo más importante usualmente es el perjuicio económico ocasionado por la pérdida de equipos o información, es allí donde muchos gerentes de negocios centran su atención.

Llegado al punto donde la eventualidad se produce y aparece el fuego en nuestro Data Center tenemos que tener en claro los tres objetivos principales, en este orden:

- Detectar el fuego.
- Comunicar la existencia de fuego a las autoridades.
- Eliminar el fuego.

El enfoque lógico es, en primer lugar, prevenir incendios, lo que simplemente implica eliminar todas las fuentes de ignición y reducir la cantidad de materiales combustibles dentro del Data Center. Eso le proporcionará al incendio menos materiales de los cuales alimentarse si el fuego se origina en otro sector.

Central detención de incendios

Es uno de los elementos fundamentales por ser un punto concentrador de información. Su función es recibir los datos de los sensores humo o térmicos y activar los elementos de extinción para disparar las alarmas en caso de incendio: sirenas, alarmas sonoras, alertas a celulares o a consolas de monitoreo.

Estas consolas deben estar conectadas a la UPS para asegurar la continuidad de funcionamiento, en caso de problemas con el circuito eléctrico.

Las centrales avanzadas tienen la capacidad de dividir el Data Center en zonas, de manera tal de que si se detecta un incendio en determinado sector no se realiza la descarga del agente extintor en toda la superficie del Data Center; sino que se limitará al área afectada, reaccionando de manera inteligente, y minimizando el impacto.

Generalmente son dispositivos de tamaño reducido (20 cm x 30 cm x 5 cm), y se instalan en la pared, ya sea dentro del centro de monitoreo, cuando fuera posible, o fuera del Data Center, antes de la puerta de entrada principal, por el riesgo que puede existir hacia las personas, según el agente extintor que se utilice. Además deben contar con circuitos de activación y desactivación manual.

Acciones preventivas

- Preferentemente el Data Center debe estar aislado de otros edificios.
- No se debe fumar en las instalaciones.
- Se deben eliminar los desperdicios inmediatamente.
- Los muebles deben ser metálicos.
- No es conveniente usar material acústico, ya que por lo general es inflamable.
- Hay que realizar inspecciones oculares eventuales para detectar el material inflamable.

El área por debajo de pisos técnico puede ser un foco de incendio potencial. No solo se acumula la basura y otros combustibles debajo de él, sino que también a veces, allí se almacenan materiales, razón por la cual es recomendable una inspección periódica para eliminar muchos combustibles potenciales innecesarios, conducida por alguien cuya prioridad sea la protección contra incendios.

Los registros físicos como papeles, cintas, etcétera, en el Data Center se deben mantener en el mínimo absoluto, y se deberían tener sólo aquellos necesarios para la operación esencial. Todos los registros importantes se deben duplicar y almacenar en una ubicación remota de modo de no estar expuestos al mismo incendio que los originales. Esos elementos se deben almacenar en gabinetes metálicos cerrados bajo llave, y las bibliotecas de cintas deben estar protegidas con un sistema de extinción de incendios.

El mismo concepto se aplica para las áreas de depósito que contienen material que no está en uso actualmente, pero que serán utilizados en el futuro, entonces deberán ser etiquetados e identificados como tales. Todos los otros cables abandonados deben ser removidos siempre que fuera posible. En caso de incendio, el aislamiento del cable puede generar humo con partículas gruesas que pueden generar corrosión para los equipos.

Dentro del plan de comunicación en caso de incendio, dos elementos fundamentales son las alarmas sonoras y visuales, que deben estar instaladas en el Data Center para prevenir pérdidas humanas, y poner así en estado de alerta al personal.

"El método más efectivo es la prevención"
Prevención = Protección

Barreras contra incendios

Dado que la historia nos dice que la mayoría de los incendios comienzan en zonas aledañas al Data Center, es deseable que éste se encuentre en una ubicación separada de otros edificios. Si las limitaciones físicas hicieran imposible el cumplimiento de ese requerimiento, se pueden colocar se barreras ignífugas desde el piso hasta el techo durante la construcción, para impedir que las llamas se propaguen hacia tales áreas, aún por debajo del piso técnico y tubos de ventilación. Existen normas que establecen los límites aceptables de tolerancia ignifuga para los Data Centers como son las normas EN 1047/2 de la Unión Europea o NBR 15247 de Brasil.

Las salas mecánicas y eléctricas, que con frecuencia son extremadamente importantes para la operación continua en Data Centers de misión crítica también deberían tener una construcción del tipo ignífuga.

Los materiales para la construcción de edificios deben ser cuidadosamente seleccionados con la idea de minimizar la propagación de incendio potencial. La NFPA 75 provee detalles respecto de los materiales de construcción permitidos, que abarcan desde puertas ignífugas hasta materiales para paredes, piso y cielorrasos interiores, e incluso aún por debajo del piso técnico, ya que el fuego podría propagarse por allí.

Los detectores para cada etapa son

- **Pre combustión:** aquí se comienza a originar el fuego, aún no es visible al ojo humano, pero que puede ser detectado por algunos sensores de alta sensibilidad que usan la tecnología CCD (Cloud Chamber Detection, detector de cámara de niebla). Ésta puede detectar partículas de hasta 0.002 micrones[1].
- **Humo visible:** funcionan cuando aparecen indicios de humo, detecta la presencia de humo en el aire mediante la absorción o difusión de la luz.
    - **Detector óptico o fotoeléctrico:** consiste en un rayo **infrarrojo o haz de rayos proyectados**, compuestos por un dispositivo emisor y otro receptor. Cuando se oscurece el espacio entre ellos debido al humo, sólo una fracción de la luz emitida alcanza al receptor, provocando que la señal eléctrica producida por éste sea más débil y active la alarma. Provee una respuesta rápida ante fuegos con humos, pero puede haber dificultades de emplazamiento en locales con ventilación o aire acondicionado, ya que impiden que el humo llegue en condiciones a activar el detector. Puede sufrir un problema de pérdida de alineación si se sitúa en estructura metálica, por lo que requiere

[1] Micrón equivale a la millonésima parte del metro. Su símbolo es μm.

mantenimiento. Resulta caro si no se aprovecha toda su longitud. Se activa cuando la concentración de humo alcanza del 1.5% al 3%.

— **De tipo puntual o haz de rayos reflectados:** también reciben el nombre de ópticos de humos puntual, en los que emisor láser y receptor se encuentran alojados en la misma cámara. No se ven en forma directa, porque sus ejes forman un ángulo mayor de 90º y están separados por una pantalla, de manera que el rayo emitido no alcanza al receptor. Cuando entra humo en la cámara, el haz de luz emitido se refracta en las partículas de humo y no puede alcanzar al receptor, activándose la alarma. El detector de haz reflejado no discrimina humo de partículas de polvo, y si bien son de carácter autorregulable por impurezas, pueden enviar señal de aviso cuando están demasiado sucios. Son más resistentes que los iónicos a las corrientes del aire, y tienen mayor respuesta, pues necesitan menos cantidad de humo para activar la alarma.

  Su principal inconveniente es que no detecta al humo negro, ya que no hay dispersión de la luz (efecto Tyndall[2]). Es recomendado para Data Centers en condiciones ambientales sin polvo. Se suelen combinar con detectores térmicos para lugares donde existan equipos eléctricos o también para detectar fuegos en los conductos de aire acondicionado. Se aconseja combinarlos con detectores iónicos.

— **Detector iónico:** se basa en la disminución que experimenta el flujo de corriente eléctrica formada por moléculas de oxígeno y nitrógeno, ionizadas por una fuente radiactiva entre dos electrodos, al penetrar los productos de combustión de un incendio. Estos detectores detectan partículas visibles e invisibles generadas por la combustión, y su mayor eficacia se encuentra para tamaños de partículas entre 1 y 0.01 micrones. Las partículas visibles tienen un tamaño de 4 a 5 micrones, y tienden a caer por gravedad, excepto si hay una fuerte corriente turbulenta en la columna que forma la llama. Este tipo de detector es más barato que el óptico, y puede detectar partículas que son demasiado pequeñas para influir en la luz.

  La cámara de ionización: contiene una ínfima cantidad (menos de 1 microgramo) de Americio-241 (241Am) que emite radiación Alfa. Este isótopo radioactivo emite partículas Alfa (núcleos de helio de alta energía) durante siglos. Debido a la gran capacidad de ionizar el aire de las partículas Alfa, solo una hoja de papel o unos 7 cm de aire son suficientes para absorberlas. La radiación pasa a través de una cámara abierta al aire donde se encuentran dos electrodos,

[2]Fenómeno físico que se hace presente cuando existen partículas de tipo coloidal en el aire, que son capaces de dispersar la luz. Descubierto en 1869, por el científico Irlandés John Tyndall.

permitiendo una pequeña y constante corriente eléctrica. Si ingresa humo en esa cámara, se reduce la ionización del aire y la corriente disminuye o incluso se interrumpe. Entonces, se activa la alarma. Cuando el humo entra en la cámara de ionización, las partículas Alfa quedan prácticamente inmovilizadas por los productos de la combustión, disminuyendo notablemente la corriente eléctrica.

Permite una detección precoz y es el más universal de todos. El problema es que puede generar falsas alarmas en ambientes con partículas de polvo, aire en movimiento, humedad elevada y variación del voltaje de la corriente.

- **Fuego con llamas:** ya comenzó el fuego y aparecen las llamas. Si bien existen detectores térmicos en el mercado no son recomendados para Data Centers. Si la idea es proteger la información, no tiene sentido gastar dinero en un sistema de detección de llamas, porque ya será demasiado tarde. Los esfuerzos se deben focalizar en las dos etapas anteriores.
- **Calor intenso**: luego de varios minutos, las llamas comienzan a tomar temperatura elevada, y se hace en este punto realmente difícil de controlar. Ídem caso anterior.

Todos los detectores de humo deberán ser sometidos a pruebas periódicas, al menos semestralmente. También deberá realizarse una limpieza periódica para quitar el polvo y la suciedad acumulada. La frecuencia de esta operación dependerá del tipo de detector y de las condiciones ambientales. Para cada tipo de detector, la limpieza, verificación, funcionamiento y ajuste de la sensibilidad se deberá hacer sólo después de consultar las instrucciones del fabricante. Normalmente la sensibilidad debe ajustarse en el laboratorio.

Los detectores no deberán instalarse en zonas donde puedan causar falsas alarmas o estén expuestos a vibraciones. Comúnmente pueden emplearse en lugares donde la velocidad del aire sea de hasta 5 m/s.

Si se colocan en ductos de recirculación de aire, hay que asegurarse de que reciban suficiente cantidad de partículas de humo para activarse correctamente.

Sistemas de extinción de incendios gaseosos

El mecanismo de extinción del fuego mediante inundación de gas se basa principalmente en el concepto de la eliminación del oxígeno, añadiendo un agente gaseoso del aire ambiente y logrando que se reduzca el porcentaje de oxígeno en el aire de manera tal de que se corte la cadena de combustión.

El gas se almacena en tubos de alta presión, conformados por uno o más tanques de almacenamiento, dependiendo siempre de la superficie que se desea proteger. En el interior de los tanques se aloja el gas que efectúa la extinción. En el momento en que los sensores detectan el incendio, le enviarán una señal a la central de incendios, advirtiéndole dónde se está generando el fuego. Luego, la central accionará la válvula de los tanques y el gas fluirá desde los tubos por las cañerías, que están en los pasillos, hasta llegar a los picos difusores de descarga, ubicados estratégicamente para llegar a cubrir toda la superficie del Data Center.

- Funciona bien en aéreas cerradas.
- En la etapa del diseño se debe tener en cuenta el volumen del área y el equipamiento que va a ser protegido, el tamaño del área destinada a almacenar los tanques y el agente extintor que se va a elegir, ya que según el agente puede requerirse mayor o menor cantidad de tanques para extinguir el fuego en la misma superficie.
- Los tanques contienen gas comprimido a muy alta presión para ser expulsado en el momento justo. Por ello deberán estar ubicados en **zonas aisladas no transitadas**, donde las personas solo accedan allí para tareas de mantenimiento, a fin de evitar lesiones accidentales.
- El gas de alta presión pude alcanzar lugares de difícil acceso dentro del Data Center.

Los gases de inundación masiva que se utilizan para extinguir el fuego en los Data Centers se pueden clasificar en cinco grupos.

Dióxido de carbono (CO_2)

Se utiliza como medio de extinción desde hace aproximadamente 80 años. Es adecuado para extinguir instalaciones abiertas sin cerramiento de superficie debido a que es esencialmente más pesado que el aire, y cuando se activa el sistema extintor disminuye la visión debido a la formación de niebla al salir el gas.

Es tóxico a determinada concentración, pudiendo incluso causar la muerte. Por eso, en algunos países las normativas locales prohíben la utilización de los sistemas de CO_2 en áreas ocupadas; sin embargo, en otros países está permitida siempre que

el área a inundar pueda ser desalojada rápidamente mientras suenan las sirenas de evacuación.

- Tiene el mejor efecto extintor de todos los gases inertes. No conduce electricidad ni deja residuos luego de su aplicación.
- Se requiere el almacenamiento medio de extinción cerca de la zona del flujo aplicado.
- Tiene un bajo costo de recarga. Pero comparado con otros agentes demanda una cantidad de tubos superior para cubrir la misma superficie.

Gases Halones

Son los que están formados por los elementos de la Tabla Periódica de Elementos, que pertenecen al grupo de los halones combinados con otros como el Carbono (C). Los halones son: Flúor (F), Cloro (Cl), Bromo (Br), Yodo (I). Estos agentes tienen más de 100 años de antigüedad. Las primeras fórmulas eran peligrosas y hasta podían causar la muerte, por eso solo se usaban en lugares donde eran extremadamente necesarios como tanques o aviones militares.

Actualmente se usan sistemas de extinción con versiones de gas Halón más modernas desarrollados en la década de los sesenta, como el Halón 1301, 1211, 1202 2402, pero se descubrió que dañaban la capa de Ozono, razón por la cual, en 1994, la producción de este gas fue discontinuada. En su reemplazo hoy se utilizan otros tipos de gases.

El Flúor se perfiló como el gran sucesor de los gases basados en Halón por sus propiedades principales de:

- Volatilidad.
- Estabilidad.
- Baja toxicidad.
- Poder de extinción.

Gases Inertes

Son gases que tienen reacción escasa o nula con otros elementos. Junto con los gases nobles están ubicados en la última columna a la derecha de la Tabla Periódica de Elementos. El Argón (Ar) es un gas noble inerte, resultado de una tecnología que separa el Oxígeno y el Nitrógeno (N) del aire, en un proceso donde el aire es comprimido y enfriado para seguir con un procedimiento de licuado. Luego se extrae cada componente por su punto de ebullición. No establece ninguna composición ni combinación con ninguna otra sustancia.

No es tóxico y no deja residuos ni depósitos aceitosos, por lo que puede ser removido del espacio de exposición por ventilación. Pueden establecerse distancias grandes entre el grupo de tanques y la zona de la extinción.

Es fácilmente adaptable a una instalación previa de gas Halón. Su costo es moderado; es seguro para las personas, y no daña la capa de Ozono.

El Argón también se puede combinar con el Nitrógeno, ya que posee además excelentes propiedades extintoras y no es tóxico.

Existe gran variedad de nombres con los cuales se comercializa este gas en función de su combinación con otros: IG-01 (Ar 100%), IG-55 (Ar 50% + N_2 50%), IG-541 (Ar 40% + N_2 52% + CO_2 8%).

Halogenados HCFC

Son agentes gaseosos basados en Flúor y que se combinan con otros elementos para extinguir el fuego. Utilizan componentes que se basan en Hidroclorofluorocarbonos (HCFC), actualmente comercializados, pero que se estima que quedarán en desuso por su contenido de Cloro. Estos agentes son HCFC-124, HCFC-mezcla A, HCFC-22, HCFC-123. Todos con diferentes combinaciones de Hidrógeno (H), Cloro (Cl), Carbono (C), y Flúor (F).

Extinguen el fuego por la absorción y extracción del calor en las llamas. Cuando el gas se descompone y la temperatura de la llama es suficientemente baja, la reacción química de combustión en cadena se detiene. Es totalmente seguro para las aplicaciones en áreas ocupadas. No deja residuos ni durante la extinción del incendio ni después de una descarga accidental. Descarga en 10 segundos o menos a una distancia no mayor de 5 m. Se requiere que almacenamiento del agente esté muy cerca de la zona de aplicación. No conduce la electricidad ni es corrosivo.

Halogenados HFC

Son los compuestos basados en Hidrofluorocarbonos (HFC); son similares a los anteriores, pero no utilizan Cloro (Cl). Existen diversos tipos de agentes extintores, emplean los mismos elementos, pero en distintas proporciones, que son: HFC-227ea, HFC-125, HFC-23, HFC-236fa, FK-5-1-12. Esto se puede observar más claramente en la tabla comparativa.

En particular, el HFC-227ea es el gas más usado en el sector de IT para Data Centers. Es un medio químico de extinción que se puede utilizar a modo de sustituto del hidrocarbonato halogenado, ya que posee alta eficacia extintora por su concentración baja del medio de extinción. Está producido por la empresa DuPont bajo el nombre comercial FM-200®.

Extintores portátiles

Deben estar ubicados de forma estratégica, en una zona de fácil acceso, y tener su debida identificación. El HFC-236fa comercializado bajo el nombre FE-36 es el reemplazo ideal para el

Halón 1211.

Son efectivos porque son rápidos de instalar, económicos, portátiles, fáciles de usar, seguro para las personas, y no deja residuos ni conducen la electricidad.

Resumen y tabla comparativa[3]

Características	CO_2	Halones	Gases Inertes Argón, Nitrógeno o ambos	Halogenados o Halocarconados Químicos orgánicos combinados Cl, F, I HCFC	 HFC
Agente	Dióxido de Carbono	Halón 1301 1211 1202 2402	IG01 IG55 IG100 IG541	HCFC-124 (Clorotetrafluoroetano) HCFC-mezcla A HCFC-22 (Clorodifluorometano) HCFC-123	HFC-227ea (Heptafluoropropano) HFC-125 (Pentafluoropoprpano) HFC-23 (Trifluorometano) HFC-236fa (Hexafluoropropano) FK-5-1-12 (C6-fluorocetona)
Fórmula	CO_2	Hidrocarburos halogenados	Ar 100% Ar 50% +N_2 50% N_2 100% Ar 40%+ N_2 52% + CO_2 8%	$CHClFCF_3$ $CHCl_2CF_3$ o $CHClF_2$ o $CHClFCF_3$ $CHClF_2$ $C_2HCl_2F_3$	CF_3CHFCF_3 CHF_2CF_3 CHF_3 $CF_3CH_2CF_3$ $CF_3CF_2C(O)CF(CF_3)_2$
Nombre comercial	CO_2	Halón 1301 1211 1202 2402	Argonfire, Argotec Argonite, Proinert NN100 Inergen	FE-241 NAF S-III R-22 Halotron I	FM-200 o FE-227 FE-25 FE-13 FE-36 Novec 1230

[3]Las fórmulas y los nombres comerciales coinciden en orden con el nombre del agente.

Daña capa Ozono	No	Sí	No	No	No
Tiempo de descarga	60 seg.	10 seg.	60 seg.	10 seg.	10 seg.
Costo	Bajo	Bajo	Moderado	Moderado	Moderado
Deja Residuos	No	No	No	No	No
Conduce Electricidad	No	No	No	No	No
Seguro para descargas en áreas ocupadas	No	Sí	Sí	Sí	Sí
Cantidad de tubos requerida para extinguir el fuego (misma superficie)	Media	Baja	Alta	Baja	Baja

Sistemas de extinción de incendios líquidos

Los sistemas de extinción de incendios por líquidos utilizan agua para apagar el fuego. Puede resultar poco práctico para un Data Center, ya que probablemente dañe los equipos que se intentan proteger. Las cañerías que transportan el agua hacia los rociadores pueden ser de tres tipos:

- **Cañería mojada:** es la más común. La cañería está llena de agua, por lo que si se activan los rociadores, el agua comienza a salir inmediatamente. Existe riesgo de goteras y si las tuberías no están bien aisladas pueden incrementar la humedad en el Data Center.
- **Cañería seca:** los sistemas de cañerías estas cargados con aire comprimido y nitrógeno. En caso de incendio el agua empuja el aire y luego comienza a salir por los rociadores.
- **Pre acción:** utiliza cañería seca para evitar descargas de agua accidental, los sistemas están conectados a un tablero principal que funciona como doble control, ya que verifica por segunda vez si existe realmente un incendio o no. Es altamente recomendado para la instalación en Data Centers.

- **Sistemas de rociadores:** básicamente están diseñados para proteger la estructura del edificio, pero no son recomendados para Data Centers. Aunque pueden encontrarse en donde sean un requerimiento obligatorio de algún organismo regulador.

  - Los rociadores se activan entre 74ºC a 79ºC; sin embargo, ese rango puede modificarse.

- **Sistemas de rociadores finos (Mist):** este tipo de rociadores descargan el agua en forma de rocío muy fino, logrando apagar el fuego absorbiendo el calor. Además, el vapor que genera bloquea el oxígeno en el ambiente; de esta forma, ataca dos de los tres lados del triángulo de fuego que se mencionó anteriormente. Es muy eficaz, ya que utiliza poca cantidad de agua, y es muy efectivo apagando el fuego, porque su activación genera un impacto reducido. Debido a estas razones cada vez son más comunes estos tipos de sistemas.

El objetivo es lograr que el rociador de agua controle y extinga el incendio sólo en la zona donde se detecta el incendio, rociando la menor superficie posible, y así evitar que se ocasionen daños más grandes.

Normalmente, las tuberías y los rociadores no gotean a menos que estén físicamente dañadas, como podría ser en un depósito. La probabilidad de daños en las tuberías y en los rociadores es remota, pero no debe tampoco ser descuidada.

Si el Data Center está en un edificio que no requiere sistema de rociadores, la alternativa es instalar un sistema extintor de agente limpio extintor gaseoso.

En aplicaciones que no pueden permitirse ninguna interrupción del negocio, incluso pueden instalarse ambos tipos de sistemas. El sistema de agente gaseoso estaría diseñado para activarse primero, y el sistema de rociadores actuaría como segunda alternativa si el sistema de agente limpio fallara o no fuera capaz de apagar el incendio. El sistema de agente gaseoso usualmente no falla a menos que esté deficientemente instalado o que las puertas estuvieran abiertas por empleados desinformados. Tales cosas podrían suceder en la práctica, así que sería óptimo tener el sistema de rociadores allí como sistema redundante de extinción de fuego.

El área por debajo del piso elevado puede estar protegida por un sistema de rociadores, un sistema de dióxido de carbono, o un sistema de agente inerte. Si se

emplea un sistema de agente inerte en el piso técnico, entonces, la cobertura se extendería al área del subsuelo. Si el área por encima del piso tiene un sistema de rociadores, tendría sentido instalar un sistema de rociadores también en el subsuelo. Sin embargo, la distancia desde la loza hasta la parte inferior del piso puede no ser lo suficientemente alta para lograr el patrón de distribución necesario desde la descarga del rociador. Si este es el caso, se puede instalar en su lugar un sistema de agente gaseoso.

Si se selecciona un sistema de dióxido de carbono, se debería utilizar un sistema especial de descarga de baja velocidad, de modo que el dióxido de carbono no se eleve por encima de la altura de la rodilla, en la sala, y permita la evacuación.

Los procedimientos de recuperación y emergencia

Cada operación del área de IT debe contar con tres planes de contingencia que serán activados en caso de catástrofe:

- Plan de emergencia de incendios.
- Plan de control de daños.
- Plan de procedimientos de recuperación.

El más ignorado de estos planes es, con frecuencia, el plan de procedimientos de recuperación o de continuidad del negocio, que se desarrollará más adelante en el capítulo 10. Allí se delinearán las tareas que el personal debe emprender, incluyendo el transporte y la comunicación, aspectos críticos para la continuidad de las operaciones del negocio.

Análisis de daños

Al desarrollar un plan de recuperación deben producirse discusiones sobre los daños ocasionados por el agua, humo y calor. El daño por el calor es con frecuencia la razón por la que los artículos expuestos son irrecuperables. Los daños por agua y humo usualmente son menos severos, pero también son los que más se malinterpretan.

El humo de una sala de informática usualmente contiene cloruro y azufre que corroe los equipos. Siempre es necesario remover cualquier remanente de estos contaminantes. El humo puede ocasionar pequeños daños inmediatos, pero cuando se los deja desatendidos por un período prolongado, los derivados corrosivos de la combustión actúan con la humedad en el aire para comenzar el proceso de corrosión.

Luego de un incendio extinguido con agua, la preocupación inmediata es el nivel de humedad que el agua ha introducido en el aire, lo que brinda una indicación de la velocidad a la que ocurrirá la corrosión. Los planes deberían enfocarse en remover los equipos de la sala a un área climatizada de humedad controlada donde

se los pueda estabilizar, limpiar con solventes, y de ser necesario, recubrirlos con un aerosol especial para evitar la corrosión.

Entonces el daño sería analizado con mayor profundidad antes de tomar cualquier decisión sobre la disposición del equipo. Una práctica común es que las compañías con frecuencia venden el equipo con un daño potencial a un tercero en vez de arriesgarse a tener problemas futuros.

El daño ocasionado por el agua no es inmediato a menos que el equipo estuviera conectado a la red eléctrica cuando se mojó. En ese caso, son probables los cortos circuitos dañinos. Sin embargo, si el equipo no estaba conectado cuando se mojó, el daño se podría evitar o minimizar.

Por eso, es importante que en el Data Center exista un sistema de protección como el EPO[4] (Emergency Power OFF) de apagado de emergencia, que corta el suministro eléctrico en todo el Data Center, apagando los equipos de forma abrupta.

Solo se utiliza en casos de emergencia extrema

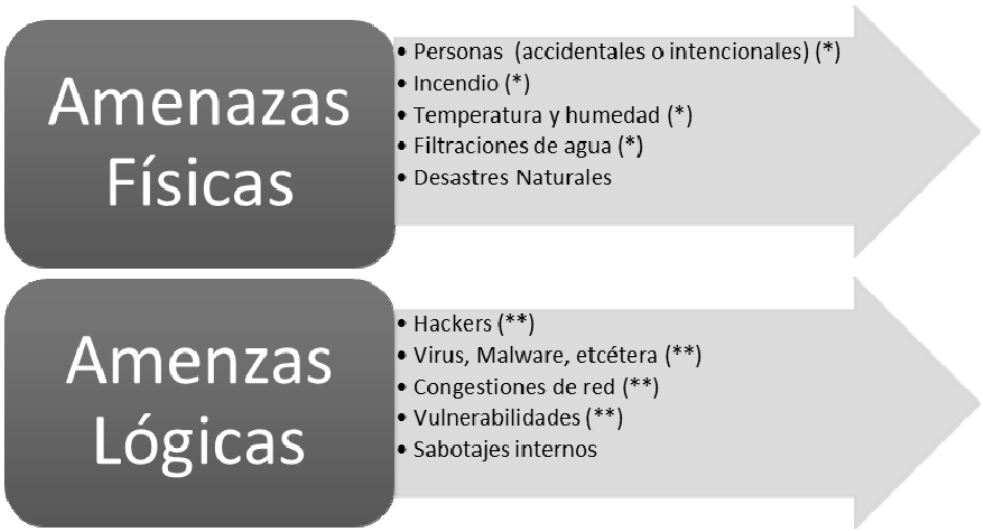
- Protección: evita descargas eléctricas a las personas que trabajen en la solución del incendio o inundación.
- Minimiza el daño en los equipos en caso de que se moje. Existe un costo elevado de activar esta función, razón por lo cual se debe emplear únicamente en casos de catástrofe.

Es fundamental que este botón se encuentre en una zona donde solo tenga acceso el personal autorizado, y cuente con un sistema que prevenga el accionar accidental como una cubierta plástica protectora. Además la restauración de la energía no se produce de manera automática desde el mismo botón, sino que deben activarse, manualmente los sistemas desde el tablero principal.

Hay que tener en cuenta que el 43% de las empresas cuyos Data Centers se incendian nunca más vuelven a abrir sus puertas, y el 29% quiebra en menos de 3 años.

[4]También se puede activar en caso de inundación.

Resumen de los distintos tipos de amenazas dentro de un Data Center



(*) Pueden ser prevenidas o mitigadas con sensores y monitoreo.

(**) Pueden ser prevenidas con herramientas de software y monitoreo.

Diseño de red

7

"Los hombres construimos demasiados muros y no suficientes puentes".

-- Isaac Newton (1642-1727) Científico, filósofo, químico y matemático inglés

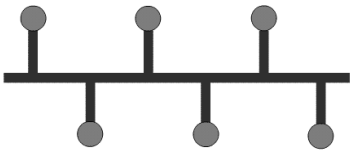
Una red de datos se establece cuando se necesita que dos dispositivos ubicados remotamente intercambien información a través de un medio que es el material físico a través del cual viajan los datos. Dichos medios pueden ser:

- **Cables telefónicos:** la información se transporta como impulsos eléctricos.
- **Cables UTP**: la información se transporta como impulsos eléctricos.
- **Cables STP:** la información se transporta como impulsos eléctricos.
- **Cable coaxial**: la información se transporta como impulsos eléctricos.
- **Fibra óptica**: la información se transporta como impulsos de luz.
- **Transmisión inalámbrica**: la información se transporta como impulsos de radiofrecuencia.

Topologías

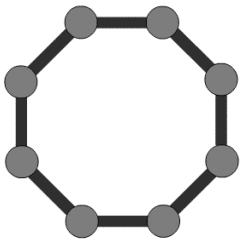
Entendemos por topología de red a los distintos modelos lógicos y físicos que componen una red de datos de acuerdo con un diseño y según cómo es la interconexión entre los nodos o elementos que la conforman.

Bus



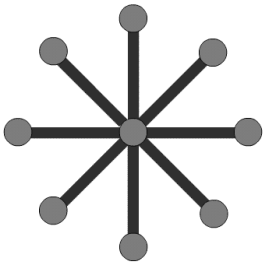
La topología de Bus tiene todos sus nodos conectados directamente a un enlace compartido, y no tiene ninguna otra conexión entre nodos, es decir, que cada nodo está conectado a un medio único común. En esta topología, los dispositivos clave son aquellos que permiten que el nodo o *host* se conecte al medio. Una de las ventajas de esta topología es que todos los *hosts* están conectados entre sí, y de ese modo, se pueden comunicar directamente. Eso la convierte en la topología más popular para los cableados de red. Una desventaja de esta topología es que la ruptura del cable troncal hace que los *hosts* queden desconectados.

Permite que todos los dispositivos de red puedan ver todas las señales de los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones de paquetes de datos, dado que solo un nodo puede transmitir a la vez por el medio.



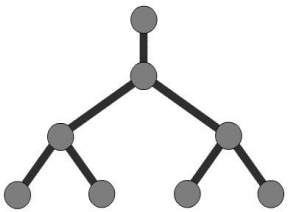
Anillo

Formada por un anillo cerrado unido por nodos y enlaces donde cada *host* está acoplado con solo dos nodos adyacentes conectados directamente entre sí por medio de cables. Para que la información circule, cada estación debe transferir la información a la estación adyacente.



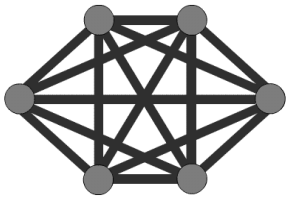
Estrella

Se caracteriza por tener un nodo central desde el que se irradian todos los enlaces hacia los demás nodos sin permitir otros enlaces. La ventaja principal es que posibilita que todos los demás nodos se comuniquen entre sí de manera conveniente. La desventaja principal es que si el nodo central falla, toda la red queda desconectada. Según el tipo de dispositivo de red que se usa, en el centro de la red en estrella, las colisiones de paquetes de datos pueden representar un problema importante, porque toda la conmutación depende de un solo dispositivo.



Árbol o jerárquico

Es similar a la topología en estrella con una distribución jerárquica ordenada por niveles (no posee un nodo central). En cambio, tiene un nodo de enlace troncal desde el que se ramifican los demás nodos. Si falla un nodo "padre" todos los "hijos" de esa rama quedarán desconectados de la red.



Malla completa

Cada nodo se enlaza directamente con los demás nodos. Este tipo de cableado tiene ventajas y desventajas muy específicas. La ventaja fundamental es que como cada nodo se conecta físicamente a los demás nodos creando una conexión redundante, si algún enlace deja de funcionar, la información puede circular a través de cualquier cantidad de enlaces hasta llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red. La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, porque de lo contrario la cantidad de medios necesarios para los enlaces y de conexiones con ellos se torna abrumadora, haciéndola extremadamente costosa y compleja.

Cableado estructurado

El Sistema de Cableado Estructurado SCS es una metodología basada en estándares de diseño que sirven para instalar una red de cables durable que integra los medios de transmisión de voz y datos, suministrando un desempeño predefinido y flexible para acompañar el crecimiento futuro de las necesidades del negocio.

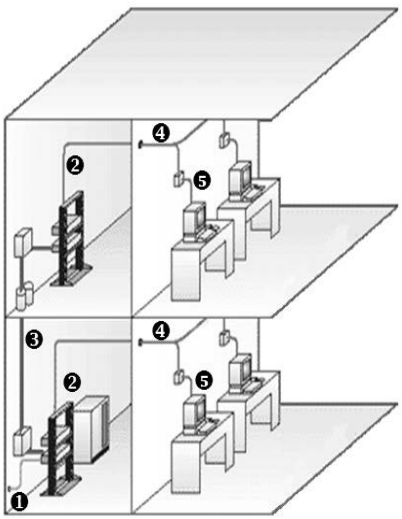
Mediante la adopción bilateral de normas por parte de fabricantes de cables y de equipos electrónicos, se hace posible la implementación de un cableado flexible y ágil como la norma EIA[1]/TIA[2]-568 o la norma ISO[3]/IEC[4] 24764, publicada en 2010. Tanto la EIA como la TIA son entidades acreditadas por el Instituto Nacional Americano de Normalización ANSI para desarrollar estándares voluntarios para la industria de las telecomunicaciones. Además también existe otra organización de

[1]Asociación de Industrias de Electrónica (Electronic Industries Alliance).
[2]Asociación de la Industria de Telecomunicaciones (Telecommunications Industry Association).
[3]ISO corresponde a las siglas de International Standards Organization (Organización de Normas Internacionales).
[4]International Electrotechnical Commission (Comisión Electrotécnica Internacional).

estandarización creada en 1973 por el Comité Europeo para la Estandarización Electrotécnica (CENELEC), utilizado principalmente en Europa, y publicado bajo la norma EN 50174, del 2009, como continuación de la norma original EN 50173, del 2007.

Este tipo de cableado es el que se utilizan cuando se crean las redes LAN (Red de área local, Local Area Network).

Así sería un esquema básico de cableado estructurado



1. Instalación de entrada es el punto donde ingresan las conexiones desde el exterior al edificio.
2. Sala local que almacena en un espacio centralizado los equipos de telecomunicaciones o red (generalmente son Racks pequeños). Suele haber al menos uno por cada piso.
3. El cableado troncal o *backbone* proporciona interconexión para los servicios de red y telefonía. Habitualmente son de fibra óptica o cables UTP de alta velocidad, por lo menos 1/10 GB, dentro de un edificio o también se usan entre edificios próximos. La distancia máxima dependerá del medio seleccionado.
4. El cableado horizontal es el medio físico que conecta la salida de un Rack del piso para la distribución horizontal o final. La distancia máxima permitida por el estándar son 90 m.
5. Proporciona una conectividad flexible para extender los diversos servicios a los usuarios final, creando una toma o salida de telecomunicaciones con conectores compatibles para los servicios red y telefonía (conectores RJ45 y/o RJ11) a fin de proporcionar conectividad bajo el código de colores de cableado T568A o T568B (recomendado). La distancia máxima permitida por el estándar son 5 m.

La norma TIA/EIA-568B del 2001 reemplazó a la 568A publicada en 1995. Es una de las principales normativas utilizadas para el cableado de telecomunicaciones. El Estándar de Cableado de Telecomunicaciones para Edificios Comerciales (Comercial Building Telecommunications Cabling Standard)es aplicable a los edificios comerciales y a los ambientes de oficina, y tiene como propósito establecer un sistema de cableado genérico para soportar ambientes con múltiples productos y procedentes de múltiples compañías vendedoras en donde se definen los criterios técnicos y de desempeño.

El planeamiento recomendado del cableado estructurado en edificios debe considerar una vida útil de 10 a 15 años. Por ese motivo siempre conviene seleccionar las últimas tecnologías disponibles, ya que en todo ese tiempo, la amortización de la inversión inicial del cableado será solo del 3% del total gastado en todo ese período en equipos, mantenimiento, costos operativos, etcétera.

La normativa define los requerimientos de los componentes necesarios para cada instalación, las distancias que tendrán los cableados, las configuraciones de las salidas o conectores y la topología obligatoria para los sistemas. En el área de trabajo el objetivo es llevar las telecomunicaciones desde la toma o conector, y a su vez, desde ese conector hasta donde termine el sistema de cableado horizontal, que será el Rack o punto final del cableado horizontal.

Características de los cables

Los cables son medios físicos que cuentan con ciertas particularidades técnicas, importantes de conocer al momento de seleccionar los materiales necesarios para realizar una obra de cableado estructurado. Dentro de los Data Centers, los más comunes son los UTP, básicamente conformados por cuatro pares de cables de cobre, cada uno de distinto recubrimiento plástico de color. Esto será se detallado más adelante, en este capítulo.

Características de los cables

- **Atenuación:** es un parámetro importante a tener en cuenta en un cable de datos. Se expresa en dB (decibeles) por cada 100 m (dB/m) y representa con un valor negativo la pérdida de amplitud de la señal a lo largo de la longitud del cable. A menor valor (menos negativo), mejor será el cable. Las causas por las que varía la atenuación pueden ser diversas, por ejemplo: características eléctricas del cable, deformación de los materiales o fallas en el cruzamiento de los cables, pérdidas de inserción debido a malas terminaciones, cambios en la impedancia, frecuencia (las mayores pérdidas se dan a mayor frecuencia de operación), temperatura, longitud del enlace, humedad, envejecimiento del material, etcétera.
- **Impedancia característica:** es la oposición del material del cable al flujo de la corriente, delimitará la *performance* de la red, y es medida en Ohms.
- **Longitud:** Se define como la distancia física del cable entre los extremos conectores finales.
- **Efecto pelicular o skin:** es un fenómeno eléctrico físico que ocurre en la corriente alterna donde la densidad de electrones que se mueven por el conductor tiende a circular por la periferia de la sección del cable a medida que aumenta la frecuencia. Por el contrario, en la corriente continua, la densidad de electrones circulante es similar en toda la sección el cable.
- **Crosstalk**: es el ruido eléctrico externo inducido por los cables u otros elementos externos: bobinas, motores, lámparas, tubos de iluminación, etcéte-

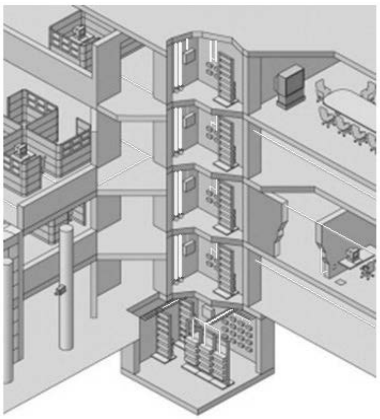
ra. También se lo conoce con el término de **diafonía,** y la relación se expresa en dB. Si tomamos p1 como potencia de la señal perturbadora y p2 como potencia de la señal perturbada, la atenuación de diafonía será:

$$A(dB) = 10log\frac{p1}{p2}\ (dB)$$

- **NEXT (Near end crosstalk):** es el ruido introducido por un par a un par receptor vecino por el acoplamiento, que causará señales indeseables. El ejemplo clásico que todos hemos experimentado alguna vez es el del teléfono ligado, donde escuchamos otra conversación o una radio en la línea. Para verificar el cable, el probador transmite una señal en un par del enlace, y mide la magnitud de la señal que se generó en otro par (el par perturbado), ese es el resultado del *crosstalk*. Según la categoría del cable, la frecuencia de la transmisión y la longitud, el límite permitido de *crosstalk* puede variar, por eso es importante conocer las especificaciones del fabricante del cable. No siempre los problemas de *crosstalk* están en el cable, muchas veces las malas terminaciones en los extremos pueden ser la causa por la cual la señal esté por debajo del umbral de aceptación de la norma TIA. Según la frecuencia de transmisión, los límites de decibeles de aceptación pueden variar.
- **FEXT (Far End Crosstalk):** ruido introducido por un agente perturbador en un extremo (cercano) sobre el receptor del otro extremo (lejano). Debe ser medido en ambos extremos del cable.
- **ELFEXT (Equal Level FEXT):** se obtiene restando a FEXT la atenuación del par perturbador como medida de normalización con respecto a la longitud total.
- **Retardo (Delay):** el retardo de propagación es el tiempo que insume una señal en viajar desde un extremo hasta el otro de un enlace. Se mide en ns (nano segundos), y depende sutilmente de la frecuencia. Cada estándar define los retardos aceptables sobre la base de la frecuencia para cada categoría. Por ejemplo, para los cables UTP Cat. 5, el valor aceptado es 5,7ns/m (nano segundos por metro); y para un cable de 100 m, el máximo es 1 μseg. (microsegundo).
- **Retardo Diferencial (Delay Skew):** es la diferencia de retardo entre dos pares de cables trenzados agrupados en cuatro pares de cables. La diferencia de retardos es importante en sistemas que transmiten y reciben simultáneamente por los cuatro pares del cable UTP. Por ejemplo, en aplicaciones Gigabit Ethernet es vital, ya que el receptor debe reconstruir la señal original sobre la base de la recepción de los cuatro pares de señales independientes. Si estas señales llegasen a destiempo, no será posible reconstruir la señal original debidamente. Por ejemplo, para un enlace de 100 m, el retardo diferencial debe ser inferior a 50 nanosegundos, y preferentemente menor a 35 nanosegundos.

- **Pérdida de retorno, (SRL, Structural Return Lost):** es una medida de uniformidad de la impedancia del cable. Es una característica de fabricación del cable y se expresa en dB. A mayor valor de SRL, mejor será el cable. Tiene más preponderancia en cables de Cat. 5e y 6.
- **Power Sum (PSNEXT):** mide los efectos de diafonía de tres pares de transmisores en relación con el cuarto par.

Red troncal o backbone: puntos de distribución



El *backbone* o red troncal es un medio de conectividad primario, de ancho de banda amplio para ser usado como sistema de distribución troncal o subsistema vertical, en una instalación de red de área local que sigue la normativa de cableado estructurado.

Para tener una red robusta y eficiente, el *backbone* debe ser una red de alta velocidad, con lo cual evitará los cuellos de botella, puesto que todas las comunicaciones pasarán por allí. En general, las empresas utilizan fibra óptica o cables UTP Cat. 6 o 6A para configurar redes de GB, ya que el *backbone* equivale análogamente al **bus** dentro del *motherboard*.

Los aspectos de diseño de la sala de equipamiento se describen en el estándar TIA/EIA-569-A, también llamado por el nombre de Estándar para las Canalizaciones y Espacios de los Edificios Comerciales (Comercial Building Standard for Telecommunications Pathways and Spaces), y define las formas y los medios de la conducción del cableado en las distintas etapas de comunicación:

Canalizaciones horizontales o bandejas portacables: son estructuras rígidas metálicas utilizadas para transportar y proteger los cables, los cuales están colocados de forma accesible recta o curva, en el suelo o sobre el cielorraso.

En el cableado que está sobre las bandejas no debe haber empalmes ni uniones de cables.

Rack de telecomunicaciones: se utilizan cuando el área de cobertura excede los 1 000$m^{2,}$ y cuando la distancia horizontal es mayor a 90 m, teniendo un Rack por piso como mínimo. Adicionalmente, podrán contener los de telecomunicaciones, como por ejemplo *switchs*.

Estaciones de trabajo: el área mínima para una estación de trabajo debe ser de 10m^2 de forma típica. Es conveniente tener una salida en forma de caja o placa, ubicada contra la pared a la altura del escritorio para facilitar la conexión en lugar

de un conector de telecomunicaciones individual. Es deseable que los conectores individuales no estén en el piso, ya que tienden a ser dañados frecuentemente por golpes.

Instalaciones de ingreso: el espacio de ingreso deberá contar necesariamente con un Rack, ubicado lo más cerca posible del punto de la entrada, y desde allí se conectará con el resto de los Racks del edificio. En las instalaciones de ingreso, se utiliza entubado metálico o de plástico rígido. Se deberá tener en cuenta el ángulo máximo de doblez o curvatura del medio físico para evitar pérdida de señal.

Para edificios viejos donde no se han diseñado los correspondientes ductos para el cableado, un buen lugar por donde pasar los cables de fibra óptica son las montantes o ductos de los elevadores, ya que los cables eléctricos no afectan a las señales que pasan por la fibra óptica. Sin embargo, no se deben utilizar los ductos de ventilación, ya que los agujeros que se deben realizar para pasar los cables pueden causar pérdidas de aire, causando un desperdicio de los sistemas de enfriamiento.

Cables de red: UTP

Actualmente los cables UTP, par trenzado no blindado (Unshielded TwistedPair) son los más usados en las redes Ethernet dentro del Data Center.

El cableado estructurado para redes de computadores tiene dos tipos de normas, la EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B), que reemplazó en el 2001 a la norma 568A. Básicamente, se diferencian por el orden de los colores de los pares para armado de los conectores RJ45. Si bien el uso de cualquiera de las dos normas es indiferente, actualmente se utiliza la T568B para el cableado recto, aunque la T568A es la más popular en las instalaciones ya vigentes. La norma también define la frecuencia de transmisión.

El cable UTP está compuesto por cuatro pares de hilos o filamentos de cobre, recubiertos en plástico de distintos colores, usados en redes de datos. Los colores deben ser respetados al momento de la instalación, porque el orden de instalación de cada hilo dentro del conector debe coincidir con el color en el terminal del cable. Cada hilo de cobre se encuentra aislado de los demás, y ellos se encuentran entrecruzados de forma continua de a pares, formando cuatro grupos de pares de cables cruzados.

Según la velocidad de transmisión, se presentan cambios en el uso de los pares, que si bien para todos los cables UTP son cuatro, algunos estándares no los usan a todos. Por ejemplo: el primer estándar 10BaseT (definido en 1990, por

IEEE5 802.3i) utilizaba dos pares y permitía velocidades de hasta 10 Mbps (Cat. 3). Luego en 1995, surgió la norma 100BaseTX que también utilizaba dos pares, pero con filamento de mejor calidad (Cat. 5), permitiendo velocidades de hasta 100 Mbps.

Más adelante, hacia 1998 se aprobó el estándar 1000BaseT, IEEE 802.3ab que sí utilizaba los cuatro pares de cables, permitiendo velocidades de hasta 1Gbps, con cables Cat. 5e.

Categoría Obtenida	Año publicación	Cantidad pares usados	Cat. Cable mínima	Velocidad Máx. de Transferencia
10BaseT	1990	2	3	10 Mbps
100BaseTX	1995	2	5	100 Mbps
1000BaseT	1998	4	5e	1 Gbps
1GBaseT	2001	4	6	1 Gbps
10GBaseT	2006	4	6a	10 a 55 Gbps

Con la búsqueda constante de mayores velocidades surgieron dos estándares para redes de alta velocidad, en 2001, 1GBaseT; y en el 2006, se lanzó un nuevo estándar 10GBaseT, permitiendo de 1GBps y hasta 10GBps (en distancias cortas, con cables de Cat. 6 y Cat. 6A[6]), ambos utilizan los cuatro pares de cables.

Es importante que el entrecruzamiento de los hilos se mantenga equidistante, siempre menor a los 13 mm a lo largo de todo el cable, ya que tiene una función muy importante que consiste en el efecto de cancelación de las interferencias electromagnéticas generadas por los electrones al pasar por el cable. Por lo general, el rango térmico de funcionamiento correcto de este tipo de cables se extiende desde los -10°C hasta los 60°C. Aunque dicha condición siempre debe ser verificada con las especificaciones del fabricante.

- Ventajas
  - Fácil instalación.
  - Económico.

[5]Institute of Electrical and Electronics Engineers es una asociación mundial creada en 1884, dedicada a establecer estándares en las distintas ramas de la Ingeniería (Electrónica, Informática, Comunicaciones, etcétera).

[6]La letra *A* proviene de la palabra "aumentada". Por eso también son denominados cables Cat. 6 Aumentada.

- Tamaño reducido.

- Desventajas
  - Sensible al ruido eléctrico y a la interferencia de otros equipos.
  - Lentos en las primeras categorías, pero ya están prácticamente en desuso.

En la norma 10BaseT y 100BaseTX, la señal es transmitida en un solo sentido por el par. En cambio, en la norma 1000BaseT, las señales viajan en ambas direcciones por el par. Por eso se debe analizar el FEXT, a mayor longitud del cable, más relevante se hace el valor.

Tabla comparativa de las distintas categorías de cables UTP

Categoría Obtenida	Año publicación	Ancho de banda MHz	Atenuación (dB)	Velocidad Máx. de Transferencia	Distancias Máx. sin repetidores	Uso
Cat. 3	1990	16 MHz	22	10 Mbps.	100 Mts.	Obsoleto
Cat. 4	1993	20 MHz	21	16 Mbps	100 Mts.	Obsoleto
Cat. 5	1994	100 MHz	22	100 Mbps.	100 Mts.	Próximo a discontinuarse
Cat. 5e	1998	100 MHz	22	165 Mbps.	100 Mts.	Cableado LAN
Cat. 6	2001	250 MHz	19,8	1000 Mbps.	100 Mts.	Cableado LAN
Cat. 6a	2008	250/500 MHz	36/21	1/10 Gigabits (según la distancia)	100/55 Mts.	Cableado LAN (alta velocidad)
Cat. 7* o Clase F	2011	600 MHz	20,8	10 Gigabits	100 Mts.	Transmisión video alta calidad
Cat. 7a* Clase F	2011	1200 MHz	21	10/40/100 Gigabits (según la distancia)	100/50/15 Mts.	Transmisión video alta calidad

Cat. 8*	Propuesta	1200 MHz	En etapa de prueba	En etapa de prueba	Max 100 Mts.	En etapa de prueba

* Si bien los cables son similares y compatibles con las versiones anteriores, en este caso los pares son blindados (ver sección STP). Hay un cambio muy importante en los conectores terminales, definidos en la norma IEC 61076-3-104 o también conocidos por el nombre comercial TERA, bautizados así por la empresa Siemon que fue la primera en aprobar el estándar con su producto. Ellos son distintos de los conectores RJ45. Estos estándares no están aprobados aún por TIA, aunque quizás en un futuro cercano sí lo sean; pero están efectivamente aprobados como estándar Clase F (ISO/IEC), que son análogos a los estándares de TIA Cat. 7 con Clase F, Cat. 6 con Clase E, Cat. 5 con Clase D, y así sucesivamente.

Para la norma 10GBaseT existe un estándar TSB-155 equivalente al ISO/IEC 24750, publicado en el 2007, y que define los parámetros del cableado y las condiciones que debe cumplir para estar certificado.

Aclaración ISO/IEC contra ANSI/TIA: ambos son organismos internacionales de estandarización reconocidos, pero la composición interna de sus miembros es distinta, lo que influye en los intereses particulares de cada uno.

ISO / IEC	ANSI / TIA
• Integrado por representantes de naciones, un voto por país. • Acuerdo OMC[7] para evitar barreras técnicas al comercio. • Acuerdos de reconocimiento mutuo. • También participan los fabricantes.	• Integrado por empresas privadas, un voto por empresa. • Respaldar los intereses tecnológicos y comerciales de sus asociados.

El principal problema de los estándares es que al intervenir tantos participantes, el proceso de aprobación es realmente largo y complejo, pudiendo tomar varios años, pero los requerimientos del mercado demandan productos que brinden mayores velocidades permanentemente, y las empresas privadas invierten mucho en investigación para lograrlo, adelantándose a los estándares. Por eso, a veces, resulta difícil seleccionar una tecnología de punta que quizás después no resulte aprobada por los organismos que certifican los estándares. También está la disyuntiva de tener que elegir una tecnología de cableado proyectado el crecimiento a diez

[7] Organización Mundial del Comercio.

años, pero con un estándar aprobado cinco o siete años atrás, que quizás ya es obsoleto. **Por esa razón, cuando se analiza la selección de un estándar de cableado estructurado es importante tener en cuenta su fecha de publicación**.

Hoy, durante el 2014, si hay que planificar un cableado, no conviene elegir un cable de categoría inferior a la que ofrece la Cat. 6A.

Prácticas de instalación del cableado

- Retirar el aislamiento del cable lo suficiente como para poder realizar la terminación, y que se mantengan los pares trenzados lo más cerca posible del punto de culminación física. La distancia máxima destrenzada del par en la conexión no debe ser mayor que 13 mm.
  - Mantener un radio de curva máximo de cuatro veces el diámetro del cable.
  - Utilizar abrazaderas o precintos con juego sin ejercer demasiada presión sobre el manojo de cables, ya que podrían dañarlos. Los precintos deben colocarse en intervalos regulares para mantener el orden así como bandejas para transportarlos, tableros de gestión y precintos.
  - En el momento de desenrollar el cable de la bovina se debe evitar la excesiva tracción del cable.
  - No torcer demasiado el cable, esto puede provocar el rompimiento de la capa protectora.

Los fabricantes de cables UTP establecen una distancia mínima de recorrido de cable, conocida como la *Regla de los 15 m,* para que según el material de construcción se pueda cumplir con las normas de certificación para todos los parámetros de calidad de señal mencionados, ya que si el cable tiene una distancia menor, no puede cumplir con algunos indicadores de certificación. Quizás no parezca relevante, pero para la conexión entre Racks, 15 m es demasiado cable, que terminará enroscado sobre la bandeja portacables o por debajo del piso. Cuando la cantidad de cables es alta, genera un exceso de cables que resulta difícil de manejar, obstruyendo el flujo de aire por debajo del piso o generando un exceso de peso en la bandeja superior.

Gracias a la evolución tecnológica de los fabricantes actualmente existen proveedores que ofrecen cables de menor diámetro que cumplen con las normas de certificación, y requieren una distancia mínima menor a 3 m para cumplir con las normas de certificación, lo cual reduce significativamente el exceso de cables entre Racks.

Cables de red: STP

Son cables de par trenzado blindado, (Shielded Twisted Pair), idénticos a los cables UTP, pero con la única diferencia de que tienen una doble protección: cada par trenzado tiene un recubrimiento metálico laminado muy fino y maya entrelazada protectora (similar a la del cable coaxial) que envuelve a los cuatro pares de cables, y le proporciona mayor calidad comparado con el UTP. Es más rígido y tiene mayor resistencia a la interferencia electromagnética externa, por lo que permite mayores velocidades de transmisión.

Este tipo de cables requieren conectores RJ49. Son básicamente similares a los RJ45, pero se caracterizan por estar blindados.

Pese a estas ventajas, este tipo de cable es muy poco usado, porque su costo es elevado comparado con el UTP, y no brinda suficientes beneficios que justifiquen la diferencia de precio para redes LAN de cableado horizontal. Pero, si se quieren alcanzar altas velocidades, los cables Cat. 7 y Cat. 7A son los que permiten tazas de transferencias superiores a los 10 Gbps.

A diferencia del cableado UTP, las instalaciones con cableados STP, como por ejemplo E_A y F_A requieren una instalación a tierra para los cables de datos, que se conecta a la malla metálica de los cables blindados.

Cables de telefonía

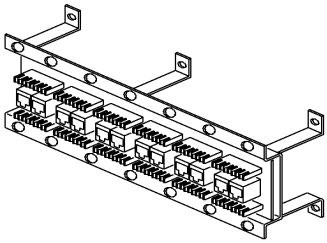
Son cables muy finos conformados por un par de filamentos únicos de cobre trenzados, también para evitar la interferencia electromagnética, recubiertos por plástico; por lo general, uno es de color blanco y el otro, azul, aunque también existen muchas otras combinaciones de colores; también, poseen otro recubrimiento plástico protector exterior. Son utilizados para el cableado horizontal final en las instalaciones hogareñas o edilicias.

Para las instalaciones de cableado estructurado se puede usar todo el tendido con cables UTP (previendo la instalación futura de VOIP[8]), y solo hacer las conexiones a las terminales de telefonía comunes RJ11.

[8]Protocolo de comunicación sobre redes de datos, también conocido como Voz sobre IP, ampliamente adoptado por las empresas por su bajo costo de llamada.

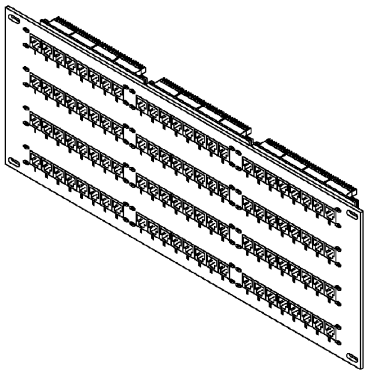
Elementos terminales

Patch panel o patchera



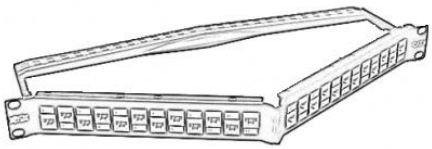
El *Patchpanel* es un elemento de red pasivo que forma parte del cableado estructurado, y es el encargado de recibir todas las terminaciones de cables. Se utiliza como medio organizador de las conexiones de la red en la cual se encuentran una cantidad variable de puertos de red, normalmente 24 o 48 en cada panel.

Aquí se muestra la vista trasera, donde se colocarán los cables en la secuencia que indica la norma a utilizarse.



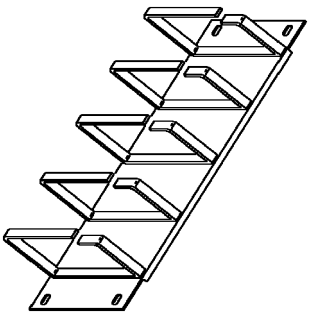
Dichos paneles se colocan en los Racks, y cada uno de estos puertos podrá ser conectado con un *switch*, router o cualquier dispositivo de telecomunicaciones situado dentro del Rack. Esta conexión se realiza mediante *patchcords*. Este sistema de *patch panel* y *patchcords* facilita enormemente la administración de las redes, ya que permite cambios en una forma muy sencilla y rápida.

También se ilustra la imagen frontal.



Por otra parte, algunos fabricantes ofrecen paneles en forma angular o *V*, que poseen las mismas características que los anteriores, pero con la ventaja de no requerir organizadores horizontales para mantener ordenado el cableado, ya que gracias a su forma, los cables se orientan hacia los organizadores verticales de manera directa.

Organizador de cables



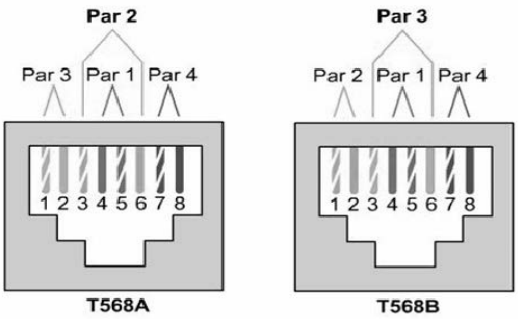
Adicionalmente, para mantener los cables prolijos, se utilizar los organizadores de cables horizontales o verticales, que consisten en elementos metálicos con cierta flexibilidad que permite maniobrabilidad, tienen la forma de *U* abierta y se colocan en los laterales de los Racks, de manera que los cables que ingresan desde el piso o el techo sean conducidos a través de dichos elementos; luego cada cable irá al *Patchpanel* correspondiente, además debe estar correctamente rotulado. Más adelante en este capítulo profundizaremos sobre este tema.

Conectores cables cobre

En las terminales de los cables de cobre, en el cableado estructurado, se utilizan dos tipos de conectores, también conocidos como Jack's, el RJ45 y el RJ11:

RJ45

Consiste en un conector plástico con una traba que impide desconexiones accidentales; cuenta con ocho terminales metálicas o también llamados pines donde se colocará uno a uno los ocho filamentos, ya sean de UTP o STP. Esta instalación es independiente de la categoría del cable con la cual estemos trabajando.



Para la norma **T568A** la secuencia de los colores es de 1 a 8: Blanco-Verde, Verde, Blanco-Naranja, Azul*, Blanco-Azul*, Naranja, Blanco-Marrón*, Marrón*.

Para la norma **T568B** el orden de los colores es de 1 a 8: Blanco-Naranja, Naranja, Blanco-Verde, Azul*, Blanco-Azul*, Verde, Blanco Marrón*, Marrón*.

*Esos cables no transportan señales eléctricas en 10BaseT y 100BaseTX.

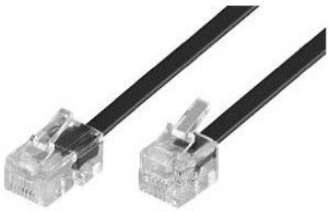
Para ambas normas dicha secuencia de colores deberá respetarse en ambos extremos terminales del cableado.

Cable cruzado: se llama así al cable que se usa para conectar dos dispositivos de manera directa, uno a uno. Para ello se mantiene el orden original en uno de los extremos y lo único que cambia es el orden de los cables en el otro extremo.

Para la norma T568A: un extremo terminal se instala con la secuencia de colores descrita en la norma, y en el otro extremo cambia el orden de los pines del 1 al 8. Deberán ir en la siguiente secuencia: Blanco-Naranja, Naranja, Blanco-Verde, Blanco-Marrón, Marrón, Verde, Azul, Blanco-Azul.

Para la norma T568B: ídem al caso anterior, pero el orden de los colores en el otro extremo es distinto, los pines del 1 al 8 deberán ir en la siguiente secuencia: Blanco-Verde, Verde, Blanco-Naranja, Blanco-Marrón, Marrón, Naranja, Azul, Blanco-Azul.

RJ11

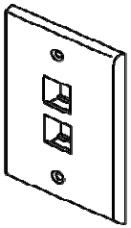


Es un conector similar al RJ45, la única diferencia es que es de menor tamaño, y se conectan hasta cuatro hilos en lugar de ocho. Se utiliza para cableados telefónicos.

En la fotografía se ilustran ambos terminales. A la izquierda, se observa el conector RJ45 (8 pines), y a la de la derecha, el RJ11 (4 pines). Ambas fichas vienen con una traba plástica superior que impide desconexiones accidentales.

Patchcords

Son los cables terminales que conectan la salida del extremo final del cableado horizontal con los equipos de los usuarios finales (servidores, computadoras personales, *notebooks*, teléfonos IP, etcétera). Generalmente son de Cat. 5 o superior, y se pueden conseguir en varios colores; las medidas van desde los 10 cm hasta los 6 m, medidas superiores pueden ser afectadas por la atenuación. Cuando se entregan los cables a los usuarios finales se les debe instruir para que no los doblen demasiado, porque sino podrían sufrir daños internos.



Fichas o rosetas de escritorio

Las llamadas rosetas o fichas terminales pertenecen al extremo final del cableado horizontal. Se colocan en la pared donde está la terminación de este cableado. Por lo general, se instalan de a uno o de a dos pares por cada puesto, según las nece-

sidades. Uno se utiliza para el cableado de la red de datos y el otro para la red de telefonía.

Cables de fibra óptica

Es un medio de comunicaciones que utiliza fibras de plástico o de vidrio recubiertas por plástico para guiar los impulsos de luz emitidas por Láser o LED (Light-Emitting Diode), que es el estándar para las transmisiones desde el origen hasta el destino.

Los bits se codifican en la fibra óptica como impulsos de luz que viajan a través de ella. Gracias a su velocidad de transferencia, y a su baja atenuación ha revolucionado el mundo de las comunicaciones, permitiendo operar en el rango de Gbps.

La luz que viaja por la fibra está en banda de los infrarrojos; por lo tanto, es invisible al ojo humano. El haz de luz se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, acorde con la *Ley de Snell*[9]. Las ventajas de la fibra óptica residen en su pequeño tamaño que varía entre 125 a 380 micrones, la resistencia total que ofrece a interferencias electromagnéticas, es decir, que se pueden usar los mismos ductos de tendidos eléctricos de alta tensión sin afectar la señal que viaja por la fibra ni tampoco es afectada por los cambios de temperatura, logrando ofrecer distancias de transmisión más largas que otros medios por su baja atenuación (0.2 dB/km), y pudiendo cubrir fácilmente trechos desde los 80 hasta los 400 km.

Sus desventajas son los acopladores y conectores que son costosos y muy complejos, que además si no se conectan con suma precisión existe la posibilidad de sufrir una gran pérdida de señal.

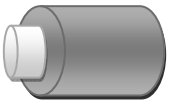
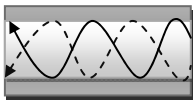
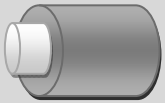
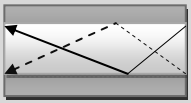
Por sus características físicas, la fibra es un medio flexible pero frágil; por eso, es importante tener en cuenta las especificaciones del fabricante en cuando al ángulo máximo de curvatura en las zonas de ingreso al Rack o al edificio, ya que un exceso podría devenir en un corte o una pérdida de señal importante. Una disminución en la potencia de la luz debido a la atenuación deviene directamente en una reducción del ancho de banda.

La fibra óptica está compuesta por dos capas, una central llamada núcleo (*core*) y una periférica de recubrimiento (*clad)*. Ambas campas tienen un índice de refracción distinto. La capa central o núcleo tiene un índice de refracción mayor al

[9]Fórmula utilizada para calcular el ángulo de refracción de luz con distinto índice de refracción, elaborada por el matemático holandés Willebrord Snel Van Royen (1580-1626).

índice de refracción del recubrimiento periférico, haciendo que la luz solo se propague a través del núcleo y quede contenido sólo en él.

Existen tres tipos de fibra óptica

Tipo de Fibra Óptica	Variación índice refracción	Estructura de la fibra	Modo de propagación	Sección total y sección del núcleo	Ancho de banda típico
Monomodo				125 μm fibra 10μm núcleo	10 Ghz/km
Multimodo Índice gradual				125 μm fibra 62,5 o 50 - 100μm núcleo	100-1000 Mhz/km
Multimodo Índice escalón				380 μm fibra 200μm núcleo	50 Mhz/km

Fibra óptica monomodo: sólo se irradian los rayos paralelos al eje de la fibra óptica, consiguiendo el rendimiento máximo. No existe propagación, lo que lo hace un medio de gran precisión, permitiendo velocidades de 1 a 10 Gbps. El costo de instalación es elevado, aunque la fibra es más barata. Proporciona gran ancho de banda con poca pérdida de señal y es ideal para distancias mayores a 60 km. Utiliza rayo láser para transmitir las señales con una corriente de 5 a 40 mA. Su vida útil es menor que el LED.

Fibra óptica multimodo: contiene varios modos de propagación donde se da el efecto de dispersión. El índice de refracción es máximo en el centro y mínimo en los extremos; por eso, a menor tamaño del núcleo, mayor será la velocidad. Tiene un costo mayor que la fibra monomodo, aunque el costo de conexión es menor, tiene mayor pérdida de señal y menor ancho de banda. Recomendado para distancias menores a 2 km. Utilizan LED como método de transmisión óptico con una corriente de 50 a 100 mA, su velocidad es lenta; en comparación con el láser, su uso es fácil, su tiempo de vida es largo, y generalmente son más económicos.

- Índice gradual: son más costosas, pero tienen mayor ancho de banda.
- Índice escalón: tienen dispersión y reducido ancho de banda; por su bajo costo, resultan fáciles de producir.

La velocidad de propagación es inversamente proporcional al índice de refracción, es decir, que la propagación por los extremos será más lenta, ya que recorren un camino más largo.

Existen muchos tipos de cables de fibra, desde los que transportan un solo filamento hasta los que tienen hasta 24 filamentos dentro de un mismo cable. Las fibras ópticas internas están identificadas con colores internacionalmente definidos por el estándar TIA/EIA-598-B, para así colocarlas en el orden adecuado, ya sea una caja de terminación o un panel de patcheo. En el siguiente cuadro se muestran las abreviaturas según el color y la posición.

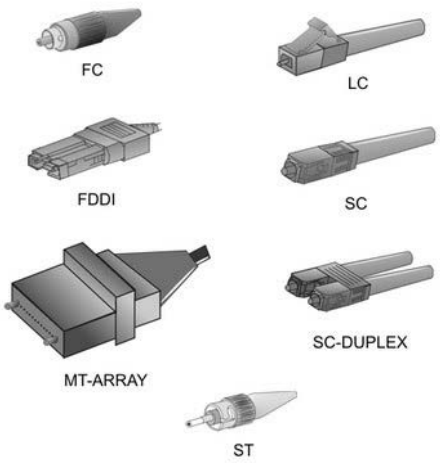
Posición	Color	Abreviatura
1	Azul	BL
2	Naranja	OR
3	Verde	GR
4	Marrón	BR
5	Gris	SL
6	Blanco	WH
7	Rojo	RD
8	Negro	BK
9	Amarillo	LY
10	Violeta	VI
11	Rosa	RS
12	Azul agua	AQ

Las fibras en el interior de un cable óptico se pueden codificar con esta secuencia hasta 24 posiciones. En este caso, desde la fibra número 13 hasta la 24 se vuelven a repetir los mismos colores, pero con la diferencia de que éstos llevan una línea de color negro que los distingue, es decir, el cable número 13 es azul con una línea negra a lo largo de la fibra.

El estándar internacional ISO/IEC 11801, compatible con la nomenclatura de la TIA (ANSI/TIA-568-C.3), especifica tres tipos de fibras multimodo: OM1, OM2, OM3 y un cuarto OM4, definido en el estándar TIA-492-AAAD del 2009. Todos tienen un tamaño de 125 micrones, y según la longitud, pueden variar entre los 33 y los 1000 m y alcanzan velocidades de hasta los 100 Gbps.

Nombre fibra	Tipo	Tamaño (μm)	Velocidad	Distancia (metros)	Haz de luz
OM1	Multimodo	62,5	1000BASE-SX	275	LED
			10GBASE-S	**33**	
OM2	Multimodo	50	1000BASE-SX	550	
			10GBASE-S	**82**	
OM3	Multimodo	50	**10GBASE-S**	**300**	
			40GBASE-SR4	100	
			100GBASE-SR 10	100	
OM4	Multimodo	50	**10GBASE-S**	**550**	
			40GBASE-SR4	150	
			100GBASE-SR 10	150	

Nunca hay que mezclar distintos tipos de fibra ni distintos tipos de cables de cobre, ya que puede devenir en una pérdida sustancial dela señal.



Conectores fibra óptica

Existen diferentes tipos de cables de fibra óptica, y los conectores que se instalan en los extremos pueden ser muy distintos. Los conectores más comunes usados en la fibra óptica para redes LAN son: ST,LC,FC Y SC.

El conector SC (Set and Connect) es un conector de inserción directa que suele utilizarse en conmutadores Ethernet de tipo Gigabit. El conector ST (Set and Twist) es un conector similar al SC, pero requiere un giro del conector para su inserción, de modo similar a los conectores coaxiales.

Estos elementos se encargan de conectar las líneas de fibra a un elemento que puede ser un transmisor o un receptor. Además de los ya mencionados, también existen los siguientes:

- FC: usado para transmisión de datos y/o en telecomunicaciones.
- FDDI: se emplea para redes de fibra óptica.
- LC y MT-Array: comúnmente usados en transmisiones de alta densidad de datos.
- SC y SC-Dúplex se utilizan para la transmisión de datos.
- ST o BFOC: se usa en redes de edificios y en sistemas de seguridad.

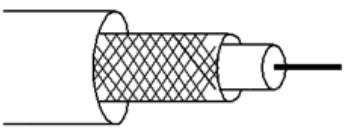
El estándar ANSI/TIA/EIA 568-B3 admite empalmes de fibra por fusión o mecánicos. En cualquiera de los casos, cada empalme no debe tener una atenuación mayor a 0.3 dB.

Si bien la fibra óptica se empezó a comercializar masivamente hacia el 2000, la idealización conceptual de poder transmitir luz a través de una fibra óptica fue desarrollada mucho tiempo antes, en 1842, por los científicos Daniel Colladon y Jacques Babinet.

Hoy en día, la tendencia es reemplazar los cables de cobre UTP por los de fibra óptica en las redes troncales por los siguientes beneficios:

- Menor cantidad de cables y de menor tamaño, ya que 24 cables UTP pueden brindar el mismo ancho de banda de una fibra de sección menor a un solo cable.
- Mayor velocidad.
- Mejor circulación de aire dentro del Rack.
- Menor consumo eléctrico de los equipos.

Cable coaxial



El cable coaxial tiene su origen en 1929, y aún continua vigente, pero con tendencia a ser reemplazado por tecnología más veloz como la fibra óptica.

El cable está compuesto por un núcleo de cobre sólido por donde circula la corriente eléctrica, rodeado por un aislante plástico, más un blindaje exterior tipo malla metálica trenzada, que bloquea los ruidos electromagnéticos y por último, otra cubierta protectora plástica más delgada. Este cable está diseñado para transportar señales de alta frecuencia.

En el pasado, el cable coaxial tenía capacidades de transmisión superiores que el cable par trenzado a 10 Mbps, por ese motivo las primeras redes Ethernet utilizaban este tipo de cables. Con el avance del tiempo, la transmisión por par trenzado se hizo superior en términos de velocidad, y si bien el cable coaxial como medio de transporte de datos tiene una propensión a desvanecerse, aún sigue y es muy usado para transporte de señales de datos telefónicos y televisión por cable.

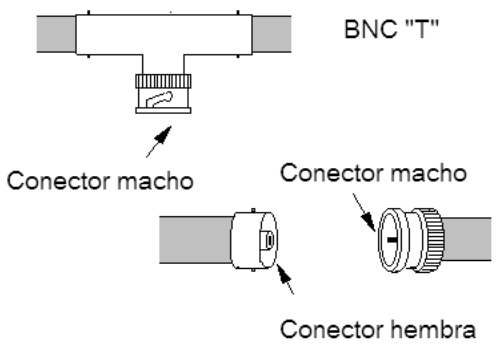
Gracias a su mallado, el cable coaxial tiene muy buena tolerancia a interferencia de señales externas y puede transportar de forma eficiente señales en un gran ancho de banda con menor atenuación que un cable normal. Su limitación fundamental: es para transportar señales de alta frecuencia en largas distancias, ya que a partir de cierto recorrido el ruido superará a la señal, lo que obliga a usar amplificadores, que introducen ruido y un aumento del costo de la transmisión por la red.

Existen distintos tipos de cables, mientras mayor es el diámetro del conductor central, mayor será la capacidad de transportar datos, pero también mayor el costo, además de los costos de los conectores.

Los cables coaxiales, definidos por la norma MIL-C-17 constan de una gran variedad, entre los que se destacan los siguientes: RG-58,RG-59, RG-6, RG-62, RG-59, RG-174, RG-213 y más. Cada uno de estos cuenta con características propias determinadas principalmente por la:

- **Sección principal:** determinante para definir la velocidad y capacidad de transmisión.
- **Frecuencia:** de 100 kHz a 3 000 MHz.
- **Impedancia característica:** es la relación entre la tensión e intensidad de corriente absorbida por el cable. Se expresa en Omnios, y varía según el tipo de cable entre 50, 52, 75, o 93 Ω.

Conectores BNC



Es el tipo de conector que se utiliza para redes de cableado estructurado basadas en cable coaxial. Además, el conector BNC[10] brinda gran seguridad y es empleado en equipamiento de audio, video y señales de radio. Existen varios tipos de conectores: RG-58, RG-59, RG-179, RG-316 y algunos más, pero básicamente son muy parecidos a la figura ilustrada. Dichos

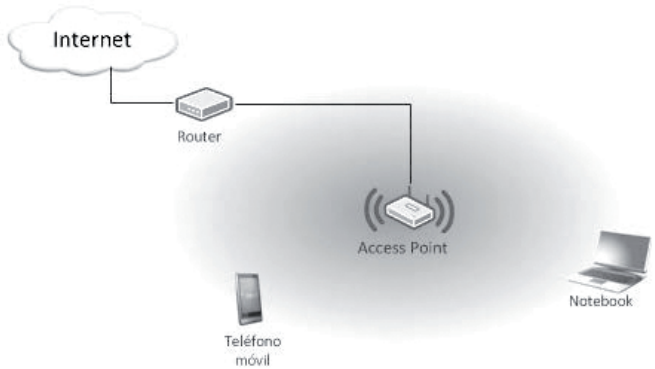
[10]Por sus siglas en ingles Bayonet-Neil-Councelman, creado por los inventores Paul Neill y Carl Concelman.

conectores varían según el tipo de cable que se quiera conectar, pero principalmente todos se componen por una ficha "macho" que se conecta en un extremo, y una "hembra" que se coloca en la otra punta o en el medio de la sección de un cable mediante un conector tipo T. Cuando se los quiere conectar, se los coloca uniendo la ficha macho con la hembra, y se da un medio giro de rosca, dejándolos así en una posición fija, puesto que quedan ya trabados.

Transmisión inalámbrica

La WLAN (Wireless Local Area Network) está definida por el estándar IEEE 802.11x, es también conocida por las siglas Wi-Fi, para comunicaciones inalámbricas mediante tecnología de radio frecuencia.

En el plano funcional la WLAN puede dividirse en dos grandes grupos. Por un lado, aquellos que son utilizados como puntos de distribución, también llamados *Access Points*, como alternativa a la LAN, pero sin necesidad de utilizar cables, lo que permite mayor movilidad. Por otro lado, el vínculo de conexión *punto a punto* para las ubicaciones geográficas con una distancia reducida, en las cuales no existen elementos que obstruyen la línea visual directa.



Como dispositivo de WLAN

Se utiliza como punto de conexión de acceso fácil y sencillo, destinado a dispositivos móviles de los usuarios. Dentro del estándar hay varios tipos que fueron surgiendo a lo largo de la evolución tecnológica, y que brindan más velocidad y mayor radio de alcance. También se debe aclarar que existen distintas formas de proporcionarle seguridad a la red inalámbrica dependiendo del uso y la confidencialidad de los datos. Sólo por nombrar algunos, pueden ser protocolos como: WEP, el WPA, o el WPA2, filtrado por MAC, IPSEC, etcétera.

- Ventajas:
  - **Movilidad:** información en tiempo real en cualquier lugar de la organización o empresa para todo usuario de la red. Ello supone mayor productividad y posibilidades de servicio, desde celulares, tabletas o *notebooks*.

- **Facilidad de instalación:** evita obras para extender cables por muros y techos, más aún en lugares complejos como podrían ser edificios históricos.
- **Flexibilidad:** permite llegar donde el cable no puede, realizar cambios por motivos de ergonomía o simplemente decorativos sin necesidad de tener que reestructurar o rehacer el cableado, sin ningún tipo de inconveniente con la LAN ya existente.
- **Reducción de costos:** cuando se dan cambios frecuentes o el entorno es muy dinámico, el costo inicialmente más alto de la red sin cable es significativamente más bajo, además de tener mayor tiempo de vida y menor gasto de instalación.
- **Escalabilidad**: el cambio de topología de red es sencillo y se trata igual a pequeñas o grandes redes, permitiendo el crecimiento escalable de ser necesario.

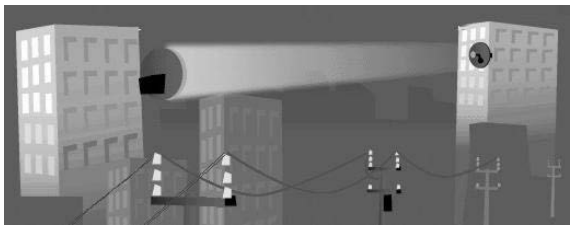
- Desventajas
  - **Velocidad:** las bajas velocidades de transmisión que presentan un aspecto negativo para su elección.
  - **Cobertura:** la distancia reducida que pueden alcanzar las ondas de radiofrecuencia o de infrarrojos es función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso las personas, afectan a la propagación de la energía.

Cuadro comparativo entre los principales estándares IEEE 802.11

Wireless Standard	Popularidad	Año Publicación	Velocidad Máxima	Frecuencia	Alcance máximo interior (mts.)	Alcance máximo exterior (mts.)
802.11a	Baja	1999	54 Mbps	5 Ghz	35	120
802.11b	Alta	1999	11 Mbps	2.4 Ghz	35	140
802.11g	Media/Alta	2003	54 Mbps	2.4 Ghz	38	140
802.11n	Baja	2009	300 Mbps	5 Ghz / 2,4 Ghz	70	250
802.11ac	-	Experimental	1 Gbps	5 Ghz	100 (estimado)	300 (estimado)

Como dispositivo de conexión punto a punto inalámbrico

Supongamos que contamos con dos edificios y se necesita una intercomunicación entre ellos para la transmisión de información. Hay varias soluciones factibles. Se podría tener un cableado dedicado, lo cual podría ser bastante caro o requeriría una instalación bastante difícil según donde nos encontremos, ya que se podría necesitar romper paredes o calles, lo que se requeriría permiso de alguna entidad del estado, descontando su inflexibilidad y escalabilidad.



Como alternativa a dicho problema existen las redes **WiMAX** (Worldwide Interoperability for Microwave Access). Es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2.3 a 3.5 Ghz, y es la marca que certifica que un producto está conforme con los estándares de acceso inalámbrico IEEE 802.16, también conocida como Wireless MAN (Metropolitan Area Network). Estos estándares permitirán conexiones de velocidades similares al ADSL o al cable módem, sin cables y con una distancia de alcance de 50/60 km, pudiendo llegar hasta 80 km; con antenas muy direccionales y de alta ganancia pueden alcanzar velocidades de hasta 75 Mbps, usando un ancho de banda de 20 MHz por cada canal siempre y cuando el espectro esté completamente limpio. Este nuevo estándar es compatible con otros anteriores como el de IEEE 802.11

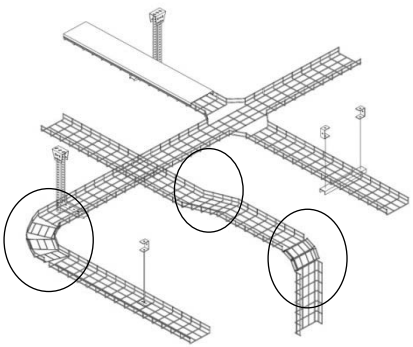
La tecnología WiMAX facilita las conexiones en zonas rurales (IEEE 802.16-2004 para acceso fijo) o de usuarios en el mundo empresarial para mejorar las comunicaciones.

Comercialmente la red WiMax se masificó gracias a los teléfonos inteligentes y a los módems USB 3G (IEEE 802.16e para usuarios móviles), debutó operativamente en el 2008, y ofrecía velocidades de descarga de entre 3.7 Mbps y 5 Mbps.

En el 2011, se aprobó el nuevo estándar IEEE 802.16 m que se lo conocerá comercialmente como WiMAX 2 o redes 4G. Diseñado para ser significativamente más rápido que su predecesor, ya que uno de sus objetivos es que la velocidad de descarga vaya desde los 100 Mbps hasta los 300 Mbps para casos de antenas direccionales.

Recomendaciones de instalación

Manejos de cables



Las canalizaciones mediante bandejas portacables son utilizadas para distribuir y soportar los cables entre la salida del área de trabajo y el cuarto de telecomunicaciones, ya sea por debajo del piso o por encima del techo.

Los cables deben ir fijados en capas mediante abrazaderas o precintos plásticos colocados con intervalos de 4 m, pero no deben tener una tensión excesiva que ejerza una gran presión sobre ellos, ya que podrían debilitar la señal.

Para evitar interferencias electromagnéticas, la canalización de los cables de datos debe mantenerse separada del cableado eléctrico, porque éstos generan grandes campos magnéticos que pueden dañar la señal que circula por los cables de datos. En caso de cruzarse deben hacerlo perpendicularmente.

Cuando desenrolle el cable de la bobina, utilizar un *stand* de soporte o carrete, de manera que permita ir extendiéndolo de manera suave, para no dañar el entrecruzamiento interno del cable. Desenrollar con la base del carretel apoyado en el piso hace que sea propenso a dobleces y quebraduras.

Como se ve en la figura, los radios de curvatura dentro de la bandeja no deberán ser abruptos, para evitar daños internos invisibles desde el exterior. Si bien no existe un estándar, para la mayoría de los fabricantes son los siguientes:

- Para los cables de cobre el radio máximo de curvatura es: 2.5 cm.
- Para los cables de fibra óptica es: 5 cm. Si no se respeta el radio de curvatura es posible que la fibra funcione, pero de seguro será con una pérdida de ancho de banda.

Al momento de la planificación se debe saber cuál es la cantidad de cables que se van a utilizar para poder elegir la bandeja portacables adecuada para soportarlos, ya que ellas tiene un límite de peso máximo que pueden tolerar, evitando así el gasto de tener que comprar dos bandejas de menor capacidad en lugar de comprar la correcta desde el momento inicial.

En el caso de no utilizar bandejas portacables, se pueden instalar soportes colgantes. Todos deberán estar a una distancia menor de 1.2 m entre sí.

Si el cableado fue instalado correctamente por empresas certificadas que siguen las normas del fabricante, es difícil tener problemas. En el mercado hay fabri-

cantes de cables que extienden certificados de garantía por hasta 20 años si contratan a instaladores autorizados.

Cuando se selecciona un fabricante de cables se debe tener en cuenta cuál es la sección del cable. Por ejemplo, en un cable UTP Cat. 6, la sección de cada cable puede oscilar entre 5.3 y 6.8 mm, o un STP puede tener una sección de hasta 7.3 mm. Por más que parezca una diferencia mínima en la sección puede resultar que en la cantidad de cables que se necesitan pasar, el volumen total de cables cambie notablemente, incluso pudiendo superar el límite de cables permitidos en la bandeja, lo que aumentaría el costo ya que se necesitaría otra bandeja adicional para pasar el resto de los cables.

Separación entre cables eléctricos y de datos

Nivel de potencia	Distancia UTP	Distancia STP
menos de 3 kva	5 cm	0
entre 3-6 kva	3 m	0,6 m
mas de 6 kva	6 m	1 m

Para evitar interferencias electromagnéticas, la canalización de las corrientes débiles transmitidas por cables de datos deben mantenerse separada de las corrientes fuertes como son los cables eléctricos y dispositivos electromagnéticos.

El cableado eléctrico genera interferencia electromagnética, que afecta a los cables de datos, en especial a los UTP, y en menor medida a los STP. A mayor voltaje mayor será la interferencia que genera el cable y más grande deberá ser la distancia entre los cables de electricidad y de datos. Si bien no existe un estándar el fabricante de cables líder en el mercado, Siemon (`www.siemon.com`), recomienda las distancias detalladas en la tabla.

Testeo y verificación

Cuando se termina una instalación de cableado estructurado, siempre se deben certificar los puestos de trabajo.

El testeo consiste en realizar una prueba con equipos sofisticados de medición, como pueden ser herramientas de los fabricantes, Fluke, HP, Microtest, entre otros, en donde se colocan dos elementos de medición, uno en cada extremo de la ficha terminal, y mediante el envío y análisis de señales, el equipo determina si la terminación del puesto es la correcta, ya sea para datos o voz.

Más allá de que la instalación sea prolija y adecuada según los requerimientos de instalación, la certificación de cada puesto es de gran importancia, ya que asegura la calidad de transmisión de los datos, dado que puede haber fallas impercepti-

bles a la vista, pero que están presentes y perjudican el buen funcionamiento del cableado. Por ejemplo, el instalador de la obra, cuando desenrollaba los cables UTP, por un manejo inadecuado, estiró los cables, haciendo que el cable internamente perdiera el entrecruzamiento y haciéndolo más permeable a la interferencia electromagnética externa. Además, incluyen un diagnóstico avanzado y la localización de fallas.

Para los cableados de fibra óptica, el análisis es más simple, sólo se deberán tener en cuenta dos parámetros: la atenuación y la longitud, que se pueden medir físicamente o en caso de fibras largas, se puede hacer por medio de un análisis OTDR (Optical Domain Reflectometer, reflectómetro de dominio óptico) es un test complejo que permite identificar la localización de una rotura, normalmente usado en las fibras monomodo.

Para las fibras multimodo se utiliza el test OLTS (Optical Loss Test Set, prueba de pérdida óptica) que mide la atenuación del enlace según la pérdida de potencia óptica recibida; suelen ser más económicas que las pruebas OTDR. Las normas TIA/EIA 568 y la ISO/IEC 11801 establecen los límites de atenuación permitidos por cada tramo y por cada empalme según el tipo de fibra.

Para las pruebas de verificación y certificación es deseable contratar una empresa que no haya participado en la instalación del cableado y que entregue un certificado escrito con un reporte sobre el estado de la instalación.

Etiquetación de cables

La rotulación de cables dentro de un Data Center consiste en colocar una etiqueta que permita identificar el cable, independientemente del producto o proveedor, brindando una administración unificada para identificar los cables de manera ágil. Por lo general, es una tarea que muchas veces queda relegada o no se realiza regularmente cuando ocurren cambios, razón por la cual, con el transcurso del tiempo, en unos años, si no se han realizado las tareas oportunamente probablemente sea muy difícil identificar un cable correctamente dentro del Data Center.

La norma ANSI TIA/EIA-606-A, publicada en 2002, es el estándar para la Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales, y está dividida en cuatro clases de administración que aumentan según la complejidad y el tamaño del Data Center:

- **Clase 1:** un edificio simple, una sala de telecomunicaciones y cableado horizontal.
- **Clase 2:** un edificio simple, múltiples salas de telecomunicaciones y cableado horizontal, cableado troncal.
- **Clase 3:** múltiples edificios , múltiples salas de telecomunicaciones, cableado horizontal y cableado troncal

- **Clase 4:** múltiples sitios, múltiples edificios, múltiples salas de telecomunicaciones, cableado horizontal y cableado troncal.

La norma establece códigos por color en las etiquetas que identifican el tipo de cable:

Color	Uso
Naranja	Terminación central de oficina
Verde	Conexión de red (lado usuario)
Violeta	Conexión mayor (Computadoras, PBX, LAN)
Blanco	Terminación troncal cables intraedificios (conexión principal e intermedia)
Gris	Terminación troncal cables intraedificios (conexión intermedia y horizontal)
Azul	Terminación de cable horizontal
Marrón	Terminación cableado troncal entre sitios
Amarillo	Mantenimiento auxiliar, alarmas y seguridad
Rojo	Telefonía

Si bien éstos son los colores que establecen la norma, siempre es preferible tener los cables rotulados en blanco sobre negro, antes que no tener nada. Generalmente se utilizan etiquetadoras portátiles de bajo costo que imprimen en cintas autoadhesivas, estableciendo un identificador único para cada cable, de manera de minimizar los errores humanos en caso de que se deban realizar cambios. Asimismo, conviene emplear una tipografía uniforme con buen contraste y una buena durabilidad (superior a los 15 años). Los marcadores de fibra sólo se deben usar para el etiquetado borrador.

Cuando se utilizan identificadores en áreas de trabajo, las terminaciones de estaciones deben tener un rótulo en la placa, el bastidor o el conector mismo.

Identificador enlace horizontal

FL = Identificador de piso y telecomunicaciones

A = identificador de *Patch panel*

NN = Número de puerto

FL-AANN por ejemplo: 2N-A31

2do piso – Ala Norte - *Patch panel*A – Puerto 31

Las buenas prácticas de etiquetado y los registros detallados son críticos para:

- El manejo de la red instalada por parte de los administradores.
- La minimización de riesgos de fallas humanas.
- El mantenimiento y rastreo de problemas.
- El procesamiento de reclamos de garantía con fabricantes de cables y componentes
- Para los *Patchpanels* las etiquetas de identificación son más simples y deben cubrir lo siguiente:

Cuarto de Telecomunicaciones A, B, C, etcétera.
Rack XX
Panel de parcheo XX
Puerto del panel XX
Voz o datos: V o D

Por ejemplo la etiqueta: A020523D

ID Sala comunicaciones A; Rack 02; *Patch panel* 05; puerto 23 y D datos

Importante

- Cuando se realizan cambios en la estructura del cableado, se deberán actualizar las etiquetas que los identifican.
- De igual manera, se deben rotular los cableados eléctricos, identificando en las terminales de conexión, cuál es la fase y cuál es la PDU fuente de dicha administración, para identificarlas en caso de mantenimiento.
- Al igual que la identificación de los cables, lo mismo debe hacerse para los Racks, los equipos de comunicaciones, la identificación de los puestos de los usuarios finales y para los servidores. Profundizaremos en este aspecto, en el capítulo siguiente.

Organización

8

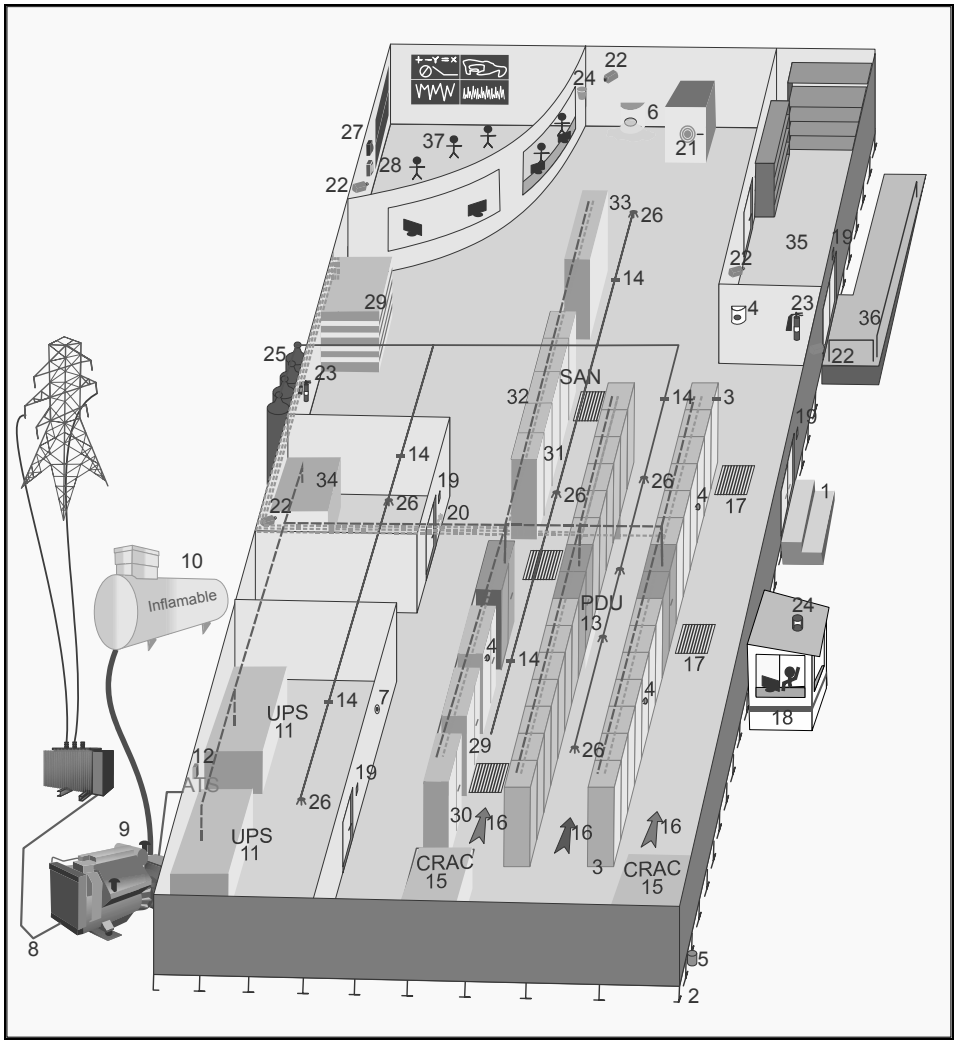
"Por muy hermosa que sea la estrategia, de vez en cuando debes mirar los resultados".

-- Winston Churchill (1874-1965) Político, escritor británico. Premio Nobel de Literatura en 1953

Visitas guiadas

Dependiendo de la naturaleza del negocio, es posible que algunos clientes pidan conocer el Data Center para asegurarse de cómo están protegidos sus datos o que, movidos por la curiosidad, quieran comprobar si se cumplen las normas de protección de datos requeridos por los organismos de supervisión. Por ello, la persona que escolte a las visitas deberá recordarles a los invitados las siguientes recomendaciones:

- **Mantenerse juntos**: que nadie quede fuera del alcance de la vista del guía.
- **No tocar:** hacerle comprender a los visitantes de la importancia de los equipos que se encuentran allí. Por eso no deben tocar ningún cable ni interruptores, y deben caminar con precaución sólo por el área que indica el guía.
- **Demostrar:** es conveniente utilizar un lenguaje simple para explicarle a las visitas, las áreas fundamentales del Data Center, su importancia y criticidad.



En la página Web del libro podrá descargar un archivo PDF de este plano, para imprimir en el tamaño que desee.

1.- PUERTA PRINCIPAL
2.- PISO TÉCNICO
3.- RACKS
4.- SENSORES TEMPERATURA Y HUMEDAD
5.- SENSOR DE LÍQUIDOS
6.- HUMIFICADOR
7.- DETECTOR DE HUMO
8.- CABLEADO RED ELÉCTRICA
9.- GENERADOR
10.- TANQUE COMBUSTIBLE
11.- UPS
12.- ATS
13.- PDU
14.- SENSOR TEMPERATURA / HUMO
15.- CRAC
16.- PASILLO FRIO / CALIENTE
17.- REJILLA INGRESO AIRE FRÍO
18.- CABINA SEGURIDAD
19.- LECTOR TARJETA CON CHIP
20.- LECTOR DE SEGURIDAD BIOMÉTRICO
21.- CAJA SEGURIDAD IGNIFUGA (PARA LAS CINTAS DE BACKUP)
22.- CÁMARA CCTV
23.- EXTINTOR DE FUEGO
24.- SIRENA
25.- TANQUE GAS EXTINTOR INCENDIOS
26.- ROCIADOR
27.- EPO
28.- CENTRAL DETECCIÓN DE INCENDIOS
29.- ROUTER SWITCH CORE
30.- BACKBONE SWITCH CORE
31.- CENTRAL TELEFÓNICA
32.- SAN
33.- DISPOSITIVO DE BACKUP
34.- MAINFRAME
35.- DEPÓSITO
36.- RAMPA ACCESO AL DEPÓSITO
37.- CENTRO DE MONITOREO / NOC

Recepción de equipos

Frecuentemente en el Data Center, se reciben distintos tipos de materiales, como: servidores, filtros de aire, cables, cintas, disco, etcétera. Ellos deberán ser almacenados hasta el momento de su utilización en una zona asilada y segura, ya

que muchas veces contienen elementos inflamables, por su envoltura exterior protectora. Dicha sala deberá estar protegida y vigilada, más aún si en ella ingresan personas ajenas a la empresa para hacer las entregas, ya que muchas veces ese espacio también se utiliza para almacenar piezas de repuesto, para reemplazarlas en casos de emergencia, como discos, memorias, fuentes de alimentación procesadores, etcétera.

Deberá contar con los controles de acceso adecuados, con buena capacidad de maniobrabilidad, como por ejemplo, rampas o elevadores, ya que muchas veces se ingresan equipos muy pesados.

Medidas básica para proteger equipos en ambientes chicos

Las salas de servidores pequeñas son uno de los problemas más difíciles de manejar, ya que en la mayoría de los casos están ubicados en locaciones remotas donde por problemas de latencia de red se instalan equipos localmente para proveer servicios a los usuarios finales. Adicionalmente en muchos casos, agregar soluciones de monitoreo o control de acceso para eso casos no resulta económicamente viable, tanto por el tamaño de la sala en relación con la inversión necesaria como por falta de presupuesto.

Los problemas más comunes son

- **Falta de controles de seguridad física:** se deberá establecer una persona de la oficina remota como punto de contacto, que posea la llave y se asegure de que nadie ingresará allí. Si el presupuesto lo permite, la colocación de una cámara para ver la sala de manera remota sería una excelente opción.
- **Problemas de enfriamiento:** una alternativa podría ser añadir una rejilla de ventilación en la parte baja de la puerta de entrada, que permita el ingreso del aire fresco y disminuya así la temperatura de la sala, pero mejor aún sería colocar un aire acondicionado, que por razones de presupuesto será un equipo del tipo doméstico. Probablemente en las oficinas remotas, los límites ambientales sean mayores que los de un Data Center grande que posee más recursos.

  La dimensión de la sala también es importante, mientras más grande sea la sala, mejor será la disipación del calor hacia todo el espacio, permitiendo una mejor temperatura promedio. Por otra parte, los componentes de construcción de las paredes y el cielorraso también influyen ya que los materiales tienen resistencia térmica, por ejemplo el yeso aísla más la temperatura comparándolo con el concreto, la situación empeora, incluso más si las paredes exteriores están expuestas al rayo del sol.
- **Falta de monitoreo:** probablemente se pueda establecer un monitoreo en el plano lógico, en el aspecto de equipos. Aunque se debe tener en cuenta que pueden darse situaciones de falsos positivos, por ejemplo: si el enlace con la

oficina remota pierde vínculo, se pueden recibir muchas alertas al mismo tiempo, pero en realidad los equipos no están apagados, sino que perdieron la conexión con la red. El monitoreo de la infraestructura física resulta muy difícil, ya que los equipos chicos no suelen estar preparados para ese tipo de funciones.

- **Problemas eléctricos:** para las salas pequeñas solo se colocan UPS, ya que un generador es económicamente inviable, generalmente proveen una autonomía de entre 15 a 20 minutos. Lo recomendado en estos casos, es seleccionar una UPS inteligente, que cuando llegue al límite de pérdida carga, comience a apagar los equipos automáticamente, evitando así que los equipos se apaguen abruptamente y previniendo fallas de hardware y software.

Estrategias para manejo cableado

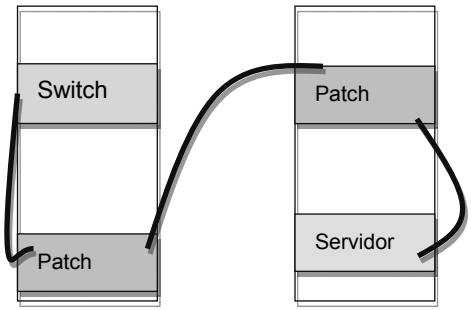
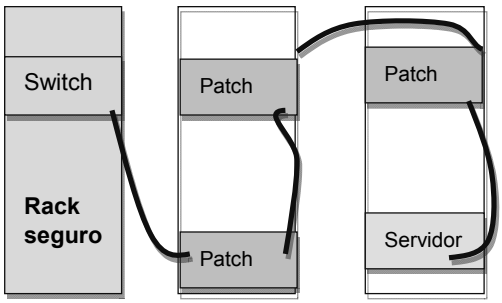
La tendencia de concentración de cables que ingresa a los Rack es cada vez mayor. Para tener un mejor rendimiento y evitar cuellos de botellas, se dividen las redes, ya sean física o lógicamente VLAN[1]. Por ejemplo, se separan:

- Red de producción, con una o dos placas físicas de red para armar una solución redundante por software a nivel de Sistema Operativo.
- Red de administración para las consolas de administración remota.
- Red de SAN.[2]
- Red de *backup*.
- Otras.

Esto puede generar un gran desorden, por eso es recomendable, en la medida en que sea posible, utilizar cableados definidos por color según la función. Además, tantos cables pueden causar una obstrucción en el flujo del aire refrigerado, causando un aumento de la temperatura dentro del Rack.

[1]VLAN o Virtual LAN es una segmentación lógica de una red que está unida físicamente, separando el tráfico para mejorar la seguridad y el rendimiento.
[2]Storage Area Network: sistema de almacenamiento a gran escala por medio de la red, conectado por fibra, ya que requiere gran velocidad de acceso.

Modelos de conexión entre el los servidores y los equipos de red

Simple	Descripción
	• Ventajas — Cantidad exacta de cables. • Desventajas — Se necesita mayor acceso al equipo de red activo, pudiendo causar costosas roturas involuntarias.
Compleja (recomendada por la TIA)	**Descripción**
 Rack de distribución	• Ventajas — Mayor seguridad. — Acceso al *switch* restringido a los administradores de red (minimiza la posibilidad de falla humana, en especial en dispositivos costosos). • Desventajas — Mayor cantidad de cables. — Se agrega un Rack intermedio de distribución.

Aunque parezca lo más simple y económico **no** es recomendable hacer conexiones punto a punto, ya que a medida que aumenta la cantidad de cables, mayores son los problemas de circulación de aire, mayor es el desorden, y aumentan las probabilidades de cometer errores humanos, convirtiendo el Data Center en un caos de cables inmanejable.

Reemplazar el cableado que circula por debajo del piso técnico y utilizar canalizaciones superiores para llevar los cables por encima de los Racks, puede generar una disminución del 24% en la energía utilizada para la refrigeración, ya que la circulación de aire es mucho mejor.

Estrategias de gestión de cableados

Distribución Encima del Rack (Top-of-the-Rack oToR)

En este esquema se dispone un equipo de red por cada Rack en la parte superior, donde ingresan los cables desde el distribuidor de la red troncal. Esta opción no posee cableado horizontal ni sigue las especificaciones contenidas en las normas de cableado de la industria. Es de fácil instalación, baja densidad de cableado, pero su desventaja es que requiere un equipo de red por cada Rack, resultando, tal vez, excesivo.

DistribuciónZonal (Middle-of-the-Row –MoR- o End-of-the-Row –EoR)

El esquema es parecido al ToR, solo que en lugar de colocar el equipo de red en cada gabinete, éste se ubica en el medio o en la cabecera de cada fila de Racks (máximo de ocho por fila). Si bien este esquema no posee cableado horizontal, se acepta como excepción a la norma, la cual permite conexiones directas entre *switchs* de acceso y servidores ubicados en la misma fila.

La interconexión de servidores es simple, reduce la cantidad de cables y hace un buen aprovechamiento de los equipos de red. Su principal desventaja es que desaprovecha el espacio crítico en la zona, porque están los servidores donde se distribuye la refrigeración, protección incendios, espacio físico, etcétera.

Distribución Centralizada (Any-to-All)

El esquema consiste en una distribución centralizada donde todo el cableado termina en los Racks de red troncal. Si la densidad del cableado utilizado no es muy alta o si las vías de canalización permiten grandes volúmenes de cableado, ésta resulta la solución ideal, dado que optimiza el uso de los puertos disponibles de equipos de red y maximiza la flexibilidad de la administración de servicios. Esto sucede, porque cualquier enlace de cableado permite su conexión con cualquier puerto de red.

Funciona bien para Data Centers pequeños, ya que la administración es simple. Para aquellos casos donde tenemos un Data Center de mayor tamaño resulta inviable por la enorme cantidad de cables que requiere.

Conclusión

La solución ideal para el cableado estructurado resulta en la combinación de los esquemas planteados, implementándolos en aquellas situaciones en donde ofrecen sus mayores beneficios. Por ejemplo: el cableado de fibra óptica para la SAN puede

implementarse en un esquema distribución centralizada, porque los cables de fibra óptica ocupan muy poco especio en canalizaciones; y por otro lado, conviene utilizar un esquema de distribución zonal para el cableado de red.

Definición y documentación de políticas y procedimientos

Como parte de las tareas de organización y administración de un Data Center es importante la documentación de los procesos y procedimientos necesarios para dar soporte a las tareas básicas, que en conjunto darán el sustento a las políticas de administración.

La documentación debe estar formalizada en un conjunto de procesos y procedimientos de forma **escrita**, redactados de manera clara y sin ambigüedades, almacenados en un lugar accesible para todas las personas que dan soporte al Data Center, y serán consultados en diversas situaciones. También es recomendable tener documentada la información útil, como la lista de contactos internos y proveedores con sus respectivos teléfonos, números de contrato de proveedores, etcétera.

Procesos ≠ Procedimientos

- **Proceso:** grupo de actividades descritas a alto nivel a partir de cierta entrada para lograr una salida deseada. Están impulsados por la búsqueda de resultados, y son dinámicos. Un proceso puede tener muchos procedimientos.
- **Procedimiento:** secuencia de pasos definidos en forma específica para ejecutar una tarea estructurada. Son estáticos y están pensados para tareas operativas.

Por ejemplo, el proceso de *Gestión ambiental del Data Center* establecerá cuáles son los límites de operatoria normal de temperatura y humedad, cuál es la temperatura en los pasillos calientes y fríos, etcétera. Como parte de dicho proceso pueden existir varios procedimientos, por ejemplo, uno sería el procedimiento de *Emergencia de altas temperaturas*, que detallará qué acciones se deberán tomar si el aire acondicionado deja de funcionar; hasta qué grado aumento de la temperatura se deberá esperar para tomar acciones; qué Racks se pueden apagar primero, etcétera. Ese conjunto de procesos y procedimientos darán forma las políticas y norma de gerenciamiento del Data Center.

Aquí se recomiendan solo algunas pautas básicas para Data Centers, que se ajustarán a las dimensiones y necesidades de cada uno:

- La prohibición de fumar en todo el edificio.
- El limitar al mínimo posible el tiempo de permanencia del personal dentro del Data Center.
- El establecimiento de un procedimiento de visitas y otro para proveedores.

- En el caso de activación del generador, los ascensores deben desactivarse y enviarse a la planta baja, como si fuera un incendio, ya que si la carga de los equipos está próxima a la capacidad total del generador puede haber un apagón general en el Data Center si se utilizan los elevadores. Si bien su consumo puede estar contemplado en el cálculo para cuando se activa el generador, cuando el ascensor arranca se produce un pico de consumo eléctrico que puede llegar a sobrepasar la capacidad total del generador, causando un apagón.
- La prohibición de ingreso al Data Center de alimentos, bebidas, elementos químicos e incluso armas, además de cámaras y celulares.
- La disposición de herramientas para realizar algunas tareas simples de mantenimiento que serán enumeradas en el último capítulo.
- El ingreso y la permanencia de proveedores al Data Center debe ser escoltado por personal interno.
- Se deben seguir las indicaciones de advertencia colocadas en el Data Center, en especial en aquellas zonas donde hay contacto con la electricidad.
- La lista de contactos con sus respectivos teléfonos, en horario de trabajo y de guardia, debe estar a mano.
- La rotulación y la visible señalización de los lugares donde se encuentran los sistemas de extinción de incendios.
- La coordinación de las visitas con los proveedores, con suficiente anticipación (al menos dos días), así como la gestión de las autorizaciones para dichos accesos.
- La metodología de recepción de equipo, ya mencionada.
- La rotulación de equipos y pasillos, ya mencionada.

Nomenclatura lógica de equipos

Dentro de la red, los equipos se identifican lógicamente con un nombre único que los distingue para por usarse en el ambiente.

El nombre de un equipo puede ser cualquiera que el administrador decida, usando letras y números, pero omitiendo algunos caracteres especiales como *$, #, -, @,* ya que no están permitidos por algunos sistemas operativos, y su longitud no debe ser mayor a 15 caracteres, en caso contrario, puede haber problemas para conectarse a equipos con nombres que excedan esa cantidad de caracteres. Aunque los sistemas actuales permiten usar nombres más largos, pero realmente no es necesario.

Si bien no existe ningún estándar internacional de nomenclatura, **cada empresa deberá definir un modelo propio** que debe ser respetado globalmente. La idea es seleccionar una nomenclatura inteligente que en base al nombre permita identificar

la ubicación del servidor, el sistema operativo, la aplicación, el entorno (laboratorio, desarrollo, test, QA, producción u otro) o alguna otra información que se considere importante. Mientras se monitorean los equipos y si se cuenta con una central única, una nomenclatura correcta puede facilitar el direccionamiento de las alertas a los equipos de soporte correspondientes o, por ejemplo, identificar problemas en sitios remotos de manera veloz.

Una estructura de nomenclatura sugerida podría ser la siguiente, con un encabezado para definir la ubicación física y una parte para variable para definir los detalles del rol de ese equipo:

Encabezado	Variable
UUUCC	SAAA###ER

UUU: ubicación física, como: nombre de un país, número de Data Center, u otra.

CC: ciudad, estado, provincia, u otra identificación.

S: sistema operativo, por ejemplo: W: Windows, L: Linux, U: Unix, etcétera.

AAA: aplicación, *CTX*: Citrix, *SAP, ERP: Enterprise Resource Planning*, *Web,* etcétera.

###: son espacios reservados para utilizar con números, preferentemente consecutivos, a partir del último utilizado.

E: entorno del servidor como *L:* laboratorio, *D:* desarrollo, *T:* test, *Q*: QA, *P:* producción.

R: zona de red donde está instalado, *I:* red interna, *D*: DMZ[3],

Ejemplos:

ARGBALSAP004TI: servidor ubicado en la Argentina, en la provincia de Buenos Aires, con sistema operativo Linux, con aplicación SAP usado para el ambiente de test y conectado a la red interna.

ARGRNWEXC003PD: servidor ubicado en la Argentina, en la provincia de Río Negro con sistema operativo Windows, ejecutando Exchange usado en el ambiente de producción y conectado a la red de DMZ.

Otro ejemplo usando una nomenclatura diferente sería:

[3]Zona de red desmilitarizada o red perimetral (*demilitarized zone*). Allí se conectan los servidores de la red que está expuestos directamente a Internet, como los servidores de correo.

DC1GUORA231PI: servidor ubicado en el Data Center número 1, usado para aplicación global "G" con sistema operativo Unix y base de datos Oracle usado en el ambiente de producción y conectado a la red interna.

Quizás al principio resulte compleja la nomenclatura si no se conocen las definiciones que representan cada grupo de identificadores, pero la información que brinda un solo nombre es muy amplia, simplifica la estandarización global y el direccionamiento de alertas en ambientes que tienen un monitoreo centralizado.

Si en una consola de monitorización aparecen repentinamente 80 alertas de servidores que no responden y todos comienzan con ARGRN, fácilmente podemos suponer que el enlace de comunicaciones entre la central y la ciudad de Rio Negro está cortado o hubo una falla eléctrica en ese sitio.

Gestión del Data Center

La gestión de infraestructura del Data Center (DCIM, Data Center Infrastructure Management) es la capacidad de lograr un buen rendimiento de los recursos administrados, buscando la optimización continua de una manera simple, considerando que cada vez hay más interdependencia entre la capa física y la capa lógica de la infraestructura. Esto se logra por medio de un monitoreo integral que facilita la gestión, la eficiencia y mantiene la disponibilidad.

Cuántas veces escuchamos este diálogo:

–¿Para qué se utiliza ese servidor que está allí?

–No lo sé, pero estaba funcionando desde antes de que ingresara a la empresa.

Esa respuesta puede parecer ilógica, pero resulta bastante habitual en la práctica, sobre todo en ambientes medios a grandes.

Probablemente ese equipo está encendido desde hace años y nadie lo usa o quizás la aplicación fue migrada a otro servidor, generando calor, consumiendo energía, es decir, haciéndole perder dinero a la empresa innecesariamente.

En el sitio `http://www.dcimexpert.com/se` pueden ingresar sugerencias y recomendaciones para mejorar las tareas de gestión.

Antiguamente la misión era sólo dar soporte a las necesidades de negocio, cumpliendo con los planes actuales. Pero hoy en día, la tendencia es distinta, la gestión administrada debe ser capaz de **brindar una ventaja competitiva para lograr el éxito del negocio**, haciéndolo ágil y eficiente de manera confiable. Los cambios de las economías son muy rápidos y el no ser capaz de responder de forma satisfactoria puede hacer fracasar un proyecto o perder una oportunidad única. Por eso, los ojos deben estar puestos en el futuro y en las próximas tendencias.

Los desafíos pueden tener orígenes muy variados: económicos, tecnológicos, el ámbito de los negocios y lo relacionado con el cumplimiento de normativas o regulaciones.

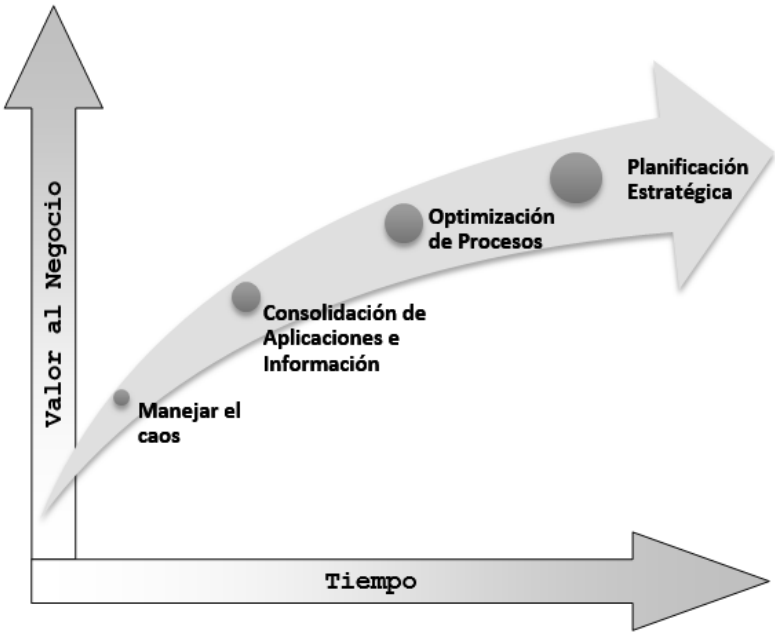
El modelo de gestión tiene cuatro etapas de evolución

0.- Manejar el caos: descubrir e investigar, ya que no se puede gestionar lo que no se conoce. Por eso, la recolección de datos básicos acelera la implementación y el mantenimiento de los activos para la posterior toma de decisiones. Hay que recolectar información, realizar diagramas de la infraestructura, identificar individuos y aplicaciones claves.

1.- Consolidación de las aplicaciones y la información: consiste en gestionar de forma eficaz los activos por medio de la consolidación de la información recolectada. Hay que identificar los puntos de monitoreo importantes, y buscar la simplificación e eliminar los desperdicios como son las falsas alertas. (Proceso Reactivo).

2.- Optimización de procesos: es indispensable realizar el monitoreo adecuado de los cambios o implementaciones sobre los activos en el Data Center, haciendo un análisis y diagnóstico, buscando gestionar los medios para lograr obtener los datos en tiempo real. Luego vendrá la comparación con la información histórica para evaluar los resultados y la documentación de las nuevas prácticas con el objetivo de reducir el esfuerzo y el MTTR.

3.-Planificación estratégica: de acuerdo con los resultados obtenidos en los cálculos e implementación, se realiza la predicción del comportamiento de los posibles escenarios futuros en las condiciones actuales, y cómo se podrían adaptar los activos hacia adelante dentro del Data Center. Esta planificación tendrá como propósito el acelerar las expectativas y disminuir los costos, asistiendo al negocio de una forma dinámica y automatizada. (Proceso Proactivo).



Con el objetivo de mantener y asegurar la capacidad de las utilidades del Data Center, hoy en día, en general ,la mayoría de los Data Centers tiene objetivos de disponibilidad mayores al 99.9%,y el responsable de la administración deberá desarrollar y mantener sustancialmente las siguientes actividades para poder lograrlos:

- Una visión clara de las estrategias de la organización.
- Entrenamiento permanente del personal.
- Una clara definición de procesos y procedimientos, fundamental para minimizar las fallas humanas.
- Controles escritos y secuencia de operaciones en caso de emergencia.
- El planeamiento de tareas y mantenimientos.
- La documentación completa, con diagramas y gráficos de la capacidad utilizada actualmente y la capacidad real disponible, como superficie disponible, espacio en el Rack, capacidad eléctrica, capacidad de enfriamiento, etcétera.
- Estar actualizado con las nuevas tecnologías.
- Mantenerse dentro del presupuesto.
- Llevar un control del inventario de partes y de la infraestructura física, preferentemente en tiempo real.
- Informes de avance de nuevos proyectos.

Desde el punto de vista del personal a cargo de la operatoria del Data Center, se debe seguir una metodología de entrenamiento que permita alcanzar un nivel elevado de conocimientos con el fin de reducir la probabilidad de errores.

Los entrenamientos deben ser evaluados, analizados y corregidos cuando los resultados no hayan sido satisfactorios por problemas de ejecución o por problemas de compresión.

La automatización simplifica y reduce la probabilidad de errores humanos, por eso siempre que sea posible es recomendable hacerlo.

Para evitar el uso de planillas de cálculo como control de inventario de los equipos dentro del Data Center, que suelen ser estáticas y no están actualizadas debidamente (en especial, cuando hay varios sitios que administrar y el crecimiento es grande), existen herramientas dinámicas que facilitan la tarea de DCIM, como: CA DCIM 4.0 de ComputerAssociates; Asset Point de Align Communications; Infra Stru Xure de APC; Operations Manager de HP; Nlyte, Open Data Software de Modius; o Avocent de Emerson, solo por nombrar algunos. Muchos de ellos poseen funcionalidad que les permiten tomar la información de manera automática según el hardware.

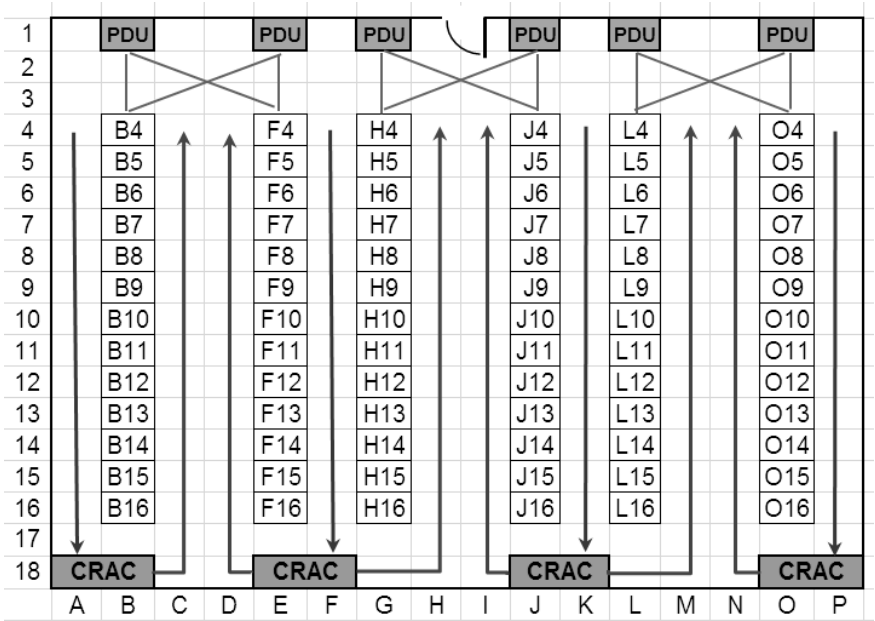
Cabe destacar que existe una solución recomendable basada en software libre llamada Open DCIM `http://www.opendcim.org` y que se instala fácilmente, basándose en una solución Web para reemplazar las planillas de cálculos.

Según la consultora Gartner, en 2010, solo el 1% de los Data Centers había adoptado este tipo de herramientas, pero se espera que para el año 2014 este tipo de soluciones sea adoptada por el 60% de los Data Centers.

Funcionalidades deseables de una herramienta de gestión DCIM

- **Centralización:** toda la información puede ser consultada desde un solo lugar.
- **Autodescubrimiento:** a medida que se agrega nuevo hardware, deberá ser visualizado en la consola, quizás haya una limitación por fabricante o modelo.
- **Visualización:** la herramienta debe ser capaz de mostrar gráficos en tiempo real y extraer reportes, para efectuar comparaciones a futuro de la capacidad actual del Data Center, como ser: red, electricidad, UPS, almacenamiento, temperatura, espacio en Racks, etcétera.
- **Comunicación:** capacidad de enviar notificaciones, alertas, correos u otras notificaciones, dadas determinadas condiciones.

La decisión de adquirir un software de DCIM no es simple, ya que el software es costoso y requiere dedicación de recursos adicionales en la configuración y puesta a punto del sistema. Dichas implementaciones no son simples y pueden llevar tiempo. El objetivo final de una herramienta DCIM es tener el control centralizado de los recursos, generar reportes sobre la base de la información recolectada, y tomar decisiones que permitan optimizar los recursos, generando ahorros en la operatoria.



Para Data Centers grandes, la identificación, como se hace con los cables de red y electricidad, es muy importante al momento de localizar los equipos. Por eso debe haber un diagrama con el esquema del diseño donde se identifiquen los Racks y los pasillos como si fuera una grilla numerada:

De la misma forma, se deberán rotular los servidores con etiquetas ubicadas en el frente de ellos. Esto servirá como asistencia de identificación para Data Centers donde los administradores estén en una ubicación remota y requieran la asistencia de una persona que se encuentre físicamente donde está el servidor, por ejemplo, para colocar un CD.

Otra buena herramienta de gestión para los administradores es conectar todos los servidores a alguna solución de KVM *(Keyboard Video Mouse)* que permiten ver de manera remota lo que muestra el servidor por pantalla, a través de la red así como también ingresar símbolos por teclado o mover el *mouse.*

Es muy importante tener diagramas actualizados de la disposición de los elementos del Data Center en planos, también llamado *layout*, ya sea desde la infraes-

tructura física y también de la infraestructura de comunicaciones, con el diagrama de todas las redes troncales y sus oficinas remotas. De esta manera, se tendrá una simple vista de un esquema simplificado de cómo es la infraestructura en caso de que tengamos algún problema, y esta representación nos podrá ayudar a entender el origen del problema.

Como parte de las tareas de mantenimiento para el buen funcionamiento del Data Center, las obras que se realicen deben estar aprobadas y coordinadas en función de la disponibilidad de los servicios que allí se alojan. Por ello es fundamental tener una buena comunicación entre los proveedores del servicio y la gestión del Data Center.

Para aquellas tareas que sean de mantenimiento repetitivo se puede establecer un esquema fijo de mantenimiento preestablecido, en donde todas las partes interesadas están notificadas de dichos trabajos con anterioridad, y conocen su posible impacto, el cual estará documentado debidamente.

Dentro del proceso de gestión de Data Centers globales para empresas grandes con diferentes sitios de alrededor del mundo se encuadra la estrategia usada por muchas compañías en distintas áreas dentro del soporte de IT, conocida como ***Follow the Su n***(siguiendo al Sol). Esta estrategia tiene como propósito brindar soporte a las operaciones globales. Fundamentalmente consiste en utilizar los recursos de la región donde es de día en ese momento para soportar allí todas las operaciones de esa región o de otras en donde sea de noche al mismo tiempo.

El objetivo es la optimización, simplificación y la reducción de costos, pero para que esta metodología funcione correctamente requiere una adaptación en las empresas que puede llevar años de trabajo en estandarización de procesos, consolidación de tecnologías y entrenamiento.

Tablero de control

Constituye una herramienta de gestión cuya característica principal es brindar información en tiempo real, **ya que no se puede controlar aquello que no se puede medir**. Está formado por indicadores que permiten ver el estado de la situación actual de un simple golpe de vista. Lo cual permite o facilita:

- Comunicar y vincular los objetivos e indicadores.
- Incrementar la retroalimentación para tomar decisiones.
- Planificar, establecer objetivos y alinear con las metas iniciales
- Transformar la estrategia y aclarar la visión.

Establecer los indicadores iniciales es la base para hacer evaluaciones cíclicas y comparar esos resultados con los planificados inicialmente.

Existen diversos tipos de tableros de control: **estratégicos,** para las decisiones ejecutivas a largo plazo; **directivos,** para las decisiones a mediano plazo; y los que tienen que ver con las tareas diarias de un Data Center, que son los **operativos**.

Tablero de control operativo: permite hacer un seguimiento al menos diario del estado de situación de una actividad determinada, para así tomar a tiempo las medidas correctivas necesarias. Está enfocado al proceso de dirigir, no de operar, dado que es una herramienta de diagnóstico y control. Idealmente debe ser automático, por ejemplo, recolectando la información desde una herramienta de DCIM, para que no sea una tarea administrativa extra.

¿Qué variables se deben tener en cuenta a la hora de armar un tablero de control para un Data Center?

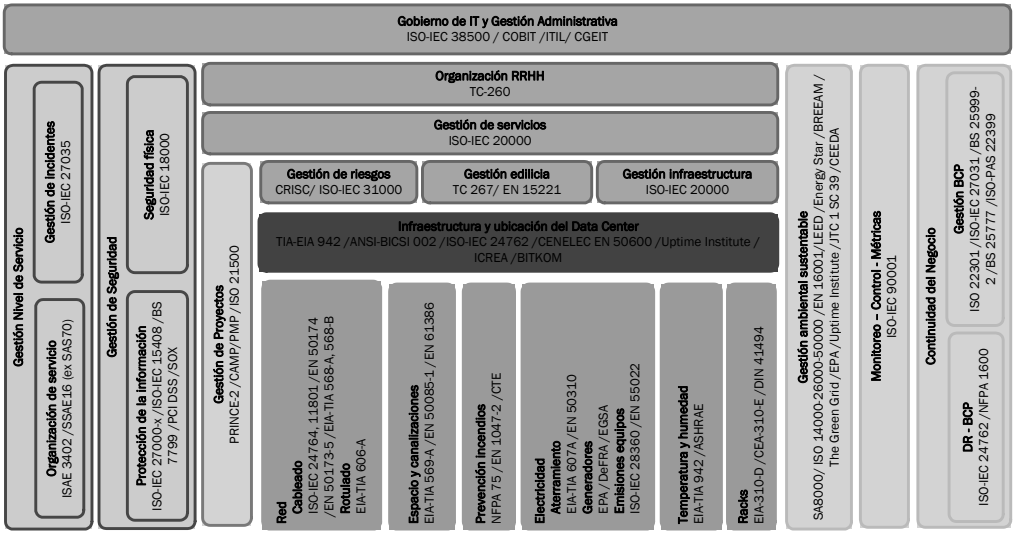
- Determinar cuáles son los valores más importantes a considerar. Por ejemplo, estado de carga de la UPS, nivel de utilización del aire acondicionado.
- Parámetro de alarma: definir los rangos por encima o por debajo de los cuales el indicador es preocupante.
- Frecuencia de actualización: intervalo de tiempo en que la información será actualizada.
- Referencia: base sobre la cual se desean calcular las desviaciones. Puede ser un estándar, la historia, el mes anterior, el promedio de los últimos dos meses, el presupuesto inicial o revisado, un objetivo o una meta, como versión más optimista del presupuesto, etcétera.
- Gráficos: definir la mejor manera de representar gráficamente la información que se está mostrando, por ejemplo: líneas, barras, etcétera.
- Notificaciones: a qué personas de nivel superior se debe informar cuando haya un indicador por encima del máximo permitido durante un período de tiempo extendido, y que pueda derivar en un problema de impacto mayor.

Estándares en el Data Center

En la etapa de diseño del Data Center, se evalúan cuáles son los estándares que se desearán alcanzar. En ese momento, surgen muchas dudas y preguntas relacionadas con el establecimiento de cuáles son los estándares correctos para lograr satisfacer las necesidades del negocio o lo mismo ocurre si se está evaluando un Data Center de un proveedor. Los cuestionamientos sobre la calidad y los niveles de servicios ofrecidos pueden generar incertidumbre en los clientes. Esta es una tarea dificultosa ya que cumplir con las exigencias de un estándar es muy complejo y costoso. Además, en el mercado, existen muchos y no es posible cumplir con todos al mismo tiempo ya que tiene objetivos y requerimientos distintos. En el gráfico, se puede observar un resumen de todos los estándares y *frameworks* que afectan a

un Data Center, desde los elementos más básico como el cableado, hasta la gestión estrategia del Gobierno de IT y cómo se relacionan entre ellos.

Estándares en el Data Center



Los gráficos de burbujas representan subdivisiones por módulos agrupadas por color según el área de aplicación, en letra negrita se pueden el nombre de cada módulo o subdivisión. Los números representan los más estándares o Frameworks más importantes para ese módulo en particular.

En la página Web del libro podrá descargar un archivo PDF de este gráfico, para imprimir en el tamaño que desee.

Optimización

9

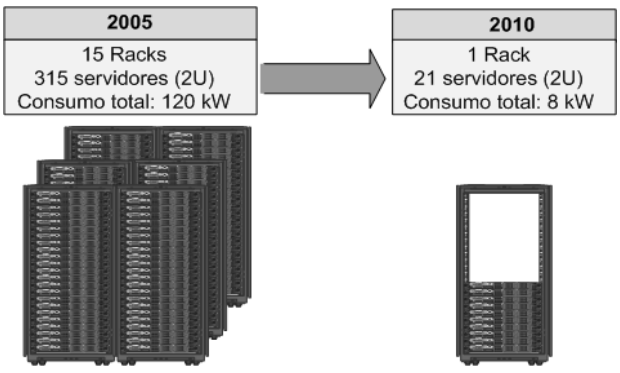
"El orden y la simplificación son los primeros pasos hacia el dominio de un tema, el enemigo real es lo desconocido".

-- Thomas Mann (1875-1955) Escritor alemán. Premio Nobel de Literatura en 1929

Las tendencias de optimización dentro del Data Center evolucionan permanentemente, y el motor impulsor de esos cambios es el avance tecnológico de los componentes que lo conforman.

Como consecuencia de ese proceso, con el paso del tiempo y la renovación tecnológica, se reduce el espacio físico ocupado y el consumo eléctrico, proporcionando la misma capacidad de procesamiento o aprovechando mejor los recursos ociosos.

Como se ve en el gráfico, a medida que pasan los años, se produce una reducción de la superficie ocupada en un 93%, y ahorro energético del 85%, manteniendo la misma capacidad de procesamiento. A su vez, aumenta la densidad de cables por cada Rack, y la capacidad de enfriamiento debe ser superior, porque la densidad es mayor.



Esto crea eficiencia, ya que la concentración de kW por Rack tiende a ser mayor con el paso del tiempo y los cambios son constantes.

Si bien el costo de la inversión inicial del nuevo equipamiento puede ser elevado, se deben evaluar cuáles son los costos totales asociados al su

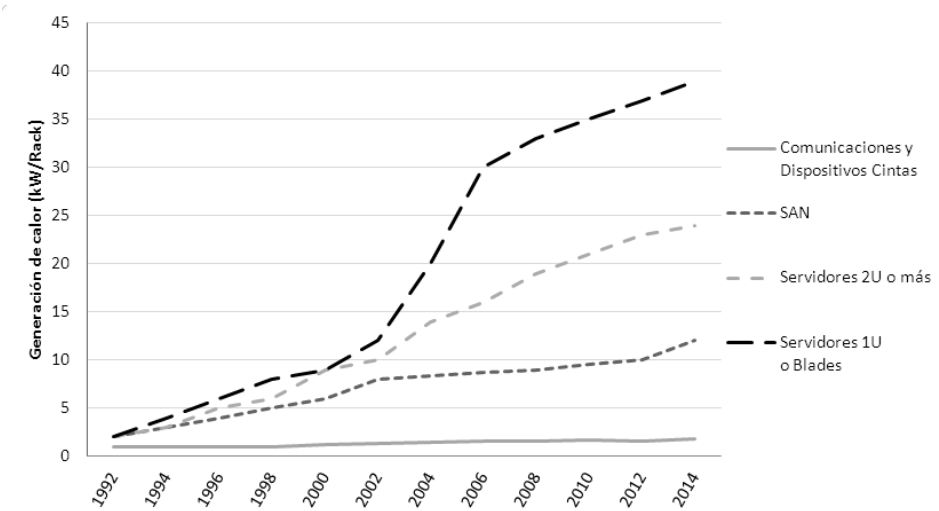
funcionamiento a lo largo de la vida útil, ya que las capacidades de los procesadores aumentan permanentemente. **La clave es encontrar el punto de equilibrio entre la inversión, la vida útil proyecta, el TCO y la disponibilidad deseada, para renovar los equipos periódicamente, y así producir ahorros a mediano o largo plazo.**

Por otro lado, existen productos como Cassatt, Power Assure, entre otros, que permiten ahorrar usando otra perspectiva, haciendo un manejo activo acorde a la utilización, permitiendo apagar o encender los servidores según la utilización o configuraciones preestablecidas.

Con las máquinas virtuales también se puede aplicar el mismo método: invernar las máquinas virtuales que no se estén usando, reduciendo el uso del procesador y disminuyendo el calor generado.

Como ya se mencionó, no todos los equipos del Data Center tienen el mismo consumo eléctrico. Los dispositivos de comunicaciones y cintas tiene un consumo bajo, los equipos de SAN también consumen poca energía. En cambio los servidores que tienen procesadores con mayor consumo sufren un incremento a medida que aumenta la cantidad de procesadores y de núcleos.

La densidad de consumo más extrema, la podemos encontrar en los servidores que ocupan 1U o en los servidores Blade. A continuación, se detalla la evolución de los equipos nombrados a lo largo del tiempo y su proyección aproximada, dado que depende específicamente del fabricante.



Dentro de los distintos tipos de SAN, por ejemplo: una unidad de gran capacidad con 192 discos SATA de 1 TB cada uno, provee una capacidad total de almacenamiento de 192 TB y solo consume 5.5 kW/h, y una unidad media con 192 discos de 146 GB cada uno, provee un almacenamiento total de 28 TB, consumiendo 5.5 kW/h.

Técnicas actuales de optimización: virtualización y nube

Virtualización

La virtualización es la técnica de abstracción de hardware que permite emular varios sistemas con características físicas similares (limitados por la arquitectura del procesador físico); de forma tal, que permita ejecutar varios recursos computacionales, llamadas máquinas virtuales. Éstas tendrán cada una su propio hardware virtual que funciona independientemente unas de otras, resultando en distintos sistemas autónomos que se ejecutan sobre un único hardware físico de gran potencia. Esto implica tener un servidor físico, un sistema operativo y un componente clave que es la capa de abstracción denominada *Hipervisor* (*hypervisor*). Estos servidores generalmente poseen dispositivos de almacenamiento de alta velocidad compartidos, simulando como si fueran varios recursos lógicos compartidos a la vez.

Por ejemplo, la virtualización de un sistema operativo es el uso de una aplicación de software para permitir que un mismo sistema operativo maneje varias imágenes de los sistemas operativos a la misma vez.

Esta tecnología permite la abstracción del hardware y el software, lo cual posibilita a su vez que múltiples sistemas operativos, aplicaciones o plataformas de cómputo se ejecuten simultáneamente en un solo servidor o PC según sea el caso de aplicación.

Si bien la virtualización es un concepto originario de los años setenta en los Sistemas UNIX, en los últimos diez años ha evolucionado de forma exponencial, gracias diversos factores:

- Velocidad de implementación.
- Hardware con mayor capacidad, en especial el incremento en procesamiento.
- Estabilidad.
- Flexibilidad, agilidad y escalabilidad.
- Portabilidad.

- Aprovechamiento de la capacidad ociosa.

Por todas estas razones, la mayoría de las empresas ha optado por utilizar tecnologías de virtualización, que a mediano y largo plazo incurren en una reducción de costo importante. Por eso, hoy en día no es raro ver empresas que tiene el cien por ciento de sus servidores virtualizados; y aquellas que están incursionando, lo hacen cada vez con más profundidad. Con una compra de 20 servidores potentes y una SAN con espacio suficiente pueden virtualizar más de 500 servidores de tamaño chico o medio, con muchas ventajas de administración provistas por la solución.

Por ello, la mayoría de los gigantes informáticos han desarrollado o adquirido productos de virtualización para poder explotar el mercado, como por ejemplo ESX de VMWare (dominante y precursor del mercado), Hyper-V de Microsoft, Xen Server de Citrix, Virtual Box de Oracle, Open Stack de Open Source, entre otros.

Aquí también entra en juego la **batalla del licenciamiento** entre las grandes empresas, ya que con el fin de imponer un producto en el mercado, más allá de sus características técnicas que estos ofrecen, las empresas salen a combatir buscando imponer sus productos a partir de otra herramienta decisoria: el precio de la licencia.

Por eso las empresas están cambiando permanentemente la forma en que se cobran las licencias de sus productos. Por ejemplo: el precio fijo por producto adquirido, precio de licencia por cantidad de memoria física, precio por procesador físico, precio por cantidad de núcleos, precio por cantidad de sesiones conectadas, etcétera. La competencia es feroz y no termina, por ello todo el tiempo están surgiendo nuevas formas de licenciamiento que pueden hacer cambiar el mercado y la dirección de los competidores.

Si bien la virtualización simplifica la tarea de los administradores de los servidores, y permite agilizar el área de IT con menores costos, para los responsables de la infraestructura de los Data Centers es un arma de doble filo, ya que para aprovechar la solución mencionada de forma ideal, se deberá reemplazar el hardware existente, comprando equipos más potentes y pequeños, que también generan más calor en una superficie menor. Además, éstos pueden requerir actualización en la infraestructura de red ya que en estas soluciones requieren redes de alta velocidad y grandes capacidades de almacenamiento para aprovechar todas las ventajas que ofrecen los productos.

Servidores en la nube (Cloud Computing)

Nube, nube, nube es una palabra que escuchamos todo el tiempo, pero no queda claro qué es:

- ¿Es un término de moda? - **Puede ser.**
- ¿Puede ser una solución para las empresas? - **Sin dudas**.
- ¿Es la solución para todo? - **No**

La nube es básicamente el utilizar servicios de algún proveedor a través de la red, pero a menor costo, como podría ser algún tipo de almacenamiento: Web Hosting, procesamiento, servidores dedicados, conectados a la red interna de la empresa o Internet.

Hoy en día los gigantes de la informática como IBM, Microsoft, Google, Oracle, AWS Amazon Web Services, Go Grid, Rack Space, Go Daddy, Sugarsync, Wuala, Salesforce, iCloud, entre otros, son solo algunos de los proveedores que están ofreciendo servicios a través de Internet.

- Ventajas
  - Simplificación: no hay problema de licenciamiento ni en relación a la infraestructura, espacio, UPS, enfriamiento, etcétera.
  - Agilidad y velocidad para adaptarse a los cambios del negocio.
  - Portabilidad: acceso desde computadoras, teléfonos móviles, tabletas, etcétera.
  - Baja inversión: hay proveedores que ofrecen precios de centavos de dólar por hora de uso con licencia incluida. Si el servidor está apagado, no se paga.
  - Menores costos operativos: se adquieren los servicios en función a la demanda real.
  - Disminuye los riesgos de inversión.
  - Ofrece la posibilidad de enfocar los esfuerzos al éxito del negocio.

- Desventajas
  - **Dependencia absoluta de la disponibilidad de acceso a Internet,** salvo en caso de tener un enlace dedicado con el proveedor. Por ello es recomendable tener dos proveedores independientes distintos, si la cantidad de servicios en la nube es lo suficientemente importante para justificar el gasto.
  - Riesgo con los datos sensibles. **Seguridad delegada.**
  - Los servicios dependen de la "salud" tecnológica y financiera del proveedor.
  - Complejidad de implementación.
  - Escalabilidad a largo plazo.

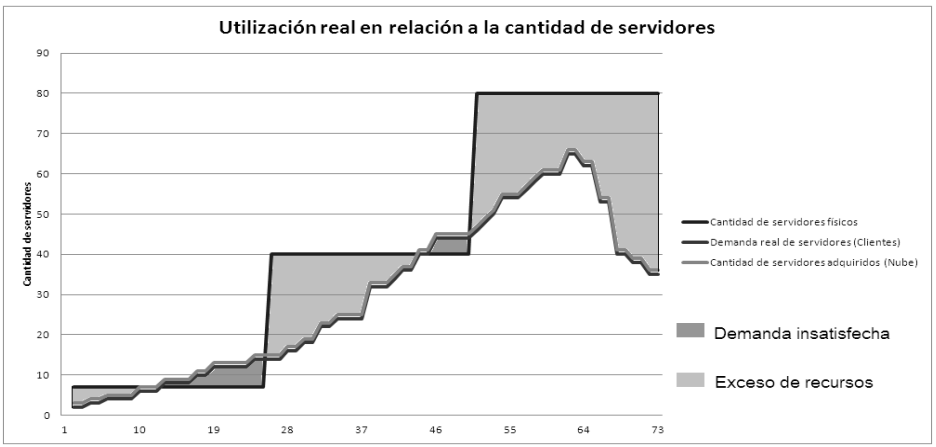
En muchos países, en particular en América Latina, adquirir un servidor puede ser un proceso bastante lento, debido a distintos factores como son las restricciones aduaneras, burocracia, distancia, etcétera. Según el país de destino, desde el momento en que se aprueba la orden de compra hasta que se recibe el servidor pueden pasar de entre dos y cuatro meses, más el tiempo que pueda llevar la instalación. Realmente es un tiempo excesivo teniendo en cuenta la velocidad de los mercados y los negocios a escala mundial. Por eso la posibilidad de adquirir un

servidor en la nube, en unos pocos minutos, y con una inversión extremadamente baja es una gran alternativa.

Con respecto a la seguridad de los datos, muchas veces los responsables de tomar la decisión son reacios a mover los servicios a la nube, ya que delega la seguridad, lo cual es comprensible. Ahora bien, muchos proveedores ofrecen condiciones que garantizan los medios necesarios para protegerlos adecuadamente, con medios de encriptación, certificados digitales, certificaciones internacionales sobre la infraestructura física, etcétera.

Supongamos un caso hipotético con un enfoque tradicional donde se deben adquirir los servidores, resulta poco flexible la forma de acompañar la demanda de crecimiento del negocio. Aun podría ser peor, si existe un exceso de recursos que estén ociosos, generando pérdidas, y se podría dar el caso donde la cantidad de equipos disponibles no fuera suficiente para satisfacer la demanda, haciendo que el negocio perdiera dinero u oportunidades. Viendo esta tendencia de incremento en la demanda, y para no correr riesgos, decidimos comprar más servidores, llegando a un total de 40 para la semana 28. Una vez que los nuevos servidores llegaron, están instalados y funcionando, volvemos a los mismos problemas una vez más: capacidad ociosa durante casi 20 semanas, lo que representa una gran pérdida de dinero.

En cambio, un enfoque basado en la nube permite acompañar el crecimiento de la demanda de forma más rápida y con una mínima inversión inicial, incluso algunos proveedores ofrecen servicios de autoabastecimiento, permitiendo en forma automática crecer en cantidad de servidores no solo por semanas, sino por días y hasta por horas.



Un caso real analizado por AWS mostró que la empresa Animoto (videoclips) lanzó una modificación en su página de Facebook, haciendo que la cantidad de visitas se potencie gigantescamente, incrementando la demanda de los usuarios y

logrando pasar automáticamente de 50 equipos a 5 000 en solo tres días; pero, al cabo de una semana, bajó la demanda y solo funcionaban 2 000 servidores. ¿Se imagina adquirir 4 950 servidores en tres días, y que para peor, al cabo de una semana, 3 000 estén de sobra? Sin duda la principal ventaja competitiva de los servicios basados en la nube es la rápida adaptabilidad al negocio y la baja inversión.

En una nota publicada por el diario *Wall Street Journal*, en agosto del 2011, Marc Andreessen, ex programador y creador del navegador Netscape en 1994[1], explica las ventajas para los inversionistas de los servicios basados en nube para el inicio de nuevos proyectos donde la incertidumbre es muy grande.

Antiguamente para poner en marcha un proyecto nuevo se requería una inversión inicial promedio de 150 000 dólares, pero desde la aparición de los servicios nube, se puede iniciar un nuevo proyecto con solo 1 500 dólares, lo que permite reducir el riesgo, disminuir la inversión inicial, simplificar la decisión y poder financiar muchos más proyectos.

Según una investigación de Gartner del año 2006, en promedio, sobre el presupuesto total de IT, el 80% se destina al mantenimiento de la infraestructura y solo el 20% se destina a innovación. Las soluciones de nube pueden ser una ayuda en la reducción de costos, pudiendo destinar más fondos a la creación e innovación.

La tendencia como solución ya es una realidad. En una encuesta realizada por el Uptime Institute en 2012 sobre 1 100 casos, muestra un crecimiento en el último año contundente. En 2011, el 16% de los encuestados estaba usando servicios de nube pública (servidores expuestos a Internet como los servicios Web); y el 35%, nube privada (servidores conectados a la red interna de la empresa por medio de un túnel VPN[2] o enlace directo con el proveedor). En 2012, el 25% de los encuestados ya están utilizando servicios de nube pública, y el 49% servicios de nube privada.

En otra encuesta realizada entre Acronisy PonemonI nstitute en 2012, arroja resultados más contundentes aún sobre la adopción de esta tecnología. Sobre 6 000 encuestados en todo el mundo, el 83% respondió que ya tenían algún tipo de servicio en la nube, aunque en promedio general solo representaba el 19% de su infraestructura, lo que marca una clara tendencia para los próximos años.

---

[1]Hacia 1996 poseía casi el 80% del mercado de los navegadores, pero por diversos motivos no siguió prosperando; luego, sirvió de base para el desarrollo del proyecto Mozilla. Actualmente es un empresario que se dedica a financiar proyectos relacionados con tecnología

[2]Virtual Private Network o red privada virtual. Es una tecnología de red que permite una extensión segura sobre una red pública no controlada como lo es Internet.

Además muchos de estos proveedores ofrecen en sus instalaciones certificaciones en sus instalaciones físicas que son realmente muy difíciles de conseguir, como:

- SAS 70 II: Relacionada con SOX (EE. UU.).
- FISMA[3]: asegura que organismos federales de los Estados Unidos (FBI, NASA, CIA, etcétera) puedan alojar sus servidores en Data Centers de terceros, de manera segura.
- HIPAA[4]: asegura la protección de los datos médicos de las personas de los Estados Unidos.
- ISO/IEC 27001: define los requerimientos necesarios para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad informática.
- PCI DSS[5]: certificación para entidades financiaras que operan con pagos electrónicos como las tarjetas de crédito y los medios de pago virtuales.

El talón de Aquiles de la nube es la latencia. El no disponer de una infraestructura de red que sea capaz de satisfacer las necesidades, puede descartar el uso de los servidores basados en la nube.

Data Center ecológicos

Hoy en día se escucha y leen cientos de artículos que hablan de Data Centers ecológicos, reducciones de emisiones, optimización ecológica etcétera.

La iniciativa voluntaria de la ONU proclamada en 1999 define los diez principios del "Pacto Global" en particular el noveno punto dice: "las empresas deben favorecer el desarrollo y la difusión de tecnologías respetuosas con el medio ambiente". Es por ello que para lograr un equilibrio y armonización entre dicha afirmación y el mundo de los negocios cuyo objetivo principal es la rentabilidad se define una estrategia a nivel directivo de la empresa de "triple resultado" o conocida como: PPP: que posee tres dimensiones que interactúan para lograr un medio ambiente sustentable y genuino (PROFIT - Dimensión económica; PLANET -Dimensión ambiental; PEOPLE - Dimensión social).

[3]Federal Information Security Management Act, publicada en 2002, en los Estados Unidos.
[4]Health Insurance Portability and Accountability Act, publicada en 1996, en los Estados Unidos.
[5]Payment Card Industry Data Security Standard (estándar de seguridad de datos para la industria de la tarjeta de pago).

Pero ¿cuál es impulsor de dicha tendencia? Es que el gerente de finanzas quiere gastar menos en electricidad o es que el gerente de marketing quiere hacer una campaña de RSE (responsabilidad social empresaria) por reducción de contaminación ambiental por medio de los instrumentos de gestión como: SA 8000; ISO 14000; ISO 26000.

La respuesta correcta es: ambas. Ambos motivos son válidos y sirven como impulsores en la búsqueda de la innovación tecnológica para alcanzar esa reducción de emisiones contaminantes.

Beneficios de la evolución ecológica

Evolución	Desde →	Hacia
Financiero	• Precio creciente de la energía • Presupuestos de IT ajustados • Reducción en el crecimiento de IT	• Habilidad para ver consumo de energía básico • Reducción de costos ahorrando energía • Presupuestos relajados que permiten crecimiento
Operativo	• Data Centers de alta densidad • Analizar los costos de electricidad y enfriamiento • Modificaciones constantes	• Mayor rendimiento por kW aumentando la productividad • Mejorar las metodologías de enfriamiento y el promedio de utilización eléctrica • Extender la vida útil de las instalaciones actuales
Ambiental	• Responsabilidad social empresaria • Baja reputación de la pública • Mejora de la moral de los empleados	• Reducción de uso energético y emisiones • Aumento de la imagen pública • Contribución positiva social al medio ambiente para crear un mejor ambiente laboral

Existen muchas organizaciones dedicadas a analizar cuáles son las tecnologías que se pueden utilizar para reducir las emisiones y cuáles son los objetivos que se deben cumplir para convertirse en una entidad certificada como lo que ocurre con los electrodomésticos, por ejemplo, que llevan una etiqueta que indican el grado de eficiencia eléctrica del equipo clasificados por el programa de *Energy Star* con letras de la A a la H, donde la A es la mejor y la H es la peor.

Aquí se enumeran solo algunos organismos internacionales que trabajan en normativas para Data Centers y edificios ecológicos:

- European Direction Energy performance in Buildings, creado en 2003, establece parámetros de construcción sustentable.
- The Green Grides una organización sin fines de lucro conformada por las empresas líderes en tecnologías que tiene como objetivo establecer métricas para medir la eficiencia ambiental.
- Energy Star (EPA): Data Center Energy Efficiency Initiatives, publicado en 2010.
- LEED (Leadership in Energy & Environmental Design) desarrollado por el US Green Building Council, en 1998. Se espera que hacia finales de 2013, esta organización publique una normativa especial para Data Centers, actualmente se encuentra en versión borrador.
- BREEAM (BRE Environmental Assessment Method). Evaluación ambiental de edificios.
- ANSI/ASHRAE 90.1: estándar de energía para edificios publicado en 2010.
- Climate Change Bill (Gran Bretaña–2007).

Para evaluar el desempeño eléctrico de un Data Center, uno de los valores más comunes es el PUE(PowerUsageEffectiveness): métrica que mide el valor de la eficiencia eléctricaen relación al consumo eléctrico total. Fue establecido por la organización *The Green Grid* (`http://www.thegreengrid.org`), en particular por uno de sus directores,Christian Belady, y su fin es establecer un parámetro para identificar qué tan eficiente es el consumo actual de los equipos.

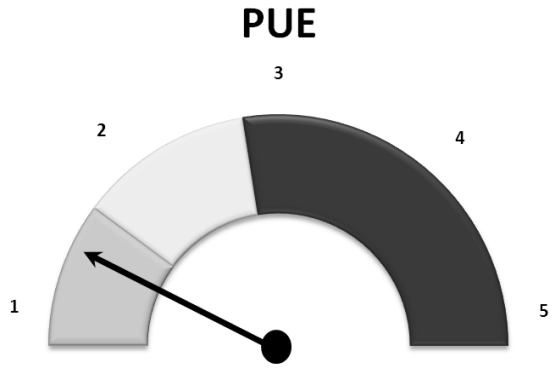
$$\mathbf{PUE} = \frac{\text{Consumo eléctrico total}}{\text{Consumo equipos de IT}}$$

Ejemplo:

$$PUE = \frac{200\ kW\ (Consumo\ eléctrico\ total)}{100\ kW\ (Consumo\ equipos\ de\ IT)} = 2.0$$

Mientras menor sea el valor PUE, mejor será el aprovechamiento eléctrico, lo que se traduce en menores costos y menores emisiones de CO_2, permitiendo reducir la llamada “huella de carbono”.

El valor perfecto sería un PUE = 1.0. Este número resulta prácticamente imposible de alcanzar, ya que quiere decir que toda la energía consumida por los equipos es igual a la ingresada en el Data Center para que funcione completamente, y donde la refrigeración, UPS, etcétera, no tuvieron consumo eléctrico. Esto es realmente difícil de que suceda.



Un PUE = 2 representa que los sistemas que forma la infraestructura consumen los mismo que todos los equipos de IT.

En el mercado de los Data Centers, los valores reales de PUE oscilan entre 1.2 y 4. Existen algunos casos extremos que logran PUE = 1.02, como es el Data Center de Portlane, en la ciudad de Nacka, Suecia, que emplea las más modernas tecnologías, *free cooling*, *flyweel* UPS, paneles solares en el techo, entre otras. Pero la realidad es que en promedio los Data Center tienen un PUE=1.8, sobre la base de un estudio realizado por el Uptime Institute, en 2011, sobre 500 Data Centers. Coincidentemente, otro estudio de EPA, en 2009, sobre 100 Data Centers analizados arrojó un promedio de PUE=1,9.

Las grandes empresas como Yahoo, Facebook, Microsoft o Google entre otras han fijado sus objetivos de PUE en un rango de 1.07 y 1.2, aunque si es ≤ a 1.5 se considera un valor aceptable. Valores superiores a 2.0 ya son considerados ineficientes, quizás años atrás, ese valor podría ser aceptable, pero las tecnologías han evolucionado hacia la optimización, permitiendo disminuir el valor del PUE en forma considerable.

Categoría	PUE
Equipos IT	1,2
Refrigeración	0,6
UPS	0,4
Iluminación	0,1
Transformadores	0,1
Ventiladores	0,2
Total	**2,6**

Como una subdivisión de la medición anterior, la organización realizó una clasificación diferencial del PUE en cuatro categorías (de 0 a 3) con el objetivo de poder identificar donde podría haber pérdidas de eficiencia con mayor exactitud, que se detallan a continuación:

PUE$_0$: se calcula igual que el PUE, pero se toma el pico del consumo eléctrico sobre el consumo eléctrico de los equipos de IT a la salida de la UPS (ambos en el último año).

PUE$_1$: se calcula igual que el PUE, pero se toma el consumo eléctrico total acumulado sobre el consumo eléctrico de los equipos de IT acumulados a la salida de la UPS, ambos valores medidos en el último año.

PUE$_2$: similar al anterior, pero la carga de los equipos de IT se toma a la salida de la PDU.

PUE$_3$: similar al anterior, pero la carga de los equipos de IT se mide en la entrada a ellos.

Complementariamente, existe otro parámetro que se utiliza en la evaluación de la eficiencia eléctrica, derivado del PUE, que mide el porcentaje de eficiencia llamado DCiE (*Data Centre infrastructure Efficiency*).

$$\textbf{DCiE} = \frac{\text{Consumo equipos de IT}}{\text{Consumo eléctrico total}} * 100 \qquad \text{que equivale a } \textbf{DCiE} = \frac{1}{\text{PUE}} * 100$$

Si bien la métrica original es PUE, la cuantificación de DCiE fue creada para entender más fácilmente la eficiencia del Data Center. Por ejemplo, un valor DCiE de 28% equivale a un PUE de 2.8. Por ejemplo, si tenemos una factura por consumo eléctrico de 1 000 dólares, sabremos que 280 dólares fueron los realmente consumidos por los equipos de IT.

A pesar de que ambas métricas fueron diseñadas para calcularse anualmente, es posible analizarlas semanal o mensualmente según las necesidades, en caso que se quiera hacer un estudio minucioso que así lo demande.

Adicionalmente, existe otra métrica más reciente, de la misma organización, para evaluar la eficiencia del consumo de agua en los equipos de refrigeración en relación a la cantidad de kW/h. Es conocida como **WUE** (Water Usage Effectiveness) y se define como el uso anual del agua dividido por la cantidad de energía utilizada por el equipamiento TI. Las unidades de WUE son litros por kW consumidos por hora.

$$\textbf{WUE} = \frac{\text{Uso de agua anual (litros)}}{\text{Consumo equipos de IT (kW/h)}}$$

Algunas empresas han avanzado en el tema del reciclaje de agua utilizando "aguas grises", no aptas para el consumo humano, pero que sí pueden servir para la refrigeración como el agua de lluvia.

El agua de la torre se evapora, en especial en verano, pudiendo dejar rastros de sustancias sólidas disueltas y contaminantes. Cuanta más agua se evapora, la

concentración de sólidos en el volumen restante de agua es mayor, lo que finalmente causará una acumulación en los tubos de condensación y en las placas de intercambio de calor, pudiendo causar daños en las cañerías a mediano y largo plazo.

CCF es una métrica creada por la empresa Upsite, que se utiliza para gestionar la eficiencia de refrigeración en el Data Center, por las siglas de *Cooling Capacity Factor*. Se calcula mediante el cociente entre la capacidad total de refrigeración sobre la carga de consumo de los dispositivos de IT (a la salida de la UPS) aumentada en un 10% (ese 10% adicional está atribuido otros factores externos que interfieren en el cálculo, como ser: iluminación, personas, estructura, etc.).

$$CCF = \frac{CapacidadTotalRefrigeración}{ConsumoEléctricoIT(SalidaUPS) * 1{,}1}$$

ERE es otra métrica creada por *The Green Grid* utilizada para calcular la eficiencia de la reutilización de la energía (*Energy Reuse Effectiveness*), como por ejemplo podría ser la reutilización del calor generado por los equipos para aclimatar las instalaciones edilicias. Es una fórmula similar al PUE, pero al consumo eléctrico del Data Center (en el numerador) se le resta el ahorro de energía eléctrica generado por la reutilización.

$$ERE = \frac{ConsumoEléctricoEquiposDataCenter - EnergíaReutilizada}{ConsumoEléctricoIT}$$

Para un nivel de detalle mayor y orientado con un enfoque puramente ecologista, existe otra métrica relacionada a esta llamada CUE (*Carbon Usage Effectiveness*), en donde se analiza la cantidad total de emisiones de CO_2 causada por los equipos del Data Center sobre el consumo eléctrico de los equipos de IT.

UUR: por las siglas de Utilización Unitaria de Rack, consiste en evaluar el porcentaje de utilización de cada rack medido en "U" o unidades de rack. Esta información es útil para comprender la utilización total y poder asociar esa utilización con el consumo o la generación de calor que provoca cada rack analizando si el flujo de refrigeración es el correcto, ya que lo no es lo mismo un rack de comunicaciones que solo tiene *patchears* que otro donde hay cinco cajones de servidores *blade*.

Por cada uno de los racks del Data Center, se debe hacer este cálculo:

$$\text{UUR} = \frac{\text{"U"}Disponibles - \text{"U"}Utilizadas}{\text{"U"}Disponibles} * 100$$

La organización LEED ofrece una certificación de eficiencia sobre la base de una tabla de puntos que va de 1 a 100, a menor contaminación ambiental producida, mayor es la cantidad de puntos otorgada, considerando emisiones, sustentabilidad, tipos de materiales usados, etcétera:

- **Certificado:** 40 a 49 puntos.
- **Plata:** 50 a 59 puntos.
- **Oro:** 60 a 79 puntos.
- **Platino:** más de 80 puntos.

El programa de *Energy Star* también tiene un sistema de clasificación por puntos, bajo principios similares a los de LEED:

- **1 a 49 puntos:** indica que el Data Center necesita inversiones importantes en equipos de IT eficientes para reducir emisiones y mejorar la eficacia eléctrica.
- **50 a 74 puntos:** es una buena calificación, pero aún se pueden hacer mejoras desde el punto de vista operacional combinado con actualizaciones menores.
- **75 a 100 puntos:** cumple con las recomendaciones de un Data Center ecológico.

Claves

Las UPS deben tener una eficacia superior al 95%. Mientras que en los equipos que funcionan a 220/240 V tienen una eficacia del 2% al 3.5% más que los que funcionan a 120 V. Multiplicado por cientos de servidores puede ser una cifra muy influyente sobre la optimización total.

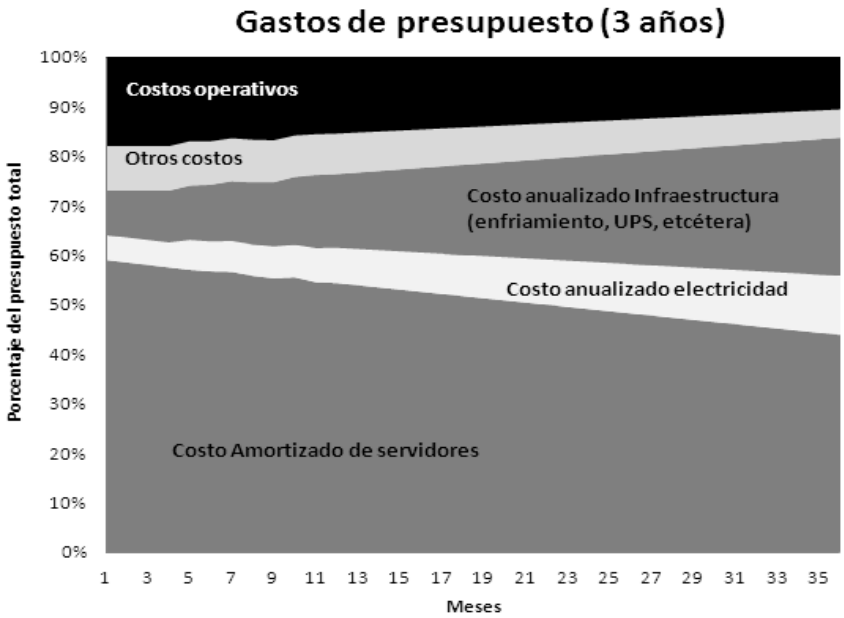
Buscar la mejor eficacia posible en todos los componentes: servidores, procesadores, PDU, UPS, transformadores, equipos de refrigeración, ventiladores, etcétera. Por más pequeña que sea la diferencia debe tenerse en cuenta al momento de la compra, ya que a lo largo de los años puede tener un impacto significativo en los costos de operación.

La organización ISO ha comenzado a evaluar el PUE como estándar internacional para el año 2013.

Costos

Cuando se habla de costos de construcción de un Data Center, hoy en día son costos muy distintos de aquellos de edificación de años atrás. Según datos del

Uptime Institute, en 1995 construir un Data Center de 2 800m^2, en los Estados Unidos, podía costar 20 millones de dólares, pero hoy en día debido a las necesidades tecnologías de las empresas y la evolución de los materiales que se mencionaron en capítulos anteriores, los costos son otros, por lo que esa cifra podría aumentar hasta los 300 millones de dólares, lo que equivale a más de 50 000 dólares por Rack.



Además, los costos operativos, en especial el consumo eléctrico, son fundamentales al momento de tomar decisiones de compra, sea cual sea el equipamiento que se está evaluando.

Según una encuesta publicada en 2006, por la consultora internacional IDC (International Data Corporation), el consumo eléctrico de los servidores producidos en el 2000, se duplicó con respecto a los modelos producidos en 2005, y esa es una tendencia que se mantiene en alza.

En la práctica se ven muchos Data Centers que están sobredimensionados y utilizan muchos más recursos (UPS, enfriamiento, Racks, etcétera) de los que realmente necesitan para operar los equipos de IT, generando un emisiones y desperdiciando dinero de forma innecesaria.

Para ajustar los costos de la infraestructura del Data Center adecuadamente a las necesidades de crecimiento del negocio, al momento de la decisión de la compra la clave es seleccionar elementos con capacidad de **escalabilidad**, ya que comprar por

demás implica una inversión excesiva en la etapa inicial y gastos de funcionamiento enormes en la operatoria hasta el momento en que se utilice toda la capacidad. La opción inteligente y rentable es adquirir los recursos necesarios para cada etapa y prever con anticipación las posibles ampliaciones en capacidad que se requieran.

Según una encuesta realizada en 2005 por AFCOM (Association for Computer Operation Managers), los requerimientos energéticos de los Data Centers aumentan en promedio un 8% por año; y para los de gran tamaño, los aumentos pueden ser de hasta el 20%. Esta es una tendencia que continua en aumento debido a todos los factores mencionados anteriormente. Estos datos no son un detalle menor al momento de seleccionar equipos, ya que la tendencia en muchos países es que el costo por kW provisto por la red eléctrica tendrá una tendencia creciente año a año, en especial cuando muchos Data Centers tienen previsto crecer en los próximos años.

Finalmente, la consultora Environmental Leader estima que el mercado de los Data Centers ecológicos se triplicará en los Estados Unidos hacia el fin del período 2010-2015 con una inversión total del 14 mil millones de dólares, lo que constituirá el 28% del mercado.

Desafíos actuales

La concentración de equipos en espacios reducidos es una tendencia de crecimiento continuo, debido a:

- Las mejoras de las capacidades de los componentes, que brindan mayor poder de cálculo en menor espacio.
- Los mayores requerimientos de enfriamiento, por mayor concentración kW/Rack.
- Los menores precios en proporción con dichas capacidades.
- Los cables de mayores velocidades a costos más convenientes.
- La cantidad de información electrónica que se requiere almacenar tiene una tendencia de crecimiento sostenido y en algunos casos se requiere mantenerla por mucho tiempo debido a disposiciones legales. Solo por citar un ejemplo, la Bolsa de Nueva York genera 2 000 GB de información por día que debe ser resguardada por años.
- Menores costos en los dispositivos SAN. Si bien la inversión inicial puede ser elevada, ya que además requiere adquirir la infraestructura de fibra, el costo almacenamiento por GB es cada vez menor, por ello la zona de Data Center destinada para la SAN debe tener espacio para crecer, ya que es fundamental para que la virtualización se pueda llevar a cabo.

Por ese motivo, la limitaciones en los Data Centers ya no son más el espacio físico, sino el consumo eléctrico y la capacidad de enfriamiento.

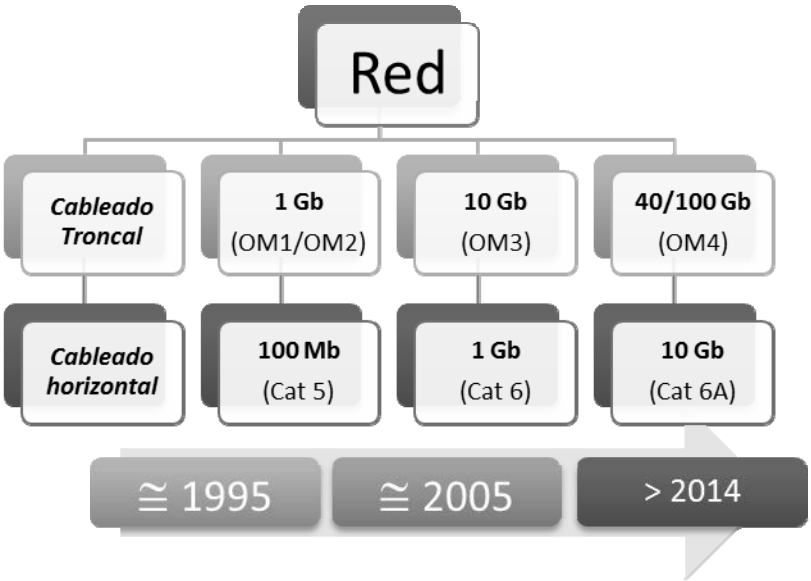
Con respecto a los desafíos relacionados con la conectividad, muchas organizaciones necesitan actualizar su cableado estructurado antes de avanzar en sus proyectos de virtualización, o al menos en las redes troncales, lo que implica una inversión considerable.

- Los organismos internacionales de estandarización están estudiando cómo fabricar en cobre cables con capacidad de 40 a 100 Gbps, logrando una reducción de por lo menos cinco veces comparada con la fibra óptica. No obstante, en esta situación, a veces los tiempos de aprobación de los estándares son demasiado largos y están por detrás de los avances tecnológicos.
- Virtualización: si consolidamos 10 servidores que trabajaban en 1 Gbps en un mismo servidor físico, debemos realizar una actualización del cableado a 10 Gbps para evitar un embudo de tráfico de red.
- La densidad de los Data Centers está en crecimiento, por ello, es otro factor crítico a considerar, especialmente en la fase de diseño. Antes se operaban entre 3 o 6 kVA por Rack, y hoy en día se puede llegar a 20 kVA con facilidad.

La reducción de los costos de las SAN, la aparición explosiva de nuevas tecnologías como iSCSI[6], la virtualización y el diseño de nuevos cables hace que las redes cada vez requieran mayor ancho de banda, y las aplicaciones hacen que un buen modelo de red troncal sea aquel que se pueda adaptar. Ya no basta con cumplir con un estándar.

Lo que quizás hace unos años parecía suficiente, dentro de poco tiempo puede ser un cuello de botella de red, porque la evolución de la tecnología es permanente.

[6]Abreviatura de Internet SCSI: estándar que permite el uso del protocolo SCSI para dispositivos de almacenamiento de alta velocidad, usando la red LAN sobre protocolo TCP/IP. Tiene menor costo que la red de fibra, y almacenamiento por SAN con un rendimiento aceptable.

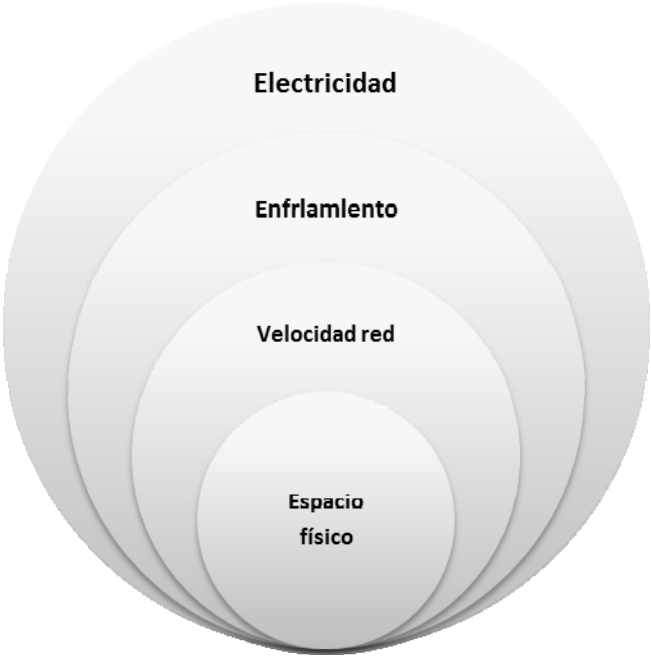


Pese al decremento de precios durante los últimos años, aún hoy las redes de fibra óptica resultan bastante costosas en algunas configuraciones, por ejemplo, para redes de 10 Gb, el costo total de una instalación cobre Cat. 6A es el 40% de una instalación de fibra. Aunque, por otro lado, una fibra de 13 mm tiene una capacidad similar a 144 cables Cat. 6 y un consumo eléctrico mucho menor.

Para definir cuál es el método enfriamiento seleccionado para el Data Center se deberán considerar muchos factores, como:

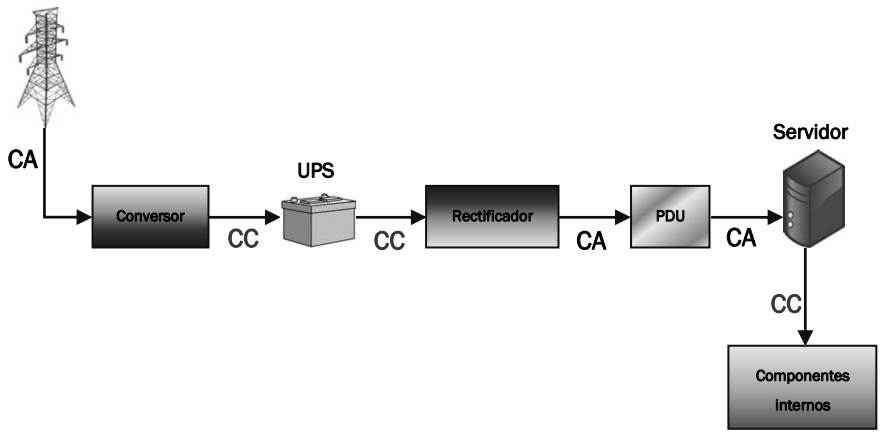
- Costo inicial de compra.
- Costo operativo.
- PUE objetivo para el Data Center.
- Costos de mantenimiento y repuestos.
- Densidad de consumo kW/Rack promedio del Data Center y proyección a futuro.
- Analizar la posibilidad de encapsular los pasillos si la densidad es alta.
- Sobre la base de la criticidad, calcular la cantidad de equipos redundantes.
- Capacidad de escalabilidad.

En resumen, las principales preocupaciones de los responsables de Data Centers para los próximos años son:



¿Existe una mejor manera optimizar el uso de la energía eléctrica?

La respuesta es compleja, pero podríamos decir que si es posible, ya que la manera de lograrlo sería mejorando la eficiencia, y eso se puede hacer eliminando los puntos donde se realizan las conversiones de CA/CC y viceversa, veamos un ejemplo típico de cómo fluye la electricidad en un Data Center:



La disputa de qué tipo de corriente eléctrica es mejor, si la alterna o la continua tienen una larga historia. A fines del siglo XIX, Thomas Edison impulsaba la corriente continua que había descubierto, por el otro lado Nikolo Testa, promovía la corriente alterna que había inventado, el proceso donde una de estas dos alternativas se impondría fue llamado "La guerra de las corrientes". Como ya se explicó anteriormente, estas son muy distintas, pero ambas deben convivir, ya que proporcionan funcionalidades diferentes debido a sus características, en resumen:

- La CC se impuso en lugares donde se requiere almacenar energía, como: pilas o baterías, y en equipos que requieran baja potencia para funcionar, pero su principal defecto es que no se puede transportar en líneas de alta tensión por grandes distancias ya que las pérdidas son muy grandes.
- Como contraparte la CA, si es capaz de recorrer grandes distancias sin sufrir pérdidas de tensión, pero el problema es que no se puede almacenar para utilizarla en otro momento.

Como se puede ver en el gráfico anterior, los componentes internos de los equipos de IT utilizan CC para su funcionamiento, pero para que la corriente llegue hasta allí, debe pasar por muchos pasos, desde la red eléctrica (CA), convertirse a (CC) para poder almacenarse en la UPS, luego se rectifica la corriente para llegar a la PDU (CA), desde allí llegará a los equipos y por último la fuente interna la transformará por última vez (CC) para alimentar a los procesadores, memorias, y otros circuitos internos.

Cada una de estas transformaciones de corrientes genera pérdidas de eficiencia, que se transforman en pérdidas económicas. Pero ¿qué pasaría si el proveedor de red eléctrica suministrara CC, cargara la UPS, pasara por la PDU y llegara a los equipos directamente sin transformaciones? Este escenario sería óptimo, ya que las pérdidas dentro del Data Center serían muy pocas y la eficiencia sería muy alta. Pero en la práctica resulta muy difícil que eso pueda suceder por diversos factores:

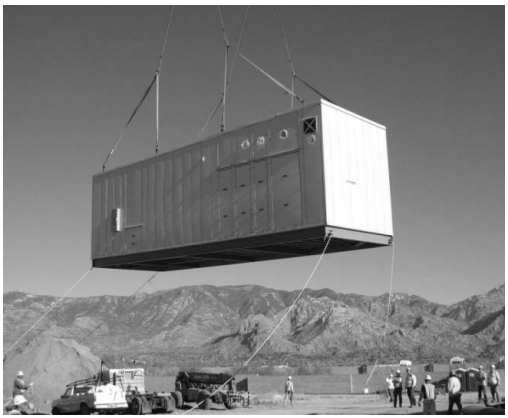
- Prácticamente, no existen proveedores de red eléctrica que suministren CC, por la deficiencia que presenta al transportarlo en largas distancias.
- Hay muy pocos proveedores en el mercado de IT que ofrezcan equipos para ser alimentados directamente con CC.

Otro desafío para los responsables de los Data Centers es un límite de actualización en el plano de las aplicaciones heredadas, también llamadas *legacy*, que consiste en aplicaciones que se siguen utilizando en la empresa, pero que no tienen reemplazo moderno y han quedado ya obsoletas por la tecnología con las que fueron construidas. Esta situación puede retrasar ese proceso evolutivo, especialmente, para integrarlas con soluciones móviles como *tablets* y *smartphones*.

En ese sentido, según un estudio de la empresa RICOH, en 2012, analizó 1 075 casos en varios países Europa de empresas chicas, medias y grandes, de las

cuales el 79% de los gerentes de IT reconocía no poder actualizar las aplicaciones para adaptarse a tecnologías móviles, porque aún continúan utilizando aplicaciones arcaicas para sus operaciones diarias.

Data Center modulares



Los Data Centers modulares son similares a una caja prefabricada que provee una solución integrada de los elementos básicos del Data Center: refrigeración, UPS, electricidad, cañerías, Racks, etcétera.

En sus orígenes, en los años noventa, en pleno auge de las empresas ".com" surgieron como alternativa a los Data Centers tradicionales. Están concebidos y diseñados como una solución en aquellos sitios donde se requiera gran velocidad de implementación.

Poseen una forma similar a un contenedor que se utiliza para transportar mercadería en barcos, e incluyen la infraestructura completa y los medios necesarios para almacenar los equipos. Dichos módulos se pueden ir anexando de acuerdo con la necesidad de crecimiento, unos con otros, armando un conjunto de bloques que se pueden integrar entre sí, y conformando un Data Center completo como, por ejemplo: Sun Modular Data Center S20 de Oracle fue la continuación del Project Blackbox de Sun Microsystems, o el POD Performance Optimizad Datacenter de HP, PMDC Portable Modular Data Center de IBM, o el MDC Modular Data Center de Dell entre otros.

Si bien en el mercado internacional tienen muy poca presencia, en los Estados Unidos, el mercado de este tipo de soluciones prefabricadas tiene una leve tendencia de crecimiento en sectores pequeños y medios, en especial, donde las condiciones de locación física son dificultosas o la velocidad de implementación es crítica.

- Ventajas
  - Agilidad y gran velocidad de implementación (semanas).
  - Flexibilidad.
  - Simplicidad.
  - Escalabilidad para crecimiento.

  - Inversión inicial baja.
  - Excelente solución para lugares de difícil acceso, por ejemplo, zonas de exploración minera o petrolera.

- Desventajas
  - Difícil adaptación en caso de decrecimiento.
  - Dependencia del proveedor (pocos proveedores, y es difícil cambiar una vez elegido).
  - Poca disponibilidad de cobertura a escala mundial.

Viabilidad técnica para alojar servidores en Data Centers externos (Housing)

¿Por qué alojar los servidores que contienen nuestra información a un proveedor, confiándole nuestro activo más preciado?

La velocidad de implementación de nuevos negocios; el incremento en la disponibilidad de los servicios que están funcionando actualmente; puede que se requiera una inversión muy importante en infraestructura que la empresa no puede afrontar; la reducción de costos; o el mejor aprovechamiento del espacio disponible pueden ser sólo algunas de las razones que lleven a tomar esa decisión. Sin embargo, deberemos siempre tener en cuenta el punto de vista técnico para no fallar en la selección del proveedor.

- ¿La velocidad de la red satisface las necesidades operativas actuales y de crecimiento a mediano plazo?
- Confirmar que la protección física de los activos es segura.
- Analizar y visitar las instalaciones del proveedor para examinar qué servicios ofrecidos se cumplen, y los niveles de redundancia (UPD, generadores, refrigeración, etcétera).
- ¿La instalación elegida tiene capacidad de crecimiento disponible suficiente?
- Asegurar que el Data Center del proveedor cumple con los requerimientos normativos, los cuales tenemos que certificar en nuestras instalaciones.
- Considerar cuál es la capacidad de respuesta del proveedor en caso de desastres y cuáles son sus procedimientos en esos casos.

Viabilidad económica para alojar servidores en Data Centers externos (Housing)

Como continuación de la cuestión anterior, una vez que se ha pasado por todos los puntos anteriores o no se cumple con alguno de ellos, pero se acepta el riesgo en función del beneficio económico, se recomienda analizar en detalle los beneficios económicos para adquirir una visión clara al momento de tomar la decisión final.

- Reducir gastos de consumo eléctrico.
- Aumentar la disponibilidad gracias a los servicios de monitoreo.
- Analizar los servicios de valor agregado que puede ofrecer el proveedor: soporte 24 x 7 en el sitio, reemplazo de partes de forma inmediata según el tipo de hardware, etcétera.

Consolidación de Data Centers

La consolidación de los Data Centers es un proceso de integración estratégico de la empresa a mediano o largo plazo cuyo fin es brindar una estructura más sólida, robusta y simplificada orientada a servicios de IT de alta disponibilidad buscando reducir costos. Normalmente se da en empresas que tienen muchas oficinas remotas, ya sean locales o internacionales. También ocurre cuando grandes empresas comienzan a absorber a empresas más chicas que tienen su propio Data Center, como sucedió con el fabricante de procesadores AMD, que llegó a tener 18 Data Centers a consecuencia de la adquisición de empresas más pequeñas. Luego de un trabajo de muchos meses que comenzó en 2008, logró en 2012 reducirlos a 9, y su objetivo final para 2014 será reducirlos a 3 grandes Data Centers.

Los enlaces de conexión LAN/WAN entre el nuevo Data Center centralizado y los puntos remotos donde se encuentran las personas que accederán a los servicios son fundamentales para lograr un proceso exitoso. Según un estudio de Forrester Consulting en 2011, en promedio el 50% de la información de las empresas se almacena en las oficinas remotas. Esta cifra es bastante elevada no sólo para mover los datos, sino también para cuando los usuarios quieran acceder a ellos al mismo tiempo, entonces, podrían surgir problemas de latencia si la red no estuviera correctamente diseñada.

El concepto de consolidación se utiliza alguna veces erróneamente cuando se habla de reingeniería, reestructuración o cuando se virtualizan servidores para mejorar el proceso de estandarización, ya que si bien es una herramienta muy útil tampoco es excluyente.

- Ventajas
  - Mejor control de los datos.
  - Reducción de costos a largo plazo.

- Mejora de los niveles de servicios y disponibilidad.
- Simplificar la administración de la infraestructura de IT.

La consolidación puede hacerse desde distintos puntos de vista, según las necesidades del negocio, capacidades de los Data Centers, factibilidades técnicas, económicas, legales, etcétera. En consecuencia, podría decirse que se trata de un proceso artesanal con muchísimas iteraciones y cambios; mientras mejor se planifique en la etapa inicial, más rápido se podrá finalizar el proyecto y menor será el impacto. Podría hacerse consolidación de diferentes tipos: Servidores, Sistemas operativos, Base de datos, Aplicaciones desarrolladas, Aplicaciones Web, Almacenamiento, Redes, Data Centers, Procesos, Backups, Políticas de seguridad, Impresoras, etcétera.

Los pasos para llevar a cabo un proceso de consolidación consisten en:

Lista de tareas

1. **Definir:** asegurar la capacidad técnica necesaria de la infraestructura para soportar la consolidación de espacio, refrigeración, electricidad, enlaces, etcétera, teniendo en cuenta la complejidad del Data Center y del negocio. Analizar la viabilidad económica del proyecto, ya sea por reducción de TCO, mejora en el servicio, mejora en la disponibilidad o simplificación de las tareas de administración. Se deben definir los roles, y establecer los objetivos financieros, de tiempo, calidad de servicio esperado o puntos de cumplimiento.
2. **Construir:** sobre la base de las ventajas enumeradas anteriormente, se deberá diseñar y planificar el proyecto, utilizando las herramientas de seguimiento de manera de contar con toda la documentación disponible en cada etapa, y así ejecutarlo y ponerlo en práctica, además de orientarse a la construcción del prototipo.
3. **Testear:** asegurar que las pruebas en las etapas iniciales se cumplan de acuerdo con los planes, y también confirmar que se alcancen los objetivos como si se trataran de sistemas con carga de trabajo real. Es conveniente repetir este proceso todas las veces que sean necesarias; las pruebas deben ser integrales y de configuración, asegurando la *performance* y funcionalidad para una correcta operación en producción.
4. **Reajustar:** establecer los objetivos deseados para poder medirlos y evaluar los resultados de las pruebas de la etapa anterior.

5. **Entrenar:** capacitar al personal a cargo de la administración sobre cómo funciona la nueva infraestructura consolidada. Se recomienda que estas personas también participen de la etapa de construcción.
6. **Ejecutar:** una vez que está probado y aceptado comienza la etapa de desarrollo del modelo que se construyó en una escala pequeña, repitiéndolo todas las veces que haga falta hasta completar el proyecto.
7. **Documentar:** es la etapa final donde se generan los documentos del nuevo ambiente que servirán como material de consulta para el personal técnico a cargo de la administración.

Errores comunes en el proceso de consolidación

- **Fallas en la recolección de información:** muchas veces las grandes empresas que tienen presencia en casi todos los países del mundo, comienzan a armar sus planes de consolidación en tres grandes Data Centers globales o más. Por ejemplo, uno para América, otro para Europa/África y un tercero para Asia/Oceanía. Pero luego de avanzar en el proyecto, el área legal notifica que ciertos servidores no se pueden sacar del país por restricciones de facturación, confidencialidad de información, cumplimiento de normas legales locales o relaciones contractuales, etcétera. Esto implica el haber trabajado inútilmente, causando una pérdida de tiempo para todos por no disponer de la información correcta a tiempo.
- **Resistencia al cambio y a entregar los servidores:** como todo proyecto de sistemas, siempre existe la resistencia al cambio, en particular aún más si se sacan los servidores físicos de una región o país para centralizar la operación en otro lugar, ya que los administradores y/o usuarios tienen la sensación de que pierden sus equipos.
- **Poca planificación:** un error común es fallar en el cálculo de los tiempos ya sea por exceso de optimismo o por desconocimiento de los ambientes. La línea de tiempo para los esquemas de migración y consolidación debe ser amplia, con no menos de uno a dos años, dependiendo de la complejidad.
- **Comunicación:** los fallos en los cálculos del ancho de banda requerido para cada sitio pueden tener un gran impacto negativo en los usuarios, en particular por la latencia si el ancho de banda no es el adecuado, por eso se debe elegir la infraestructura correcta. Una mala estimación puede hacer que un archivo tarde minutos en abrir desde una ubicación remota, en lugar de segundos.
- **Información**: no incluir a todos los equipos puede acarrear serias complicaciones al proyecto, sobretodo en la etapa de planificación. Preferentemente hay que incluir a aquellas personas que hayan desarrollado tareas similares.
- **Cambios inoportunos:** hacer modificaciones importantes en Aplicaciones críticas o en la Infraestructura simultáneamente durante el proceso de

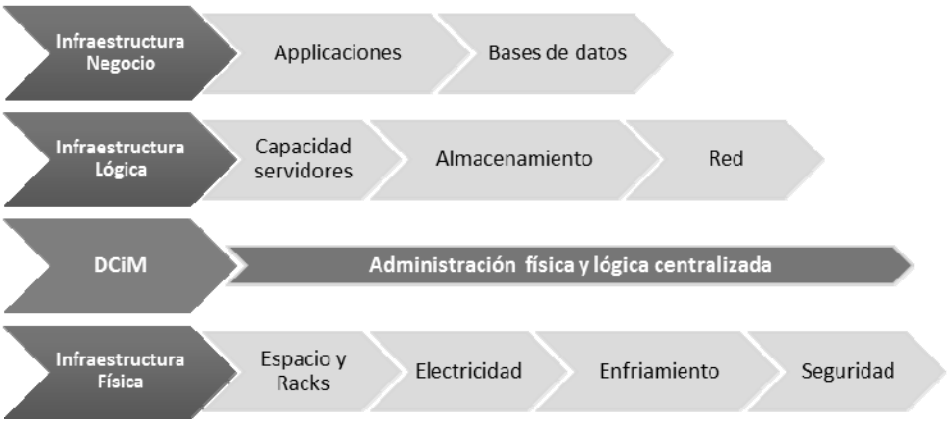
consolidación es un error grave, ya que una puede ser afectada por la otra o viceversa. Por eso, dentro de la planificación se deberá contar con un calendario con la fechas de los posibles cambios para adelantar o posponer cambios según sea lo mejor.

La consolidación de Data Centers ayuda a las empresas a simplificar sus planes de recuperación de desastres. Esto último será detallado en el próximo capítulo.

Monitoreo centralizado

La solución de monitoreo ideal es aquella capaz de concentrar y recibir todas las alertas en una sola consola, algo bastante difícil de lograr, ya que requiere tiempo y dinero debido a la gran cantidad de elementos dentro de un Data Center, por ejemplo, los recursos físicos o lógicos, que pueden ser de diversos fabricantes de servidores con distintos sistemas operativos, sensores de todo tipo, dispositivos de red, almacenamiento, base de datos, aplicaciones o sitios Web, etcétera.

Una solución integral de monitoreo debería proveer toda la información de manera centralizada y mantener un registro histórico para extraer estadísticas de disponibilidad, facilitando la gestión de niveles de servicio, o incluso obtener métricas de rendimiento por equipo para identificar posibles congestiones o sobredimensionamientos, y reasignar recursos que aseguren una distribución equitativa que permita aumentar el rendimiento.



Una solución eficaz de gestión de la infraestructura de suministro eléctrico, refrigeración y Rack de las redes de TI requiere la supervisión y el control de un gran número de dispositivos individuales y puntos de datos para el funcionamiento correcto de la infraestructura física de la red. Además, la solución de gestión debe

integrarse perfecta y simultáneamente con los sistemas de gestión de la red y del edificio.

El monitoreo es la base del mantenimiento preventivo, y permite acciones proactivas en lugar de reactivas. Puede darse en muchos niveles, como se mencionó en varias oportunidades, desde los más detallados y simples hasta los más complejos.

Una buena práctica para el control ambiental es regular la temperatura y mantenerla acorde a las condiciones establecidas previamente, ya sea a nivel de sala, fila o Rack.

Como parte de la infraestructura física, el monitoreo de la energía que se está consumiendo, el estado actual de las baterías o la detección de fallas en las PDU son parte de los indicadores que se deben tener en cuenta para asegurar una infraestructura robusta.

Existen un gran número de productos de monitoreo en el mercado destinados a tal fin, que permiten enorme granularidad, pudiendo generar alertas programables muy diversas, desde un aviso en caso de que un banco de memoria esté fallando en un servidor hasta disparar una alerta en el caso de que un sitio Web no está disponible en Internet. Sin embargo, para el responsable del Data Center lo más importante es determinar la capacidad de utilización real y la capacidad disponible. Por ejemplo, si estamos hablando de una nueva base de datos debemos ser capaces de responder rápidamente si disponemos de los recursos necesarios para alojarla, o en caso contrario, qué recursos deberían adquirirse.

Distintas soluciones de monitoreo permiten la integración: Tivolide IBM, Open Manager de Dell, Insight Manager de HP, Nagios, Orion, GFI, SCOM de Microsoft, etcétera. Algunas son propietarias de los fabricantes del hardware y otras no.

Según el uso que le otorguemos a las consolas, se las puede dividir en dos grandes grupos. Por un lado, aquellas orientadas a equipos de IT llamadas Enterprise Management System (EMS); por ejemplo: Open View, Nagios, o Tivoli. Por otro lado, aquellas que sirven para el monitoreo del equipamiento estructural de los edificios y se denominan Building Management System (BMS). Ambas consolas pueden estar centralizadas en una sola, utilizando Modbus[7] como medio de comunicación entre ambas, a fin de detectar fallas tan pequeñas como una URL[8] que no está funcionando, fallas de hardware en un servidor, un router desconectado, problemas de temperatura con un aire acondicionado, indicadores bajos en una UPS o un ascensor que no funciona.

[7]Es un protocolo de comunicaciones publicado por la empresa Modicon, en 1979, usado para controladores lógicos programables.
[8]Uniform Resource Locator o conocida comúnmente como dirección Web.

Por suerte, existen consolas capaces de centralizar toda esta información y enviar alertas automáticamente, si bien la configuración inicial puede ser compleja. La integración simplifica la administración y asegura la agilidad de respuesta. La solución óptima es la selección de una herramienta de DCIM que permita el monitoreo de los recursos de infraestructura física y lógica de manera integral, proveyendo las siguientes características:

- **Escalable, modular y flexible:** analizar los costos y métodos de licenciamiento así como las actualizaciones y simplicidad de uso. Evaluar los tipos, marcas y modelos de elementos soportados por la herramienta. Estudiar también las formas de extracción y visualización de datos.
- **Arquitectura de comunicación abierta:** seleccionar aquella que permita soportar varios protocolos, diversas interfaces de programación y conexión con otras consolas.
- **Estandarizado:** si bien requiere mucho trabajo de configuración, si el diseño de la herramienta demanda configuraciones que son simples de replicar, la tarea será más rápida, más aún en esos casos donde se tiene más de un Data Center.
- **Soporte:** la asistencia del proveedor es importante para las situaciones donde se deben monitorear nuevos equipos.

Luego de realizar tareas de consolidación y virtualización en los Data Centers se deberá analizar el resultado de la planificación realizada, asegurando mantener el enfriamiento y los requerimientos eléctricos de modo eficaz, ya que si la densidad de equipos aumentó para optimizar el uso de los recursos, pero no se tomaron las medidas correspondientes de reubicación de equipos, es posible que los niveles de PUE aumenten en lugar de disminuir.

Otra buena práctica propuesta por la organización *The Green Grid*, es el DCMM (*Data Center Maturit yModel*) publicado en el 2011, el cual permite clasificar el nivel de "madurez" de los componentes del Data Center: electricidad, red, almacenamiento, gestión, refrigeración, en función de dos aspectos: por un lado, la eficiencia sustentable y por otro, la inversión, clasificándolos de 0 a 5 según los métodos que se estén utilizando.

Enlace recomendado:

`http://www.thegreengrid.org/Global/Content/Tools/DataCenterMaturityModel`

Continuidad del negocio

10

"No podemos solucionar problemas usando el mismo razonamiento que usamos cuando los creamos".

--Albert Einstein (1879–1955) Físico alemán. Premio Nobel de Física en 1921

Es una metodología usada para crear y validar un plan que permita la persistencia de las actividades del negocio en situaciones fuera de lo normal como pueden ser una inundación o un incendio; a esos eventos se los llama desastres. Este tema ya ha sido analizado en el capítulo 1.

Por su alto impacto y la gran dependencia tecnológica que tienen todas las actividades comerciales, es una de las razones principales por las cuales las empresas hacen planes de continuidad del negocio, a fin de seguir operando aún en circunstancias adversas. Aunque, claro está, esto tiene un costo, razón por lo cual en función del presupuesto y las posibles pérdidas de deberá seleccionar un plan acorde.

Existen dos tipos de interrupciones. Por un lado, las **planificadas**, que son aquellas donde se debe interrumpir el servicio para realizar un servicio de mantenimiento o una mejora. Por otro lado, las interrupciones **no planificadas**, que son aquellas no intencionales, y en las cuales nos centraremos en este capítulo.

Al desarrollar un plan de recuperación, el objetivo es regresar la operación del negocio al nivel en que estaba el día antes de la catástrofe. Si su negocio es tomar pedidos por medio de una línea telefónica y continuar con la entrega de productos, el esfuerzo de recuperación debería estar dirigido hacia el restablecimiento de la operación telefónica y la conexión del personal a los sistemas de procesamiento informático y telefónico, lo cual permitirá que continúen los envíos.

El plan final podrá incluir una instalación redundante en otro sitio remoto que tenga acceso a los datos obtenidos de las copias de seguridad. Si la operación no es tan crítica o la instalación redundante no ha sido considerada por razones presupuestarias, es imprescindible un buen plan de recuperación.

Cada hora perdida decidiendo sobre un enfoque o experimentando con diferentes técnicas es una hora de interrupción al negocio que genera pérdidas.

Las empresas deberán desarrollar un plan integral, de forma artesanal para así enfrentar las consecuencias el día del desastre, ya que no existe una solución única, sino que es propia de cada empresa, diseñada a medida.

Ciclo De Vida Del Plan De Continuidad Del Negocio O BCP (Business Continuity Plan)

Un BCP no es un plan del área de IT solamente, sino que involucra a toda la empresa por completo desde la restauración de servidores hasta las tareas operativas, ejecutivas y directivas. En el plan interactúan las personas de la organización con la tecnología, los procesos y la infraestructura.

Ciclo de vida del Plan de Continuidad del Negocio

- **Análisis y planificación:** cuando se inicia el proyecto se debe tener en consideración **todo** el negocio por completo, haciendo un estudio de necesidades y evaluando la situación actual. Luego, se debe hacer un minucioso análisis de riesgos del impacto al negocio (BIA, Business Impact Analysis), análisis de pérdidas, cuantificación de consecuencias, etcétera e identificar las **aplicaciones críticas,** que forman el núcleo operativo: inventarios de aplicaciones y servidores, diagramas de red e infraestructura. Adicionalmente, hay que identificar los posibles escenarios y análisis de amenazas. En esta etapa, se definirán bajo qué condiciones se activarán los

procesos de contingencia y cómo será el camino que se tome para volver a la situación de operación normal.

- **Diseño de solución**: se buscará la manera en que se pueda llevar a cabo el plan de contingencia de manera integral desarrollando una estrategia de mitigación. Debe ser comunicado correctamente a todas las áreas, preferentemente siguiendo los estándares. Además se procederá con la elaboración de una lista de prioridades con un orden específico y se confeccionará un *checklist* para los equipos con identificación de contactos internos y proveedores clave. Se definirán los equipos y los procesos de recuperación así como la selección de la estrategia de *backup* y los objetivos de los tiempos de recuperación (RTO[1]). Asimismo se establecerá el tiempo máximo de interrupción tolerable (MTPOD[2]), el punto de recuperación objetivo (RPO[3]), la forma de interactuar y los roles clave.
  - **RPO:** refleja el punto tolerable de restauración de los datos. Por ejemplo, se define si es aceptable contar con los datos de las 00:00 h del día en que ocurre el desastre, o si se prefiere las 00:00 h del último domingo de la semana en que ocurrió el desastre. Obviamente esto está relacionado con la solución de *backup* elegida, que será detallada más adelante en este capítulo.
  - **RTO:** es el tiempo en que se desean tener los datos recuperados y disponibles. Por ejemplo, en cinco horas, diez horas, etcétera.
  - **MTPOD:** es el tiempo aceptable de recuperación total. Luego de haber alcanzado el RTO, queda pendiente restaurar las operaciones al punto normal. Esto puede requerir configuraciones adicionales que agregan más tiempo a la restauración del servicio.
- **Implementación**: es el desarrollo del plan, incluye la puesta en marcha de un ejercicio de simulación, que quizás para empresas chicas o medianas pueda ser inviable por razones presupuestarias, pero que son realmente importantes, como los ejercicios de evacuación de incendios en los edificios, entrenamiento, documentación y capacitación. Es recomendable que todas las tareas sean coordinadas por un Comité de Crisis que debe estar previamente designado y conformado por personas que conozcan bien el negocio, tengan poder y capacidad para tomar decisiones. Lo importante se debe anteponer a lo urgente, ya que una mala decisión puede ser contraproducente.
- **Testeo y aceptación:** en el momento de ejecución del ejercicio de simulación o cuando se activa el BCP, realmente, **la comunicación entre todas las partes tiene un rol fundamental para alcanzar el éxito**. Se deberá hacer la

[1]Recovery Time Objective. Se mide en horas.
[2]Maximum Tolerable Period of Distruption. Se mide en horas.
[3] Recovery Point Objective es el objetivo deseado de recuperación.

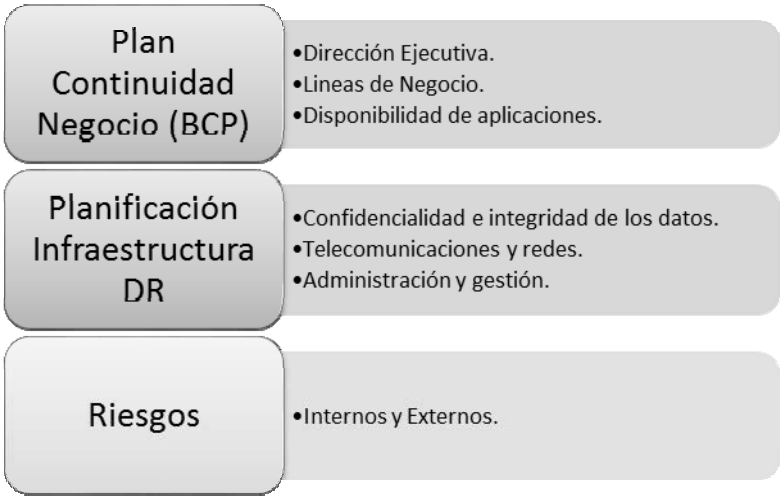
verificación, corroborar los pasos correctos, determinar desvíos, identificar puntos débiles, análisis de costos y luego tomar medidas correctivas, llamadas lecciones aprendidas (*lesson learned)*. Ellas realimentarán el proceso de diseño de la solución a fin de introducir mejoras.

Es recomendado hacer una prueba completa de todo el BCP **al menos una vez al año**, aunque pueden hacerse pruebas parciales con menor frecuencia para probar nuevas tecnologías o soluciones parciales para ciertos eventos.

- **Mantenimiento:** se debe comunicar y mantener actualizado el plan aprobado, asegurando que el personal esté debidamente entrenado. Hay que mantener un monitoreo continuo para el establecimiento de políticas estratégicas, además de identificar nuevas tecnologías o cambios operativos, legales, regulatorios directivos que permitan mejorar el diseño de la solución.

Se recomienda tener un repositorio de versiones y además un documento de control de cambios entre las distintas versiones para ver de manera simple cuales fueron las mejoras introducidas.

Sin duda estas planificaciones requieren dedicación de recursos, tiempo, recolección de información, infraestructura, etcétera, que en definitiva es dinero, pero si la catástrofe ocurre las consecuencias económicas serían mucho peores.



Cuando se está ejecutando un BCP, la confiabilidad de la información toma un rol fundamental, ya que los falsos positivos o falsos negativos pueden llevar a tomar decisiones catastróficas, en situaciones que por sí mismas ya son críticas, pudiendo además tener consecuencias devastadoras.

Se recomienda visitar los sitios mencionados a continuación, en donde se puede acceder a información actualizada sobre el tema:

Disaster Recovery Journal: `http://www.drj.com/`

The Business Continuity Institute: `http://www.thebci.org/`

Disaster Resource: `http://www.disaster-resource.com/`

Planes Para La Recuperación De Desastres O (DR, Disaster Recovery)

La planificación y preparación son esenciales para el éxito empresarial. Sin embargo, debido a los desastres son raros y ocasionales, y puede no ser una prioridad para algunas empresas. En su lugar, tomadores de decisión suelen concentrarse en los desafíos de negocios donde el retorno de su inversión es clara y medible. El DR forma parte del BCP, pero no lo es todo, el objetivo es reanudar y resolver el impacto inmediato causado por un evento inesperado. Por ejemplo restaurar lo más rápido posible un servidor que ha sido hacheado es parte del DR, pero un BCP es un concepto más amplio.

Los gerentes de IT que confían en sus planes de recuperación de desastres, lo hacen porque tienen confianza en los siguientes pilares:

- Capacidad y disponibilidad para adaptar nuevas tecnologías.
- Confianza en sus procedimientos y políticas.
- Soporte en el plano ejecutivo para la implementación de las estrategias, ya sea de recursos y de presupuesto.

¿Qué pasaría si su negocio experimentó un importante apagón o si sus sistemas fueran infectados masivamentepor un virus? En el caso de un terremoto o una inundación, ¿Tiene planes para restaurar los datos y procesos críticos? ¿Su empresa sabe qué sistemas y aplicaciones son las más importantes? ¿Tiene *backup* consistentes? Con plan sólido de DR se pueden responder a esas preguntas satisfactoriamente.

Hoy en día las empresas buscan un RTO cada vez más pequeño, ya que no quieren perder dinero

Consideraciones a tener en cuenta al momento de armar un plan de DR consolidado y centralizado:

- Identificar las aplicaciones críticas para el negocio.
- Pérdidas financieras importantes.
- Impacto a los clientes.
- Problemas legales.
- Sistemas on line 24 x 7.
- Servidores Web públicos, con potencial daño a la imagen de la empresa.

- Identificar las aplicaciones que manejan y guardan información que tiene requerimientos legales.
- Comprender que un plan de DR es inherente a todas las unidades de negocios.
- Identificar los puntos de fallas únicos o también llamados SPoF (Single Point of Failure).
- Tener especial consideración en el momento de la preparación para aplicaciones obsoletas que aún estén en funcionamiento. Por lo general, esas aplicaciones son bastante más difíciles de restaurar.
- Estrategia y políticas de resguardo o *backup*.
- Identificar a los equipos que realizaran el test posrestauración.
- Identificar aplicaciones que tomarán más de 48 h en restaurarse.
- Plan de comunicación actualizado.

Las empresas que cotizan en la bolsa de valores de Wall Street están obligadas a cumplir con los requerimientos de la ley conocida como SOX o Ley Sarbanes Oxley[4]. Allí se establecen muchas pautas y controles que van desde aspectos financieros y patrimoniales hasta normas regulatorias relacionadas con el área de IT, específicamente en los artículos 404, 405 y 406. Si bien se trata de una ley estadounidense, ella obliga a que las filiales de esas empresas también la cumplan, por ello las empresas multinacionales de capitales estadounidenses se ven afectadas.

Fallar dos años consecutivos el ejercicio de DR puede hacer que una empresa deje de cotizar en bolsa de Wall Street.

Existen diversos tipos de organismos internacionales que brindan recomendaciones sobre cómo seguir un plan de BCP basado en las mejores prácticas, como por ejemplo: Basel II, COBIT, ISACA Guidelines G32 for BCP Auditing, ISO 22301, publicada en mayo de 2012; BS 25999-2 estándar británico, NFPA 1600. Y en particular también hay otras regulaciones que son obligatorias según los requerimientos de cada país y según el tipo de industria. Por ejemplo, los Estados Unidos es uno de los países que más regulaciones tiene: ASIS International Organizational Resilience; ANSI Standard California SB 1386; Fair Credit Reporting Act, Federal & Legislative BC Requirements for IRS; FFIEC BCP Handbook; FRB-OCC-SEC Guidelines for Strengthening the Resilience of US Financial System: GAO Potential Terrorist Attacks Guideline; HIPAA relacionado con los servicios de salud y alimentación; Final Security Rule; NASD Rule 3510; NFA Compliance Rule 2-38;

[4]Es una ley creada por dos senadores estadounidenses, el demócrata Paul Sarbanes y el republicano Michael Oxley, en el 2002, luego de los fraudes financieros de ENRON, Tyco International, WorldCom y Peregrine Systems.

NFPA 1600; NIST 800 Series; North American Electric Reliability Council (NERC); NYSE Rule 446; SOX.

En 2012 Quantum Corporation realizó una encuesta entre 500 gerentes de IT, de empresas de más de 100 empleados. En ella se revelaba que el 90% creía ser vulnerable a un evento de desastre. Además, el 27% sufrió algún tipo de incidente de seguridad en el último año, de los cuales el 15% se debió a desastres naturales.

Para lograr una alta disponibilidad de las aplicaciones que le permitan a la empresa desarrollar su actividad en caso de catástrofe, los componentes que aseguran esa meta son:

Implementación de un Plan DR en IT

Dentro de las tareas de DR, el área de IT tiene una gran parte de la responsabilidad en el logro de un BCP exitoso a partirdel momento en que se declara la situación, ya que es la base de la pirámide.

Se necesitará contar con la gente para indicada para poner en marcha el plan:

- Identificación de los posibles escenarios, haciendo un análisis de amenazas.

- Activación del sitio de contingencia.
- Administración de hardware y software.
- Utilizar herramientas de software para restaurar equipos físicos en hardware que sea distinto del original.
- Recuperación de la infraestructura de la red física y lógica.
- Tener la documentación que respalda la secuencia de restauración de los equipos, ya que si el orden no es el correcto puede haber problemas más adelante.
- Administración de los sistemas operativos
- Asegurarse de poseer todas las claves y licencias para llevar a cabo la restauración cuando se reinstalen los sistemas.
- Recuperación de las base de datos.
- Recuperación de los servidores y aplicaciones.
- Testeo.

Una tendencia bastante habitual en el área de IT es virtualizar todos aquellos servidores relacionados con el ambiente de DR, siempre que sea posible, ya que la recuperación es mucho más sencilla y rápida. Adicionalmente, los proveedores de soluciones de virtualización ofrecen productos que simplifican y agilizan las tareas de *backup* y restauración de máquinas virtuales, permitiendo tiempos de recuperación muy reducidos en comparación con la restauración de los equipos físicos.

Complementariamente existen tareas y soluciones que agilizan y facilitan el plan de DR. Aquí se detallan algunas para tener en cuenta:

- Realizar restauraciones eventuales eligiendo servidores de manera aleatoria, usando una red aislada, a modo de prueba.
- Tener un software de *backup* y restauración centralizado para simplificar las tareas.
- Mantener copias fuera del sitio, al menos, semanalmente.
- Documentar paso a paso las instrucciones de recuperación y las configuraciones especiales en caso en que las haya.

En un escenario de una empresa grande que posee un Data Center central con 1 000 servidores y 300 oficinas remotas o sucursales que por problemas de latencia poseen sus propios servidores locales (por ejemplo: servidor de aplicación, servidor de archivos/impresoras, central telefónica, *router*, *switch*), probablemente el plan de DR tienda a focalizarse en las aplicaciones críticas del Data Center central, pero no en las oficinas remotas. Esto sería un error que se podría subsanar fácilmente, pero para ello existe una condición fundamental: la **estandarización.**

Si en todas las oficinas remotas existiera homogeneidad de infraestructura, para el departamento de IT sería simple tener una sucursal de respaldo de

contingencia en su depósito, conformada por un servidor de aplicación, servidor de archivos/impresoras, central telefónica*, router* y *switch* preparados.

En caso de desastre en alguna oficina remota, un incendio, por ejemplo, solo habría que configurar las aplicaciones, servidores, equipos de red, u otros, que incluso podría automatizarse por *script*, para luego transportar los equipos a la oficina remota, y solamente encenderlos para tener la sucursal nuevamente operativa.

Nociones básicas de backup y estrategias

Proteger el negocio de la pérdida de datos por desastres naturales o causas accidentales es una de las máximas prioridades de las empresas, aunque muchas veces tienda a quedar relegada por otras cuestiones. Conceptualmente, la idea es sencilla, aunque puede resultar difícil implementar un conjunto de operaciones de *backup* eficaces y efectivos. Probablemente esta sea una de las tareas más difíciles de definir en el área de IT, ya que al momento de tomar las decisiones y definiciones con respecto a la política de *backup* elegida, entran muchísimas variables en juego, como: velocidad de la red, velocidad del dispositivo de *backup*, cantidad de cintas necesarias para el *backup*, tiempo de retención, volumen total de datos, cantidad de copias (según el tipo de negocio, pueden existir reglamentaciones de entidades regulatorias de carácter obligatorio para tener más de una copia del *backup* por día), tiempo de restauración de datos, presupuesto para cintas, disponibilidad del personal para cambiar las cintas, durabilidad de las cintas, método de encriptación de las cintas, en particular aquellas que serán usadas como copias secundarias que se alojaran en otro sitio físico, etcétera.

Las empresas tienen un desafío constante, cada vez deben manejar mayores volúmenes de datos, ya sea por expansión, facilidad para almacenar documentos en forma electrónica, requerimientos normativos, etcétera. En algunos casos, el crecimiento puede alcanzar entre un 40% y un 60% anual, lo que genera nuevos problemas: ¿Cómo se manejan esos datos? ¿Cómo se respaldan y cuáles de ellos son realmente críticos para el negocio? Generalmente, se almacenan sobre la base de datos y no suelen ser más del 15% al 20% del total de los datos.

Durante las últimas décadas, se han desarrollado aplicaciones de software de *backup* que reducen la complejidad de las tareas de *backup* y restauración. Hacer copias de seguridad de los datos sólo es una parte de un plan de protección contra los desastres, y si el proceso no se diseña meticulosamente, es posible que no proporcione el nivel de capacidad de recuperación de desastres ni de protección de datos deseado.

La comprobación de los *backup* es tan importante como copiar. Si hay una ley de Murphy que siempre se cumple en IT es: “cuando realmente se necesita restaurar los datos siempre hay problemas, porque los medios físicos o archivos están dañados”.

Un *backup* o copia de seguridad es un almacenamiento secundario de los datos, utilizado a efectos de protección de la información. En cambio, el archivo contiene los datos primarios y se traslada a un tipo de soporte menos caro como una cinta magnética, para guardarlo a largo plazo a menor costo. Por ejemplo, cuando existen regulaciones legales que obligan a las empresas a retener información por largos períodos de tiempo o a realizar más de una copia para almacenarla en otra ubicación como sucede con las entidades que están reguladas: los bancos.

Para las operaciones de *backup* existen tres métodos básicos en la forma de realizar los resguardos para los cuales se utilizan los atributos de los archivos: **nombre del archivo, tamaño, fecha última modificación** y otros que están generalmente ocultos como: **fecha último backup** *o* **Archive** según el sistema operativo, que funciona como **bandera** (*flag*) para marcar ese archivo desde la última vez que se le hizo el resguardo. Cuando los archivos se resguardan, el archivo se **marca** mediante ese atributo, si luego el archivo se modifica, entonces se quita esa marca para volver a resguardarse la próxima vez que se ejecute el *backup*.

Backup completos

Es el tipo de backup más básico, y consiste en copiar la totalidad de los datos en otro soporte de almacenamiento físico: cintas, discos, o algún otro tipo de medio transportable. La ventaja principal de la realización de un *backup* completo es que cada vez que se ejecuta la operación, se dispone de la totalidad de los datos en un único medio de almacenamiento. Esto permite restaurar los datos en un tiempo mínimo, pero el inconveniente es que lleva más tiempo realizar un *backup* completo y requiere más recursos. Por ello, sólo se realizan periódicamente, y el resto pueden ser incrementales, diferenciales o una combinación de ambas, dependiendo del caso. De esta forma, se busca optimizar los tiempos de resguardo, restauración y espacio necesario.

Backup incrementales

Solo se respaldan los archivos que fueron modificados desde la fecha del último *backup*, independientemente del tipo. Lo que hace que, por lo general ,el espacio necesario y la cantidad de archivos sea menor que el tipo anterior pero en oposición, la restauración de datos necesita tanto del respaldo actual como del respaldo completo y todos los incrementales intermedios.

Backup diferenciales

Se respaldan todos los datos modificados luego del último respaldo completo, por lo que no toma en cuenta si los archivos ya han sido incluidos en algún respaldo diferencial o incremental intermedio.

En la tabla descrita a continuación, se puede ver un ejemplo básico de cómo funcionarían los tres tipos de *backup* durante tres días, de un conjunto de cinco

archivos de datos de 1 GB cada uno. Allí se pueden apreciar las diferencias en cantidad de archivos almacenados.

Tamaño de Datos	**Día 1** Domingo	**Día 2** Lunes	**Día 3** Martes
Datos1 = 1 GB	Datos1	**Datos1 modificados**	Datos1
Datos2 = 1 GB	Datos2	Datos2	**Datos2 modificados**
Datos3 = 1 GB	Datos3	Datos3	Datos3
Datos4 = 1 GB	Datos4	Datos4	Datos4
Datos5 = 1 GB	Datos5	Datos5	Datos5
Total de datos a respaldar	**5 GB**	**5 GB**	**5 GB**

Tipo de Backup	**Día 1** Domingo	**Día 2** Lunes	**Día 3** Martes	**Total**	**Descripción**
Backup Completo	5 GB	5 GB	5 GB	**15 GB**	En cada día se hace un backup completo. Ventaja: Todos los días se resguardan todos los datos. Desventaja: Utiliza mucho almacenamiento y demora mucho tiempo
Backup Completo + Backup Diferencial	**Backup Completo**	Backup Diferencial 1 GB (solo Datos1)	Backup Diferencial 2 GB (Datos1 y Datos2)	**8 GB**	Después del último backup completo, por cada día se resguardan todos los archivos que se han modificado desde la última vez. Ventaja: Con el último backup completo y el último diferencial puedo recuperar toda la información. Desventaja: No es el método más óptimo si hay muchos archivos modificados.

Backup Completo + Backup Incremental	**Backup Completo**	Backup Incremental 1 GB (solo Datos1)	Backup Incremental 1 GB (solo Datos2)	**7 GB**	Cada día se resguardan archivos que se han modificado desde el último backup completo Ventaja: Es el método que mejor optimiza el tiempo y el espacio. Desventaja: Para restaurar todos los datos se necesita el ultimo backup completo, mas todos los backups incrementales de cada uno de los días. Si falla uno solo, no voy a poder recuperar toda la información.

La tabla comparativa indica las diversas operaciones de *backup* según el día y cómo es el funcionamiento diferente de cada tipo de *backup*. Asimismo, muestra las diferencias de los resultados de cada una de las estrategias elegidas, con sus defectos y virtudes.

También, observamos que inicialmente, siempre hay que realizar un *backup* completo al menos una vez, luego, se puede realizar otro *backup* completo, incremental o diferencial.

Generalmente los *backup* completos suelen hacerse durante los fines de semana, ya que requieren más tiempo para completarse, y el uso de los recursos del equipo (red, CPU, memoria, etcétera) suele ser bajo en esos momentos, permitiendo a la tarea de *backup* utilizarlos para finalizar sin inconvenientes.

A partir de estos tres tipos de *backup* principales, se puede definir una estrategia propia para la protección de datos según las necesidades de negocio y el presupuesto. Normalmente se utiliza uno de los enfoques siguientes:

- Completo semanal (domingo) + Diferencial diario (lunes a sábado)
- Completo semanal (domingo) + Incremental diario (lunes a sábado)

En la elección de la estrategia de *backup* óptima hay que sopesar numerosas consideraciones. Normalmente, cada alternativa y opción estratégica tiene sus ventajas e inconvenientes en términos de rendimiento, niveles de protección de los datos, cantidad total de datos conservados, y costos. Sólo si hablamos de respaldo en cintas, existen gran diversidad de productos de distintos formatos, con distintas velocidades, capacidades de almacenamiento, durabilidad y costos por unidad.

La implementación de una política de *backup* deberá estar definida sobre la base de la tolerancia a las catástrofes a fin de ofrecer la restauración más rápida

posible dentro del presupuesto y brindar la capacidad de poder recuperar los datos perdidos de manera accidental.

Como se mencionó anteriormente, a la hora de decidir la estrategia de *backup*, la cuestión no es tanto qué tipo utilizar como cuándo utilizar cada una de las opciones, y cómo combinarlas con la realización de pruebas para cumplir los objetivos generales de costos comerciales, rendimiento y disponibilidad al momento de la restauración.

Topología

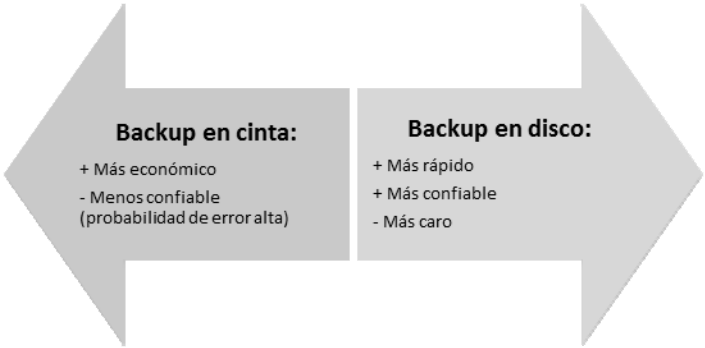
- **Centralizada**: múltiples clientes envían sus datos por la red a un único servidor de respaldo, el cual se encarga de almacenar los datos en el medio correspondiente. Entre las ventajas de esta arquitectura se destaca el menor costo en realizar la configuración y operación para la protección de los entornos de respaldos debido a que todo es controlado desde un único equipo, generalmente controlado por un brazo robótico que administra las cintas. Si hablamos de respaldo en disco, los costos en hardware son menores si se compara un disco de 1 TB que es más económico que comprar cinco de 200 GB. Este método es ampliamente utilizado por empresas medias y grandes.
- **Descentralizada**: cada cliente guarda su información en los dispositivos de respaldo directamente conectados a ellos. Como ventaja se destaca que cada cliente puede restaurar sus datos independientemente, sin necesitar comunicarse con otro servidor, evitando así el uso de la red. Pero es un método caro; requiere muchos dispositivos con altos costos de operación, mantenimiento e inversión, ya que las cintas se deben cambiar equipo por equipo, manualmente. Generalmente es usado por empresas pequeñas.

Las empresas que buscan alto rendimiento de red y tienen presupuesto suficiente diseñan una infraestructura de red aislada de la red de producción, exclusivamente dedicada para realizar el *backup*. De esta manera,se separa el tráfico entre las redes, mejorando la seguridad y sobre todo el rendimiento. Para esto, los servidores deben contar con una placa de red extra que se conecta a la red de *backup*, por lo que, mientras se efectúa el *backup*, los paquetes que circulan por la red de producción no se verán afectados.

Una solución aún mejor es la conocida como *LAN free* (libre de red LAN). Debido al gran avance de las virtualizaciones, la disminución de los costos de los equipos SAN o NAS[5] los ha vuelto cada vez más masificados y habituales, Dicha solución de *backup* no accede al servidor a través del sistema operativo para tomar

[5]Dispositivo de almacenamiento masivo por red (Network Attached Storage). Puede ser accedido por muchos equipos, pero tiene menor capacidad y velocidad que una SAN. Aunque su costo también es menor.

los datos que necesita resguardar, sino que accede directamente a la SAN generalmente por fibra óptica, haciéndolo muchísimo más rápido y eficiente, porque accede a los datos directamente sin intervención del sistema operativo ni interferencia en sus operaciones, hechos que disminuirían la *performance*.



Beneficios de un DR centralizado

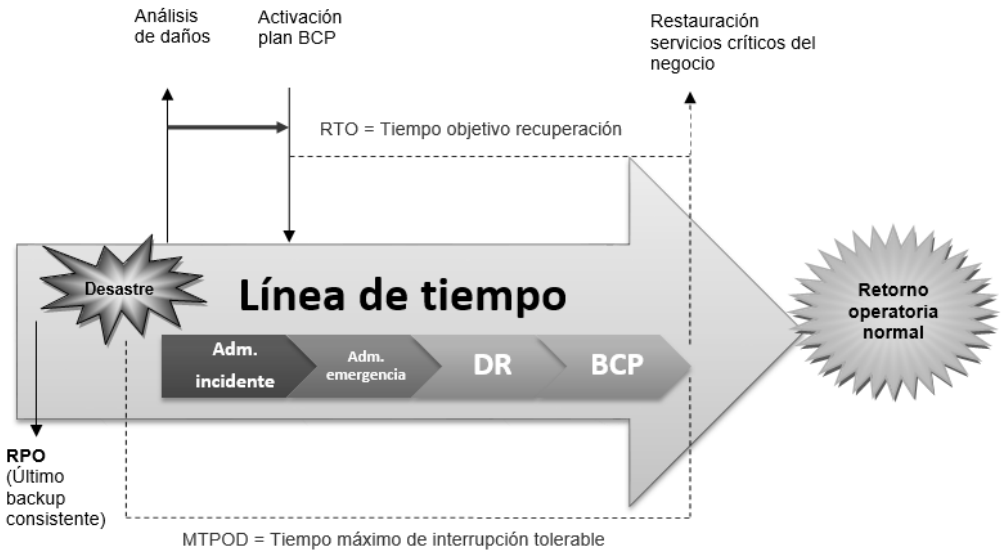
Muchas empresas ven a los requerimientos que se mencionaron anteriormente como trabas o dificultades que deben cumplir y nada más. Pero en realidad tiene un objetivo: buscar una transformación que brindará un entorno más saludable, haciendo que las empresas transformen sus ambientes a fin de acceder a los siguientes beneficios:

- Estandarización y simplificación de sus ambientes de IT.
- Automatización de los procesos manuales.
- Reducción de riesgos.
- Introducción de mejoras en los entornos que resultarán en reducción de costos a largo plazo.
- Documentación y comprensión de un plan que permita darle continuidad al negocio en caso de catástrofe.

El testeo de la ejecución del plan o simulación, sea o no obligatorio por las regulaciones existentes, es muy importante, ya que permite al personal estar entrenado para actuar en el momento real o sugerir mejoras a los planes. De la misma forma que en los edificios se hacen simulacros de evacuación de incendios. El estándar ISO/IEC 24762 provee recomendaciones para efectuar un plan de DR exitoso, y el estándar ISO/IEC 27035 provee lineamientos para actividades relacionadas al manejo de incidentes.

El aporte de la consolidación de los Data Centers simplifica la tarea en el caso en que se necesite aplicar el plan de contingencia.

En el gráfico se puede apreciar cómo serían los pasos a seguir en caso de que se declarase un desastre



En el momento en que se declara el desastre, se procederá a analizar los daños. Si la administración de incidentes decide declarar la emergencia, se procederá a activar el plan de BCP que se declara el desastre, y se procederá a analizar los daños.

Si la administración de incidentes decide declarar la emergencia, se procederá a activar el plan de BCP. Allí comenzará a trabajar el grupo designado para la administración de emergencias, tratando de restaurar el servicio según el RTO preestablecido. Para ello se deberá recurrir al plan de DR, donde el área de IT restaurará el o los equipos a afectados, retornando los datos del negocio al RPO establecido con antelación. Luego se procederá a continuar con la parte operativa y funcional del BCP, donde se verificarán las aplicaciones y se ejecutarán los planes ejecutivos que hagan falta, asegurando que se cumpla con el tiempo MTPOD preestablecido para retornar a la actividad normal del negocio.

Según un estudio realizado a más de 6 000 participantes de 18 países por la consultora Acronis Global Disaster Recovery, en 2012, el 53% de los encuestados que trabajan en el sector industrial no creían ser capaces de realizar una recuperación rápida en caso de desastre, ya que sus soluciones de *backup* no integran los ambientes físicos y virtuales correctamente.

Data Center de respaldo para DR

Un Data Center de respaldo consiste en un sitio de contingencia que reemplazará al de producción solo con las aplicaciones definidas como críticas para el BCP.

Data Center de contingencia estándar

Consiste en disponer de un espacio físico vacío con la capacidad de contener y soportar las aplicaciones pertenecientes al grupo de DR; preparado con la estructura eléctrica y de refrigeración mínima para cubrir la contingencia de esos equipos. Se debe considerar con la posibilidad de que los equipos se demoren en conseguir en la zona, por ejemplo, Firewalls (cortafuegos) o algún reemplazo similar. Este método tiene un costo bajo, salvo por el desaprovechamiento del espacio, pero los tiempos de restauración son muy lentos (de días a semanas), ya que se debe conseguir el equipamiento, armar la infraestructura, luego instalar las aplicaciones; y finalmente, restaurar los datos de las cintas.

Data Center en la nube

Utiliza los servicios ofrecidos por los proveedores basados en Internet o a través de un enlace punto a punto por medio de un proveedor que ofrezca una conexión privada. Los costos son menores y la velocidad de instalación de los nuevos servidores es muy rápida, están basados en máquinas virtuales, pero lo que demandará más tiempo será la restauración de los datos, porque las cintas de contingencia deben ser enviadas hacia el proveedor, también habrá que restaurar las aplicaciones; y luego, restaurar los datos.

Data Center asincrónico (mirror off-line)

Consiste en tener otro Data Center duplicado en una ubicación remota en donde se replican todos los servidores críticos de manera asincrónica. Esto puede realizarse en un sitio privado o contratado por a algún proveedor, pero con la salvedad de que los datos de esas aplicaciones críticas se copian al Data Center de contingencia de manera automática fuera del horario de operatoria diaria; por ejemplo, por las noches, mediante diversas herramientas. Tiene un costo alto, ya que todos los servidores están disponibles, pero sólo se utiliza la red dedicada para la transferencia de datos al Data Center de respaldo cuando no afecta las operaciones en horario central; por lo cual, en caso de desastre, el tiempo de recuperación es menor a un día.

Generalmente este servicio es empleado por empresas que procesan sus operaciones más importantes en servidores Mainframe, del rubro bancario, por ejemplo, ya que en caso de desastre no pueden quedarse sin operar, y tener un Mainframe de respaldo resulta impráctico debido a su altísimo costo, pudiendo costar varios millones de dólares solo un Mainframe.

Data Center sincrónico (mirror on- line)

Llamado espejado o (*mirroring*), es una estrategia donde en el Data Center de respaldo propio o rentado a algún proveedor replica todos los datos de la aplicaciones críticas, tomándolos desde el Data Center de producción, de modo constante en tiempo real, copiando bloque a bloque; de manera tal, que si ocurre un desastre, la recuperación es instantánea, pudiendo tomar tan solo algunos minutos.

Es la estrategia más rápida y costosa, ya que requiere tener todos los servidores duplicados y exige tener un gran ancho de banda disponible solo para la copia de los datos en tiempo real. Por lo que los costos en infraestructura de red son altos, además del mantenimiento e la implementación del software encargado de hacer que esa replicación funcione: Softek de IBM, Stream de Oracle, u otras soluciones provistas por los fabricantes de la SAN. Está claro que este tipo de soluciones están reservadas para empresas grandes que manejan presupuestos de infraestructura millonarios y no pueden sufrir interrupciones en la operatoria de sus servicios debido a sus altísimos costos.

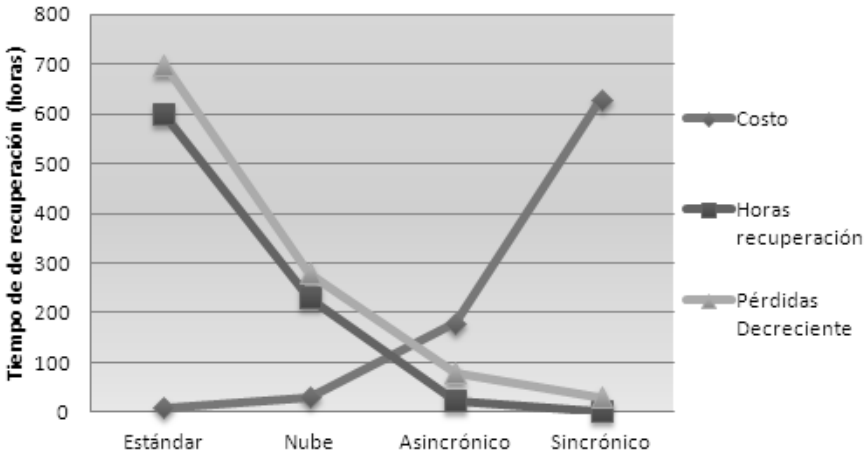
Importante

Si se elige una estrategia sincrónica es fundamental que dicho proceso sea monitoreado constantemente a fin de corregir los desvíos, ya que de nada sirve una inversión tan grande para luego tener problemas de inconsistencia de datos por problemas de sincronismo.

Ambas estrategias, asincrónicas o sincrónicas son válidas mientras sean adecuadas entre el balance de costo y tiempo de RTO, adecuando el tipo de método de replicación elegido, ya sea por SAN, por red o a nivel de servidores o de base de datos, ya que los tiempos de recuperación de datos por medio de las cintas magnéticas son lentos para las necesidades de negocio de muchas empresas.

Los fabricantes de SAN como EMC, IBM, HP, Hitachi o Dell, entre otros ofrecen soluciones de replicación que se ajustan a cualquiera de los dos tipos. También para replicación por red a nivel de sistema operativo o replicación por red con productos que optimizan el tráfico de manera segura y eficiente.

En el gráfico, se muestran los cuatro tipos de estrategias de Data Center de contingencia teniendo en cuenta dos variables: el tiempo de recuperación de las actividades y el costo operativo que tienen cada una de las soluciones de manera estimativa. Además, se puede ver una línea que estima cuáles serían las pérdidas. Nótese que la curva es arbitraria a modo ilustrativo como ya se ha mencionado, en el capítulo 1, dependerá del tipo de negocio.



Para decidir cuál va a ser la metodología elegida para el Data Center de contingencia, se deberán analizar los costos por las pérdidas y los costos por la implementación de la solución, además de la variación en horas por cada tipo de solución sobre la base de la complejidad de las aplicaciones que se restaurarán.

Fallas comunes BCP

Las principales causas por las cuales los planes de BCP pueden fallar total o parcialmente son:

- **Fallas en la planificación**: los planes debe ser compresibles, detallados y consolidados. Muchos responsables de aplicaciones, encargados de generar la documentación, relegan la tarea porque les consume mucho tiempo, y también por la falta de recursos económicos.
- **Fallas en la administración de los cambios**: los planes no se mantienen actualizados acordes con las modificaciones en la operatoria del negocio, que es muy dinámica y en evolución constante, cambiando procesos de negocios, personal, proveedores, etcétera. Si no se ponen al día los planes de BCP, quedan obsoletos en poco tiempo.
- **Fallas en la revalidación**: el proceso de validación y test debe ser consistente, ejecutado al máximo nivel de profundidad posible, preferentemente, incluyendo usuarios finales, teniendo en cuenta tanto os objetivos planeados como el suministro de retroalimentación para las acciones correctivas.

Mejores prácticas

11

"El futuro mostrará los resultados y juzgará a cada uno de acuerdo a sus logros".

-- Nikola Tesla (1856–1943) Inventor, Ingeniero mecánico y eléctrico serbio

Recomendaciones para construir un buen Data Center desde el inicio

Según los resultados arrojados por un estudio de Gartner, del 2010, se estima que cualquier Data Center mayor de siete años resultará obsoleto si no se actualiza, teniendo en cuenta los cambios tecnológicos disponibles, la necesidad de mayores velocidades de red, de reducción de emisiones y menores consumos, o de mayores requisitos de disponibilidad.

La construcción u ampliación de un Data Center es una tarea extremadamente compleja que requiere la participación de muchos proveedores. Por tal motivo intervienen muchas personas, y la coordinación debe estar a cargo de un Gerente de Proyecto (*Project Manager*), quien además de lograr la correcta interacción de todas las partes en tiempo y forma, deberá identificar los roles clave, los riesgos, documentar reportes de avance, planos, procesos, entre otras tareas.

Incluir todos los costos en el cálculo del TCO. Cuando se hace la planificación por lo general a diez años, además de los costos iniciales de instalación se deben incluir dos componentes fundamentales:

- Costos de mantenimiento: gastos relacionados con las tareas preventivas de la infraestructura a lo largo de la vida útil: reemplazo de partes, limpieza, etcétera.
- Costos de operación: son los gastos en que se incurrirán durante todos los años para que el Data Center funcione debidamente: energía eléctrica, personal, sistemas seguridad, etcétera.

Hacer una estimación correcta del presupuesto. La evaluación debe estar acorde a las necesidades actuales y futuras, considerando la posibilidad de expandir los recursos según la demanda, en tiempo y forma.

Evaluar si es realmente necesario la utilización de piso técnico: puede ser un costo evitable si se utilizan otras tecnologías y acelera los tiempos de implementación.

Seleccionar la disponibilidad correcta. Como ya se ha mencionado en los capítulos 1 y 2, establecer el nivel de disponibilidad acorde a las necesidades es fundamental, ya que sobredimensionarlo eleva el presupuesto de manera considerable y menospreciar su dimensión puede traer consecuencias graves para el negocio.

Seleccionar el diseño antes de elegir la ubicación. Esta estrategia debe utilizarse especialmente con los Data Centers grandes. Primero se deben analizar los requisitos de disponibilidad eléctrica o de proveedores de red, probabilidad de ocurrencia de amenazas naturales o creadas por el hombre; y luego, elegir el lugar físico donde se instalará el Data Center.

Diseño de configuración de los Racks. Hay que tener en consideración en el diseño del plano de cómo se colocarán los Racks sobre la superficie en cantidad, posición, tamaño de pasillos, equipos de gran tamaño; y luego, habrá que colocar las paredes para optimizar los espacios, ya que puede ocurrir que se dispone de una superficie con x metros cuadrados y se calcula que entrarán *xx* Racks; pero luego aparecen columnas en el medio que impiden armar una línea de Racks y se termina desaprovechando el espacio o también si se requiere colocar un equipo muy grande de dimensiones especiales. Por eso, la recomendación es diseñar las filas de Racks, tuberías de refrigeración, y luego diseñar la ubicación de las paredes, evitando así los espacio inutilizables.

Diseñar pensando en minimizar el acceso al área donde se encuentran los servidores. Si logramos reducir al mínimo la cantidad de personas que acceden al Data Center, podremos evitar muchos errores humanos. Por ello, mientras sea posible, los equipos que requieran mantenimiento o acceso a proveedores deberán estar en un área separada.

Selección de método de cableado. Si existe la posibilidad de elegir la forma en que se pasarán los cables, siempre es preferible pasar los cables por encima de los Racks antes que pasarlos por debajo del piso técnico:

- Menor riesgo de errores humanos ya que se evita la congestión de cables debajo del piso, que dificulta la tarea de identificación.
- Mejor maniobrabilidad.
- Mayor flexibilidad.

Actualmente la tendencia general de los nuevos Data Centers es instalar los cables de red y electricidad por encima de los Racks, ya que agiliza los tiempos de implementación y elimina el costo de instalación del piso técnico. Muchas veces, la

instalación de caminos redundantes para la infraestructura complica los diseños, por lo que se debe tratar de mantenerlo lo más simple y económico posible.

En caso de que se utilice piso técnico, el cableado deberá circular por debajo del pasillo caliente, permitiendo el libre flujo de aire por debajo del pasillo frío.

Elección del tipo de alimentación eléctrica. Conviene elegir una distribución eléctrica para que los equipos funcionen a 220/240 V, ya que la eficiencia eléctrica en todos los componentes es mejor. El mismo concepto aplica para las UPS.

Selección de la UPS correcta. Como se mencionó en el capítulo 4, existen muchos tipos de UPS, cada uno para un objetivo distinto, desde Data Centers pequeños, medianos a grandes. La clave es siempre analizar la eficiencia de la solución según su carga y elegir la que mejor se adapte a las necesidades del negocio.

Refrigeración. Este aspecto es similar al punto anterior: la cantidad de soluciones disponibles es muy diversa y la decisión se deberá considerar sobre la base de factores como la superficie del Data Center, la densidad kW/Rack, el consumo, o mantenimiento, el PUE objetivo, o la ubicación física, entre otros. Pero sí es una buena práctica aislar los pasillos, ya que los paneles de aislación resultan económicos en relación a todos los costos y brindan un ahorro importante en eficacia, sobre todo para densidades medias o bajas con posibilidad de crecimiento.

Otra buena práctica es establecer zonas con distintas densidades y estrategias de enfriamiento diversas para cada una, optimizando así los recursos. Este aspecto ha sido analizado en profundidad, en el capítulo 5.

Sistemas de seguridad. Hay que diseñar los sistemas y elementos de seguridad física, ya mencionados en el capítulo 6, acorde al presupuesto y a la sensibilidad de los datos que se almacenaran en el Data Center. La clave es buscar el equilibrio óptimo y planificar para aumentar los niveles de seguridad a futuro en caso en que sea necesario.

Establecer un PUE objetivo. Si se define un PUE próximo a 1.0 se logrará que los costos a largo plazo disminuyan de manera considerable así también como las emisiones de CO_2, sin dejar de lado el ROI de las inversiones para cumplir con esa meta.

Analizar las mejores prácticas y regulaciones a cumplir. Según el objetivo para el cual se está diseñando el Data Center, se deben tener en cuenta las distintas mejores prácticas, regulaciones o estándares (ya estudiados en diversas partes de este libro). En ese sentido, es importante hacer una aclaración:

- **Regulaciones:** son de carácter obligatorio según el tipo de actividad. Están reguladas por una ley, y no cumplirla puede hacer que el organismo regulador quite la licencia de habilitación al negocio para desarrollar la actividad.
- **Estándares:** son disposiciones concretas sugeridas por organismos reconocidos, que en el marco del cumplimiento con las normas establecidas certifican que la empresa cumple con los criterios delineados en el modelo.

- **Frameworks:** como el nombre de la palabra lo indica, son marcos de trabajo, son los más flexibles, ya que no están regulados. Ofrecen una metodología sugerida de trabajo que se adaptará a las necesidades operativas del negocio.

Aquí hemos nombrado solo algunos, pero existen muchísimos más, en especial en materia de regulaciones, ya que dependen de cada país y rubro comercial.

Regulaciones	Estándares	Frameworks
•SOX	•CIS	•COSO
•LOPD	•NIST	•COBIT
•GLBA	•NSA	•ITIL
•FISMA	•ISO 24762	•ISO 17799
•HIPAA	•ISO 27001	•NIST
•FRC	•ISO 27002	•OECD
•PCI DSS	•ISAE 3402	
	•ASHRAE	
	•LEED	

Bitácora de incidentes

Una excelente práctica que los responsables de los Data Centers conviene que incorporen a su rutina de trabajo es un registro de incidentes para documentar todos los eventos relevantes que ocurrieron en el Data Center a fin de evidenciar cronológicamente los eventos ocurridos con el objetivo de detectar patrones anómalos y descubrir la verdadera causa de esos eventos. Este procedimiento se denomina ”análisis de la causa raíz” (Root Cause Analisys, RCA), y se ampliará más adelante, en la siguiente sección.

Ejemplo de una bitácora de incidentes con los datos mínimos que deberá contener

Fecha	Incidente	Resolución	Causa	Impacto	Efectos	Clasificación
16/11/2010	Se interrumpió el suministro eléctrico por una falla en una PDU. Incidente #99999	Cambio de plaqueta en el circuito interruptor	Componente dañado	**Nulo**	Los sistemas redundantes brindaron la energía necesaria	Sistema Eléctrico
21/04/2011	Filtración de agua detectada por un sensor de líquidos. Incidente #99999	Detección de fuga y reemplazo de cañería	Falla del material	**Nulo**	La pérdida de líquido fue pequeña y no causó efectos	Aire Acondicionado
28/09/2011	Durante tareas de mejoras de red, se desconectó por error una fibra de la red troncal. Incidente #99999	Reconectar la fibra	Error humano	**Medio**	Se detectó una disminución en la velocidad de la red	Redes
02/05/2012	Mediante una alarma se detectó que una unidad de refrigeración dejó de funcionar. Incidente #99999	Llamar al proveedor y reemplazar el compresor que se había descompuesto	Falla del material	**Bajo**	La temperatura en uno de los pasillos del Data Center se elevo 5°C durante 6 horas	Aire Acondicionado

12/08/2012	Se interrumpió el suministro eléctrico en todo el Data Center debido a una falla en la batería del generador. Incidente #99999	El proveedor del servicio eléctrico restauró el servicio.	La batería del generador estaba defectuosa por no tener el mantenimiento correcto	**Alto**	Todos los equipos del Data Center se apagaron	Sistema Eléctrico

La idea principal es utilizar toda esta información para confeccionar estadísticas y analizar los indicadores de factores repetitivos en donde se deba hacer foco para eliminar riesgos. En el caso de administrar varios Data Centers, se debería agregar una columna extra con la ubicación o todas aquellas que el responsable considere que le sean de utilidad para sus tareas.

Análisis Causa-raíz

Consiste en una metodología estructurada para hallar una solución definitiva que permita resolver un problema de manera de evitar su repetición en el futuro.

El incidente es lo que vemos por encima del suelo, pero las verdaderas causas que lo originan pueden estar ocultas en la raíz.

La práctica conocida como RCA se basa en el supuesto de que los problemas se resuelven mejor al tratar de corregir o eliminar la verdadera razón por la cual se originaron en lugar de simplemente solucionar el incidente.

- **Incidente:** evento no deseado que se interpone en el curso normal de algo o degradación del servicio.
- **Problema:** es la causa indeterminada de varios incidentes.

Existen muchas metodologías similares para hacer el análisis, y todas buscan el mismo fin. Si bien no es la idea desarrollarlas a todas, solo enumeraremos algunas como: **diagrama de Árbol**, **diagrama causa efecto de Apollo**, **diagrama de**

Fishbone o de Ishikawa[1], y el más popular de todos: el **diagrama de los Cinco Porqué**[2](FiveWhy's).

Ejemplo de un Análisis de Cinco Por Qué

Fecha: 12/08/2012 3:40 AM Duración interrupción: 3:00 horas

Incidente #: 99999 (si existiera una herramienta para la gestión de incidentes)

Descripción del problema: se interrumpió el suministro eléctrico en todo el Data Center.

Impacto al negocio: todos los servidores del Data Center se apagaron abruptamente a las 4:00 AM, afectando a 240 equipos.

Cantidad de usuarios afectados: estimado entre 20 y 50 personas, ya que era un domingo por la mañana.

Resolución: el proveedor del servicio eléctrico restauró el servicio.

Línea de tiempo:

- 3:40 AM: se interrumpe el suministro eléctrico de red y comienzan a funcionar la UPS.
- 3:50 AM: al activarse la alarma de fallo eléctrico, el generador debería comenzar a funcionar, pero no se enciende. En este momento, a la UPS solo le quedan 10 minutos de autonomía. El personal de monitoreo se pone en contacto con los responsables del mantenimiento eléctrico.
- 4:00 AM: la UPS agota toda su carga y todos los equipos del Data Center se apagan abruptamente, ya que el generador no estaba encendido.
- 4:50 AM: el responsable del mantenimiento eléctrico llega al Data Center y comienza a trabajar en el generador para determinar el problema.
- 5:30 AM: el diagnóstico indica que el generador no arrancó, porque la batería falló. No hay forma de iniciarlo, ya que no hay batería de reemplazo para encenderlo.
- 6:10 AM: se restaura el servicio eléctrico de red.

[1]Creado por el químico japonés Kaoru Ishikawa, en 1943.
[2]Técnica desarrollada por TaiichiOhno (1912-1990), ingeniero industrial japonés.

- 6:15 AM: se comienzan a encender todos los servidores. Algunos presentan dificultades, y los administradores deben intervenir para solucionar los problemas.
- 7:00 AM: se verifica que todos los servidores y todas las aplicaciones están funcionando correctamente.

Análisis Causa-raíz: problema: se apagaron todos los equipos del Data Center a las 4:00 AM por fallas en el generador:

- ¿Por qué el generador no inició cuando la UPS agotó su carga?
- ¿Por qué la batería de arranque del generador no pudo poner en marcha el motor de ignición?
- ¿Por qué la batería no tenía carga suficiente y estaba agotada?
- ¿Por qué se había cumplido el ciclo de la vida útil de la batería y no había sido reemplazada a tiempo?
- ¿Por qué debido a diferencias económicas con el proveedor del servicio de mantenimiento del generador, el último mantenimiento se había realizado seis meses atrás?

Factor contributivo: cuando se reemplazo la batería por primera vez no se utilizó el repuesto original, sino que se usó una batería similar de menor calidad.

1. Plan de acción: resolver los problemas económicos con el proveedor inmediatamente o conseguir otro proveedor alternativo para que realice el mantenimiento de manera urgente.

   Responsable: Gerente de IT.

2. Plan de acción: conseguir una batería de reemplazo y almacenarla dentro del Data Center para casos de contingencia.

   Responsable: responsable de la instalación eléctrica.

Lección aprendida: no dejar pasar más de un mes entre cada mantenimiento del generador, sea cual sea el problema con el proveedor debe ser resuelto de manera expeditiva para evitar faltas en el mantenimiento que puedan derivar en acciones de alto impacto negativo.

Esta metodología de análisis está fuertemente relacionada con las prácticas descriptas en la sección que viene a continuación.

Utilización de metodología ITIL

La ITIL (Information Technology Infrastructure Library) es una metodología desarrollada a finales de 1980,y es conocida como la Biblioteca de Infraestructura de Tec-

nologías de la Información. Se ha convertido en una guía a nivel mundial para la Gestión de Servicios Informáticos; iniciada originalmente como una guía para el gobierno del Reino Unido, su adopción ha demostrado ser de gran utilidad para muchas organizaciones de todos los sectores e industrias. Muchas compañías la utilizan como base de consulta, educación y soporte de herramientas de software. Hoy en día, ITIL es conocido y utilizado mundialmente, y si bien pertenece a la Oficina de comercio gubernamental (Office of Government Commerce, OGC) ,es de libre utilización.

ITIL fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia en aumento ha dado como resultado una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones IT a la gestión de servicios IT. La aplicación de este modelo de trabajo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, éstas deben ser manejadas por los procesos de mantenimiento y operaciones.

La edición 2011 de ITIL está formada por cinco libros:

- Estrategia de servicio.
- Diseño del servicio.
- Transición del servicio.
- Operación del servicio.
- Mejora continua del servicio.

En esos libros, se detallan las funciones y procedimientos que ayudarán a tener una metodología de trabajo ordenada y predecible. Se destacan: Centro de servicios; Gestión de incidentes; Gestión de problemas; Gestión de configuraciones; Gestión de cambios; Gestión de versiones; Gestión de niveles de servicio; Gestión financiera; Gestión de la capacidad; Gestión de demanda;Gestión de la continuidad del servicio; Gestión de Disponibilidad; Gestión de seguridad, mejora continua.

A lo largo de todo el ciclo de los productos y servicios de IT, la fase de operaciones alcanza cerca del 70%-80% del total del tiempo y del costo, y el resto se invierte en el desarrollo del producto. De esta manera, los procesos eficaces y eficientes de la Gestión de servicios IT se convierten en esenciales para el éxito de los departamentos de IT. Esto se aplica a cualquier tipo de organización, grande o mediana, pública o privada, con servicios IT centralizados o descentralizados, con servicios IT internos o suministrados por terceros. En todos los casos, el servicio debe ser fiable, consistente, de alta calidad, y de costo aceptable.

Dentro de la **Gestión de administración para la infraestructura física del Data Center** se destacan un grupo de procesos, los cuales proveen una herramienta para alinear los servicios de IT con los objetivos del negocio.

- **Gestión de incidentes:** tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.
- **Gestión de cambios**: es la evaluación y planificación del proceso de cambio para asegurar que si éste se lleva a cabo, se haga de la forma más eficaz posible, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio IT.
- **Gestión de la disponibilidad**: es responsable de optimizar y monitorizar los servicios IT para que funcionen ininterrumpidamente y de manera fiable, cumpliendo el acuerdo de nivel de servicio (Service Level Agreement, SLA), y todo ello a un coste razonable. La satisfacción del cliente y la rentabilidad de los servicios IT dependen en gran medida de su éxito.
- **Gestión de la capacidad:** es la encargada de que todos los servicios IT se vean respaldados por una capacidad de proceso y almacenamiento suficiente y correctamente dimensionada. Sus responsabilidades son:
  - Asumir un rol clave para asegurar que se cubran las necesidades IT actuales como la planificación a futuro.
  - Controlar el rendimiento de la infraestructura IT.
  - Desarrollar planes de capacidad asociados a los niveles de servicio acordados.
  - Gestionar y racionalizar la demanda de servicios IT.

Análogamente a los procesos mencionados anteriormente, como **Estrategia de administración y gestión de la infraestructura física del Data Center**, el responsable debe en consideración:

- Implementar un sistema de administración de incidentes.
- Definir un proceso para realizar cambios.
- Definir y monitorear las métricas de disponibilidad.
- Monitorear los cambios en la capacidad a largo plazo.

Idealmente este plan se debe implementar en un plazo de tres a seis meses, y revisarlo periódicamente, pero no debe ser mayor a un año, salvo en el caso en que los cambios en el negocio requieran redefinición de objetivos. Estas mejoras son beneficiosas a mediano y largo plazo y brindan la posibilidad de identificación de riesgos de manera sencilla, reduciendo el riesgo de las interrupciones y optimizando la productividad del personal.

Métricas de disponibilidad

El análisis de métricas de disponibilidad es importante para asegurar el cumplimiento de los niveles de servicios que se planificaron en la etapa de diseño contrastado

contra lo que se está cumpliendo realmente. También es muy útil en el análisis del cumplimiento de objetivos acordados con los clientes y proveedores de servicios.

SLA es un concepto devenido de las prácticas de ITIL para formalizar el acuerdo entre dos partes, de forma **simple, realista y medible.** En él se detallará el desempeño esperado de las prestaciones brindadas por el proveedor, pudiendo variar según el tipo de acuerdo, ya sea externo o considerando al cliente como si fuera interno. Obviamente a mayores exigencias en los niveles de servicio, mayores serán los costos.

Al brindar un número claro que no da margen a discusiones, se utiliza en los contratos para establecer las penalidades o multas en caso de incumplimiento por parte del proveedor.

Antiguamente los SLA y los SLO (niveles de servicio objetivo, Service Level Objective) consideraban solo los pedidos del cliente, pero actualmente esta tendencia está cambiando, buscando el establecimiento de acuerdos entre ambas partes donde ambos salgan beneficiados en una relación "ganar-ganar", por ejemplo, permitiéndole al proveedor tiempos de interrupción programados para hacer mejoras en su infraestructura y así puede brindar un servicio de mejor calidad.

- **SLO:** es el análisis de la disponibilidad de un objetivo en particular, analizado individualmente.
- **SLA**: nivel de acuerdo de servicio. Es un concepto general que analiza la disponibilidad de un servicio función del tiempo.

Ejemplo: a un cliente se le provee un servicio de *housing* a 10 servidores con aplicaciones Web, y el proveedor se compromete a que todos estarán 99.5 % disponibles mensualmente, con un tiempo de interrupción máximo de 4 horas. Debido a un problema del proveedor, uno de los servidores estuvo desconectado de la red 6 horas, por lo cual no se cumplió con el SLO esperado para ese equipo en particular. Pero haciendo las métricas de SLA mensual se obtiene que:

Cálculo de disponibilidad mensual real:

- 9 servidores x 24 (horas) x 30 (días) + 1 servidor x 24 (horas) x 29 (días) + 18 (24 horas del día – 6 horas de la interrupción)
- 6480 + 696 + 18 = 7194 horas

Disponibilidad óptima total:

- 10 (servidores) x 24 (horas) x 30 (días)= 7200 horas

$$SLA = \frac{7194}{7200} \times 100 = 99{,}91\%$$

Por ello es posible que no se cumpla con un SLO en particular, y exista una penalidad o no por ello, pero también se puede observar que no siempre significa que no se cumpla con el SLA mensual acordado.

Es recomendado que las métricas de disponibilidad se realicen desde un lugar externo a la red de proveedor, ya que nuestros servidores Web pueden sufrir una interrupción por un problema en su Firewall, pero desde la red interna esa interrupción no queda registrada.

Los SLA también se pueden usar como límites de operación o para disparar procesos de contingencia, siempre y cuando sea una interrupción o degradación de servicio no planificada.

Algunas métricas que se pueden tomar para la SLA pueden ser:

- Porcentaje de disponibilidad de un servicio o aplicación.
- Cantidad de usuarios conectados simultáneamente.
- Velocidad promedio de la red.
- Cantidad de transacciones.
- Cantidad de Gbps enviados o recibidos.
- Otros.

Si el objetivo es brindar servicios a los usuarios finales, nuestros niveles de SLA y métricas deberán hacer foco en las prestaciones que los usuarios utilizan para lograr satisfacer sus necesidades; y en caso de encontrar desvíos, tomar las medidas correctivas a tiempo con una visión proactiva.

Además los SLA sirven para analizar el rendimiento como indicadores, detectar fallas, tendencias de crecimiento o decrecimiento para luego tomar de decisiones.

Control ambiental

El orden y la limpieza maximizan la durabilidad de los componentes dentro del Data Center y disminuyen las probabilidades de catástrofes. Aquí se detalla una lista de recomendaciones a considerar como política de gestión para lograr buenos resultados:

- Mantener el orden y no juntar basura en el Data Center cuando se desembalan los equipos. Las cajas de cartón pueden ser un foco de incendio potencial, razón por la cual, cuando los equipos se terminan de colocar, todo el material sobrante debe ser eliminado del área de trabajo.
- Prohibir fumar en todo el Data Center.
- Prohibir el ingreso con alimentos o bebidas al área donde se encuentran los equipos.

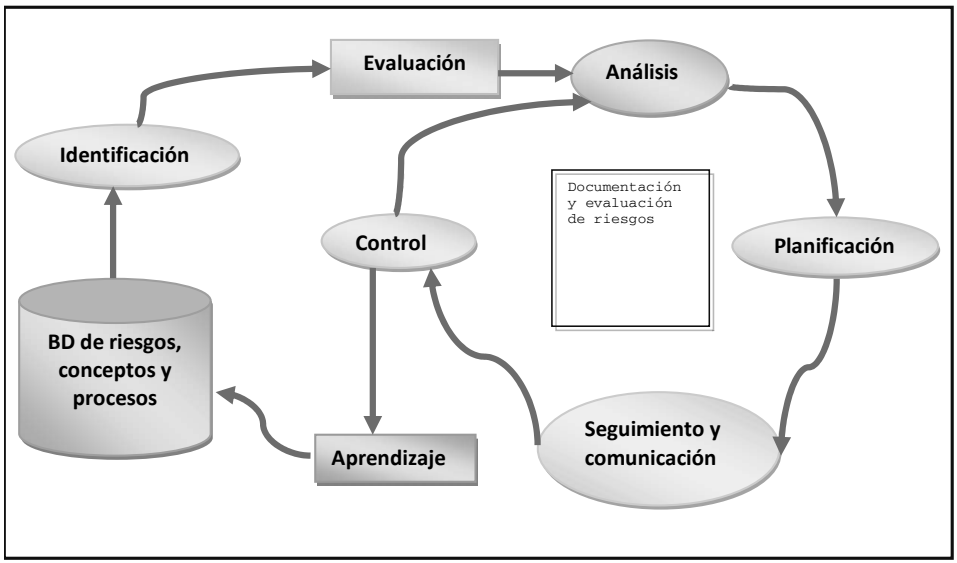
- Documentar los accesos, personas, motivos, tareas que realizará, etcétera.
- Prohibir la toma de fotografías, salvo expresa autorización de los responsables a cargo de la seguridad del Data Center.
- Mantener limpios los pisos y los Racks, ya que el polvo que ingresa del exterior puede dañar los equipos. Dicho proceso debe hacerse con **mucha precaución** de no desconectar ningún cable de manera accidental. Además se recomienda utilizar algún medio que remueva el polvo sin dispersarlo, usando una aspiradora.
- Evitar los cambios de aire dentro del Data Center en ambientes controlados, manteniendo las puertas cerradas para que el aire frío permanezca en el ambiente.
- Cambiar los filtros de aire regularmente, según las indicaciones del fabricante, además es recomendado tener un *stock* permanente de esos repuestos.
- Realizar inspecciones oculares esporádicas de rutina para detectar problemas nuevos como: roedores que se comen los cables bajo el piso técnico, filtraciones, fugas, goteras, falta de rótulos, Racks mal cerrados, etcétera.

Administración de riesgos

La administración de riesgos es una **metodología continua** que debe ser parte del día a día por su fundamental importancia, ya que los riesgos tienen un gran impacto sobre la ejecución exitosa de todo proyecto. Puede definirse como un conjunto de procesos que dirigidos hacia la administración efectiva de oportunidades potenciales y efectos adversos no deseados.

- **Riesgo**: es un problema que aún no ocurrió.
- **Problema:** un riesgo al que le llegó la hora.

Ciclo de vida del riesgo



Identificación de los riesgos

Es el primer paso, la detección, previo a la evaluación. Para administrar el riesgo de forma eficaz se debe establecer claramente de qué modo se analizarán las consecuencias además de crear un plan de acción para solucionar el riesgo. Aunque el ámbito del riesgo está limitado a la tecnología que el equipo posee, la atención debe ser lo suficientemente amplia como para abordar todas las fuentes de riesgos, incluido la tecnología, proceso, entorno y personas.

Evaluación de riesgos

Consiste en la recolección de información relativa del entorno del problema para evaluar un riesgo en particular. Se deben obtener datos suficientes que permitan analizar de forma eficaz el estado actual del entorno y determinar el grado de las consecuencias ante posibles amenazas.

Análisis de riesgos

El objetivo es separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para dirimir en la evaluación y tratamiento de los riesgos. El análisis de riesgos implica prestar consideración a las fuentes de riesgos, sus consecuencias, y las probabilidades de que puedan ocurrir esas consecuencias. Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado a los riesgos similares o de bajo impacto. La fórmula más simple es determinar la exposición al riesgo de la siguiente forma:

Exposición al riesgo = impacto x probabilidad de ocurrencia

Obviamente, haciendo que el impacto (daño) y/o que la probabilidad de ocurrencia tiendan a cero, lograremos que la exposición al riesgo disminuya.

Posibles alternativas considerando el impacto y la probabilidad de ocurrencia como variables

Exposición al riesgo		Probabilidad de ocurrencia		
		Bajo	Medio	Alto
Impacto	Bajo	Bajo	Bajo	Medio
	Medio	Bajo	Medio	Alto
	Alto	Medio	Alto	Alto

Este tipo de clasificación se ha confeccionado a modo de ejemplo. Para hacer un análisis más detallado, el impacto y la probabilidad de ocurrencia deberían tener valores numéricos entre 0 y 1. A mayor grado de exposición al riesgo, mayor es el problema que tenemos que resolver.

La magnitud de las consecuencias de un evento y la probabilidad del evento (con sus consecuencias asociadas) se evalúan teniendo en cuenta los controles existentes. Las consecuencias y probabilidades se combinan para producir un nivel de riesgo.

Se pueden determinar las consecuencias y probabilidades, utilizando análisis y cálculos estadísticos. Alternativamente, cuando no se dispone de datos anteriores, se pueden realizar estimaciones subjetivas que reflejan el grado de convicción de un individuo o grupo de que podría ocurrir un evento, o resultado particular con distintos grados de refinamiento, dependiendo de la información de riesgos y datos disponibles. Según las circunstancias, el análisis puede ser cualitativo o cuantitativo.

Estrategia de planificación de los riesgos

Existen cuatro estrategias posibles para tomar como alternativas ante la existencia de los riesgos. De allí se desprenderá el plan de acción según cada método.

- **Aceptación**. se considera la posibilidad de aceptar un riesgo si el efecto de la exposición al riesgo es menor al valor de la solución, o en casos donde no es posible aplicar solución alguna, ya que se encuentra fuera del alcance de las posibilidades. Por ejemplo: derrumbe de los mercados. Eso sería prácticamente una resignación, aun así, para este caso, se pueden aplicar estrategias de mitigación.
- **Eliminación:** se trata de una reacción extrema al riesgo, que se lleva a cabo cuando la repercusión del riesgo supera el beneficio que se obtiene del activo, haciendo nulo el impacto o/y eliminando la probabilidad de ocurrencia.
- **Transferencia:** la transferencia de riesgos es una buena alternativa para proyectos grandes donde a otro grupo o empresa se le requiere una solución para eliminar el impacto o la probabilidad de ocurrencia. Un ejemplo sería: contratar un seguro.
- **Mitigación:** se aplica una estrategia de atenuación del riesgo, reduciendo en parte la probabilidad de ocurrencia o disminuyendo el impacto, ambos combinados lograrán que el riesgo sea menor. La mitigación es la principal estrategia de administración de riesgos por ser la más viable económicamente.

En esta etapa es donde se deberá documentar y comunicar los riesgos, definiendo claramente cuál es la estrategia definida para cada uno, los roles y las responsabilidades.

Seguimiento y comunicación de los riesgos

El seguimiento constituye la función de supervisión del plan de acción de riesgo y es fundamental para la implementación eficaz de planes de acción. De esta forma, asegura que las medidas preventivas o los planes de acción se llevan a cabo puntualmente y dentro de las restricciones de recursos. Durante el seguimiento de los riesgos, la actividad principal será supervisar las medidas de los riesgos y garantizar la activación de los eventos de modo que las acciones de riesgo planeadas se lleven a cabo de forma eficaz.

Control

Consiste en la revisión de las acciones que se han detallado como planes de actividades de planificación. Los resultados de las pruebas deben documentar la efectividad de los planes preventivos y reactivos a fin de determinar si son los adecuados para los requisitos de la organización.

Las actividades deben evaluar la eficacia de cada plan elaborado. Es importante realizar de forma continua pruebas de las soluciones de riesgos para así poder detectar nuevos peligros que puedan aparecer debido a contramedidas nuevas.

Aprendizaje

Para la evaluación de los riesgos debe registrarse rápidamente a fin de proporcionar la información reciente y actualizada. El registro del conocimiento tiene tres objetivos claves:

- Registrar las lecciones aprendidas, especialmente aquéllas relacionadas con la identificación de los riesgos y las estrategias de mitigación correctas.
- Aumentar la eficacia de la disposición operativa en términos de la capacidad de la organización para ejecutar planes de respuesta a incidentes, y volver a utilizarlos en otras áreas de una manera más dinámica.
- Mejorar el proceso de evaluación de los riesgos a través de la captación.

Base de datos repositorio de riesgos, conceptos y procesos

Funciona como una base de conocimiento que sirve para evitar prejuicios subjetivos. Cuando se analizan las consecuencias y probabilidades, deberían utilizarse las mejores técnicas y fuentes de información disponibles como:

- Registros anteriores y experiencia relevante.
- Prácticas y experiencia de la industria publicada en libros y revistas.
- Experimentos y prototipos.
- Opiniones y juicios de especialistas y expertos.

Ejemplo práctico de análisis de riesgo dentro de un Data Center

En una inspección de rutina se ha detectado que dentro del Data Center, uno de los ductos de ventilación del aire acondicionado se encuentra obstruido, impidiendo el ingreso del aire frío al sector donde se encuentran alojados los servidores que manejan la línea de producción de una planta industrial cuyo costo de interrupción por hora es extremadamente alto.

Actualmente la empresa se encuentra en serios problemas financieros y no puede afrontar el costo de la reparación del ducto ya que requiere de una obra grande y muy costosa. La temperatura actual de los dos Racks donde se encuentra la zona afectada es de 32°C, mientras que en otro sector la temperatura es de 24°C. En total son 8 servidores críticos, el resto son de otras aplicaciones no críticas.

En este momento estamos en primavera, pero los pronosticadores climáticos estiman que este verano será mucho más caluroso que los anteriores, pudiendo alcanzar temperaturas de hasta 40°C.

Análisis:

Exposición: interrupción de la línea de producción por sobrecalentamiento en los servidores que manejan la fabricación de insumos.

Impacto: muy alto, interrumpir la línea de producción puede traer más problemas financieros que pueden poner en riesgo la existencia de la empresa = 0.98.

Probabilidad de ocurrencia: según los pronósticos climáticos y los problemas de temperatura, en ese sector la probabilidad de ocurrencia es muy alta = 0.95.

Exposición = 0,98 x 0,95 ➔ Exposición = 0,931

Alternativas de estrategias:

- Aceptación: el riego es demasiado alto. Aceptar el riesgo es prácticamente llevar a la empresa a la quiebra.
- Eliminación:
  - Conseguir un préstamo bancario para hacer la obra, pero la empresa no tiene buena calificación crediticia para poder obtenerlo.
  - Mover los servidores a otro Rack donde no haya problemas de refrigeración. Pero no se puede hacer, ya que los otros Racks están ocupados y el tiempo para mover los equipos físicos es demasiado grande, ya que implica tener que detener la línea de producción por un lapso de tiempo excesivo.
  - Virtualizar los 8 servidores no es posible ya que la empresa no tiene recursos suficientes para ello (CPU, memoria, almacenamiento y licencias).
- Transferencia: en este escenario es difícil poder transferirle el riesgo a un tercero, ya que el problema está en la locación física.
- Mitigación: virtualizar los 4 servidores que más calor generan y son los que tienen mayor cantidad de procesadores; apagarlos dejando en funcionamiento los virtuales y dejando encendidos los 4 servidores físicos que funcionan como *backup* de la línea de producción. De esta manera se reduce la temperatura en ese sector, haciendo que la probabilidad de ocurrencia baje a 0.12.

Exposición = 0,98 x 0,12 ➔ Exposición = 0,1176

Así se logra disminuir de manera considerable el riesgo. Ahora, se deberá documentar, discutir, comunicar, decidir; y posteriormente, ejecutar el plan de acción seleccionado.

Luego de ejecutar las acciones, se deberán hacer los controles regulares para verificar si la temperatura ha disminuido de acuerdo con los planes estipulados.

Rol del responsable del Data Center

La infraestructura física es el cimiento del área de IT; por eso, debe prever con anticipación que la dirección del Data Center esté preparada para acompañar la dirección del negocio en forma ágil.

Una recomendación es tener piezas de repuestos en el Data Center, en caso de contingencia, siempre y cuando sea viable y sin salirse del presupuesto; quizás un filtro de un aire acondicionado, un sensor, una batería de un generador o alguna otra pieza menor pueda evitarnos un gran dolor de cabeza.

Además el responsable del Data Center debe estar permanentemente atento a las evoluciones tecnológicas para sugerir cambios tecnológicos o estratégicos de la compañía que le permitan adaptarse con velocidad, reduciendo los costos operativos y aumentando la disponibilidad de los servicios.

Notificaciones de cambios en la infraestructura

Cuando se realizan cambios en la infraestructura es importante que las personas que puedan ser afectadas potencialmente estén debidamente informadas, ya que pueden ser de gran impacto. Aquí se sugiere un modelo de cómo notificarlo:

Asunto: Mantenimiento preventivo generador principal

Para: SysAdmin@empresa.com

GerentesIT@empresa.com

LideresApp@empresa.com

datacenterStaff@empresa.com

Cuerpo del correo:

Número de cambio: CR44133 **(*)**

Hora inicio: domingo, 18 de agosto 2012, 13:00 h.

Hora finalización: domingo, 18 de agosto 2012, 19:00 h.

Sistemas afectados: ninguno

Aplicaciones afectadas: ninguna

Descripción: los técnicos de la empresa proveedora del generador realizarán las tareas de mantenimiento preventivo anual correspondientes, en las cuales se reemplazarán los filtros de aire y combustible. Además se comprobará el estado de baterías y otros componentes básicos.

Riesgos: en caso de producirse un corte en el suministro de la red eléctrica se activarán las UPS con autonomía de 15 minutos, tiempo suficiente para suspender las tareas de mantenimiento y volver al generador a su funcionamiento normal (ya que las tareas de mantenimiento se realizarán de a una a la vez).

(*) Nota: si bien al tener un número de cambio, damos por descontado que se están siguiendo con las metodologías de ITIL, mucha gente puede pensar que tener el cambio aprobado es suficiente, ya que los aprobadores deben prestar su consentimiento para dicha tarea; pero de todos modos, no está de más enviar una comunicación como recordatorio.

Consejos para el verano

- Tomar mediciones de temperatura en la parte delantera de los servidores a una altura de 2/3 del total del Rack.
- Ubicar los equipos de mayor consumo en la parte más próxima a la entrada de aire frío del Rack.
- Ajustar la temperatura del pasillo frío según la capacidad de enfriamiento.
- Asegurar que las rejillas del piso elevado estén bien situadas para el flujo correcto de aire.

- Colocar obturadores en los espacios vacios dentro del Rack.
- Comprobar cables en las partes laterales o posteriores de los Racks que permitan la expulsión del aire caliente.
- Cuando la habitación no está ocupada, apagar las luces y los monitores. Esto puede ahorrar entre 1% y 3% de la carga eléctrica y calor. Si existen cámaras de vigilancia instaladas, la luz deberá encenderse automáticamente al detectar la presencia de personas.

Herramientas

La variedad de herramientas con las que debe contar el equipo a cargo del las tareas de mantenimiento y operación diaria del Data Center puede variar según las dimensiones y la disponibilidad presupuestaria, aunque la mayoría son de muy bajo costo y tenerlas disponibles son de gran utilidad para el personal. Aquí se enumeran algunas:

- **Elevadores:** son carros móviles con capacidad de elevación para colocar y sacar servidores de los Racks, ya que son pesados, y colocarlos en posiciones elevadas puede resultar muy difícil.
- **Etiquetadoras para cables**: rotuladoras portátiles que funcionan con cintas térmicas autoadhesivas y permiten imprimir inmediatamente etiquetas. Se colocan con facilidad sobre los elementos que se quieren identificar como cables, Racks, servidores, *switchs*, *routers*, *Patchpanels*, etcétera.
- **Ventosa:** mediante una manija con un mecanismo adherente por succión de goma de uno o dos extremos se pueden levantar las baldosas del piso técnico fácilmente y con seguridad.
- **Destornilladores:** se debe contar con variedad de destornilladores de diversas formas y tamaños (planos, Phillips, etcétera), ya que pueden resultar útiles para tareas de mantenimiento.
- **Pinzas pelacables:** son herramientas para pelar cables que se usan para cortar el revestimiento de los cables y el aislamiento de los hilos.
- **Impactadoras (Punchdown):** usadas en las terminaciones de los cables UTP se insertan los filamentos en los bloques de conexión o patcheras. Esta herramienta posee un mango ergonómico y sirve para insertar uno o varios hilos de cobre de los cables en los *Patchpanels*.
- **Precintos:** son elementos de plásticos o de velcro utilizados para organizar y ordenar el cableado estructurado.
- **Pinza crimpeadora:** también llamada tenaza engarzadora, se utiliza para instalar conectores, conocidos como Jacks RJ11 o RJ45 machos en el extremo de un cable. Se insertan los hilos en un conector macho siguiendo las corres-

pondientes normativas de colores y se inserta el conector en la herramienta, ejerciendo presión hasta que el conector emita un chasquido que confirme que está en su lugar.

- **Patchcords**: cables prearmados para realizar conexiones, pueden ser de cobre o fibra óptica.
- **Teléfono en el Data Center:** es recomendable que exista una línea telefónica en el Data Center, preferentemente inalámbrico, para ser utilizado por el personal en caso de que se requiera asistencia remota.
- **Tester de cables:** está formado por dos elementos: un emisor y un receptor. Se deberán colocar ambas piezas en cada extremo del cable que se desea corroborar. El emisor tiene un conjunto de luces indicativas que muestra la secuencia de orden; en caso de fallas, las luces no aparecerán como una secuencian ordenada. Este es un elemento de bajo costo y no es capaz de detectar fallas complejas como problemas de diafonía.
- **Tester eléctricos y de temperaturas (multímetros):** para tomar muestras aleatorias y detectar fallas de manera preventivas de tipo eléctrico, de temperatura o humedad.

Recomendación: usar sólo materiales certificados que cumplan las normativas de estandarización.

Errores comunes

Diseño

- Sobredimensionamiento de recursos.
- Ubicación de equipos Racks de alta densidad en zonas donde no hay suficiente capacidad de enfriamiento.
- Colocar los Racks de tamaño no estándar ubicados en el medio de una fila. Lo correcto sería ubicarlos en una zona distinta, ya que por lo general alojan equipos especiales que generan más calor.
- Falta de inversión en la infraestructura y en el mantenimiento, pudiendo convertir un Data Center capa IV en uno capa III.
- Fallas en el cálculo de la potencia eléctrica por no considerar el factor de potencia.

Componentes

- Emplear Racks con puertas de vidrio que impiden el ingreso del aire frío en lugar de puestas con paneles perforados. Antiguamente, eran bastante usuales, hoy en día se encuentran prácticamente en desuso.

- El uso de materiales no certificados o instaladores no recomendados por los distribuidores.
- Dejar a los servidores encendidos generando calor no cumple ninguna función operativa para el negocio, ya sea por aplicaciones decomisadas o migradas a otros equipos. Es muy común en Data Centers grandes donde no hay buenas metodologías de control.
- Dejar las luces y los monitores encendidos genera un consumo eléctrico y calor innecesario.
- Colocar los equipos apoyados unos sobre otros en lugar de disponerlos en los Racks con guías. Reemplazar una parte defectuosa dificulta la tarea, ya que requiere mover varios equipos.
- Colocar los equipos al revés, con el frente hacia atrás, eliminando calor hacia el pasillo frío y tomando aire por el pasillo caliente.

Ambiental

- Exceso de refrigeración o incorrecto flujo de aire hacia los Racks.
- Falta de controles como sensores estáticos o revisiones manuales.
- Falta de paneles obturadores en los Racks.
- Pasillos no divididos en frío y caliente o no aislados.
- Equipos conectados consumiendo electricidad y generando calor, pero que no cumplen ninguna función operativa.
- Bajar la temperatura a las unidades de enfriamiento cuando el problema está relacionado con el flujo del aire y no con la temperatura.
- Velocidad excesiva en los ventiladores de descarga de aire frío que impide el flujo correcto.

Red

- No aprovechar las capacidades redundantes de los equipos por no colocar los cables de red o electricidad necesarios para tener una doble vía.
- Colocar gran cantidad de cables desordenados ingresando al Rack que impiden el correcto flujo y la adecuada refrigeración.
- Asegurar el ancho de banda adecuado en las zonas que así lo requieran, ya que no todo el Data Center necesita una capacidad uniforme de transmisión.
- No etiquetar los cables ni los PDU, Racks, equipos de IT, etcétera.
- Confundir latencia de aplicación con latencia de red.

Seguridad

- Falta de controles de acceso acorde con la criticidad de los equipos.

- Omisión de inspecciones oculares esporádicas, ya que no siempre las cámaras registran todo. Por eso, es recomendable que periódicamente el personal de seguridad realice inspecciones de las instalaciones para detectar así desvíos a las normas establecidas.
- Instalación de ventanas hacia el exterior.
- Fallas en los cálculos de agentes extintores gaseosos para alcanzar a toda la superficie.
- Excesivos puntos de accesos al Data Center.
- El CCTV no cubre áreas importantes de vigilancia.

Operación

- Falta de las métricas iniciales para realizar comparaciones futuras.
- Ausencia de planos, diagramas de red, procesos y procedimientos escritos.
- No eliminar los puntos de falla únicos por falta de sistemas redundantes.
- Consolas de monitoreo no consolidadas, que demoraran el procesamiento de alguna alerta.
- No realizar la correcciones en los sistemas de monitoreo cuando se detectan falsos positivos.
- Falta de mantenimiento preventivo.
- Escasa comunicación cuando se realizan tareas de mantenimiento que puede llegar a causar un impacto negativo al negocio.
- Falta de análisis de riesgos o de documentación correcta.
- Las fallas en el entrenamiento o en la selección del personal son críticas, ya que el porcentaje de incidentes causados por errores humanos es mucho mayor que el causado por falla de componentes.
- Servidores que se encuentran encendidos permanentemente, pero solo se utilizan el último día hábil del mes para ejecutar un proceso que dura cuatro horas.
- Falta de control de los costos operativos, como ser electricidad, entre otros.
- Falla en los planes de BCP.

Bibliografía

Antony Adshea - Essential Guide to Disaster Recovery - 2012.

ASHRAE - Thermal Guidelines for Data Processing Environments - Expanded Data Center Classes and Usage Guidance - 2011

ASHRAE, The Green Grid - EPA - Measuring PUE for Data Centers - 2011.

BICSI Telecommunication Association. “Residential Network Cabling”, McGraw-Hill - 2003.

Bob Woolley - Top 10 Mistakes in Data Center Operations - 2010.

Brian Fortenbury- High Performance Buildings: Data Centers: UPS -2005

John Bryan, Fire Suppression and Detection Systems - 1982

Business Savvy - SOX 404 Internal Controls (White Paper) -2005

Castro Lechtaler - Fusario - Teleinformática para Ingenieros en Sistemas de Información (1999)

Chandrakant Patel- Thermal Considerations in Cooling Large Scale High Compute Density Data Centers - 2002

Richard Crane - How Things Work: Ionization Smoke Alarm; TPT - 1984

Cummings, Haag & McCubbrey - Management Information Systems for the Information Age. - 2005

Dave Patterson - A Simple Way to Estimate the Cost of Downtime - 2002

David Hornby and Ken Pepple - Consolidation in the Data Center - 2002

David Jenkins - Data Center Efficiency and Optimization -2010.

David Jenkins - The Efficient Data Center -2011.

David Moss- Data Center operating temperature: What does Dell recommend - 2009

Disaster Recovery - EC Council - 2011

Don Fitchett - What is the True Downtime Cost (TDC)? - 2002

Donna Scott - Gartner IT Security, Best Practices for Continuous Application Availability - 2005

Douglas Alger - Build the Best Data Center Facility for Your Business - 2005

Edward Wustenhoff - Building a Service Level Agreement in the Data Center - 2002.

Energy Star Program EPA - Report to Congress on Server and Data Center Energy - Law 109-431 - 2007.

Forrester Consulting - Successfully Consolidating Branch-Office Infrastructure - 2011.

Forrester Research, “Market Update: BSM/SLM Technologies,” Thomas Mendel, November 2004

Gartner - Eight of Ten Dollars Enterprises Spend on IT is "Dead Money" - 2006

Gartner Group - DCIM: Going Beyond IT - 2010.

Gary Stoneburner, Alice Goguen - Risk Management Guide for Information Technology Systems - 2002

Gomez, Incorporated - Service Level Agreements and Management - 2006.

HP - Optimizing data centers for high-density computing - 2005

HP - Cooling strategies for IT equipment - 2010.

IDC - Total expenditures assume US industrial electricity prices - 2006.

Infonetics Research, The Costs of Enterprise Downtime, North American Vertical Markets - 2005

Nestor Botta - Agentes extintores - 2010

Intel White Paper - Turning Challenges into Opportunities in the Data Center - 2007.

Jonathan Koomey (PhD), “Estimating Total Power Consumption by Servers by the US and the World” 2007

James Glanz - Power, pollution and the Internet - New York Times - 2012.

Janice Gibson - Ricoh Document Governance Index - 2012

John Rath - Data Center Strategies -2011.

Jonathan G. Koomey, Christian Belady, Michael Patterson, Anthony Santos - Assessing trends over time in performance, costs, and energy use for servers - 2009

Joseph Seymour y Terry Horsley - Los siete tipos de problemas en el suministro eléctrico - 1996.

Julius Neudorfer, Frank Ohlhorst - Data Center efficiency metrics and methods - 2010.

Kenneth Brill - Data Center Energy Efficiency and Productivity - 2007.

Kevin McCarthy - Comparing UPS System Design Configurations - 2005.

Klaus Schmidt - High Availability and Disaster Recovery - 2006

Klaus-Dieter Lange - Assessing Trends over time in performance cost and energy usage for servers - 2009.

Kurt Dillard - The Security Risk Management Guide - 2006

Lawrence Berkeley National Laboratory and Stanford University - Assessing trends over time in performance, cost and energy use for servers - 2009.

Lawrence Berkeley National Laboratory's (LBNL) - High Performance Buildings Data Centers UPS - 2005

Leo Wrobel - Evaluating Collocation Providers for Disaster Recovery and Critical Communications - 2008

Madhav Chitturi - Effect of High and Low Temperatures on UPS systems - 2005

Marc Andreessen - Why Software Is Eating the World - WSJ - 2011

Matt LePard - Essential Standby Generator System Requirements for Next Generation Data Centers - 2011

McKinsey & Company - Revolutionizing Data Center Efficiency - 2011

Michael E. Bullock - The 5 Pitfalls of Data Center Consolidation and Relocation - 2008

Michael Wallace & Lawrence Webber - The Disaster Recovery Handbook- 2011

Michel Crouhy - The Essentials of Risk Management - 2005

Mike Ebbers - Smarter Data Centers: Achieving Greater Efficiency- 2011.

Mike Hagan - Top 9 mistakes in DC planning - 2010.

National Academy of Sciences - The Internet Under Crisis Conditions: Learning from 9/11 - 2003.

National Renewable Energy Laboratory (NREL), Best Practices Guide for Energy-Efficient Data Center Design- 2011

Neil Rasmussen - Management Strategy for Network Critical Physical Infrastructure- 2003.

Neil Rasmussen - UPS Topology - 2004

Neil Rasmussen - Vatios y Voltamperios: confusión en potencia - 2010.

NFPA 75 Standard for the Protection of Information Technology Equipment, 2009

Nlyte Software paper - Getting started with Data Center Infrastructure Management - 2011

NTP 215 Ministerio de Trabajo y Asuntos sociales España - Detectores de humo - 2003

NTP 66 Ministerio de Trabajo y Asuntos sociales España - Sustitutos y alternativas para halones de extinción - 2003

Patrick Donovan - Avoiding Common Pitfalls of Evaluating and Implementing DCIM Solutions - 2012

Peter Sacco - The Difference between Data Centers and Computer rooms - 2001

Pitt Turner, John Seader, Kenneth Brill - Tier Classifications Define sites Infrastructure Performance - 2006.

Ponemon Institute - Calculating The Cost of Data Center Outages - 2011

Report to Congress on Server and Data Center Energy Efficiency Public Law 109-431,

Rich Castagna - Storage - Replication for DR Essential Guide - 2009

Rob Dearborn - The Costs of Enterprise Downtime: North American Vertical Markets 2005

Rob Menuet, Pitt Turner - Continuous cooling is required for continuous availability - 2010

Rob Snevely - Enterprise Data Center Design and Methodology - 2002.

Robert Wolfgang - Principios fundamentales de los generadores para el área de IT - 2004

Ronald Bowman - BCP for Data Centers and Systems: A Strategic Implementation Guide - 2008

Sassan Ahmadi - Mobile WiMAX - 2011

Section 404 of SOX is effectively The Forced Implementation of Best Practices - 2005.

Shadan Malik - Enterprise Dashboards - 2005

Standard on Automatic Fire Detectors. NFPA 72E - 1982.

SunGard Group- The root causes behind failed recoveries - 2012.

Susan Snedakek - Business Continuity & Disaster Recovery for IT Professionals - 2007

The Acronis global DR index: 2012 - Ponemon Institute -2012

TIA-942 - Telecommunication Industry Association, 2005

Tony Evans - The Different Technologies for cooling Data Centers - 2012.

Pitt Turner, John Seader, Kenneth Brill, “Tier Classifications Define Site Infrastructure Performance” 2006

U.S. Environmental Protection Agency, 2007

Uptime Institute - Data Center industry survey - 2012.

Uptime Institute - Procedures and Guidelines For Safely Performing Work in an Active Data Center - 2007

Victor Avelar - How Overhead Cabling Saves energy in Data Centers - 2011.

VMware, Inc. - The Top Ten Most Forgotten Things When Building a Disaster Recovery Plan - 2010

Curtis Preston - Unix Backup and Recovery - 2007

Wil Allsopp and Kevin Mitnick - Unauthorized Access: Physical Penetration Testing For IT Security Teams - 2009.