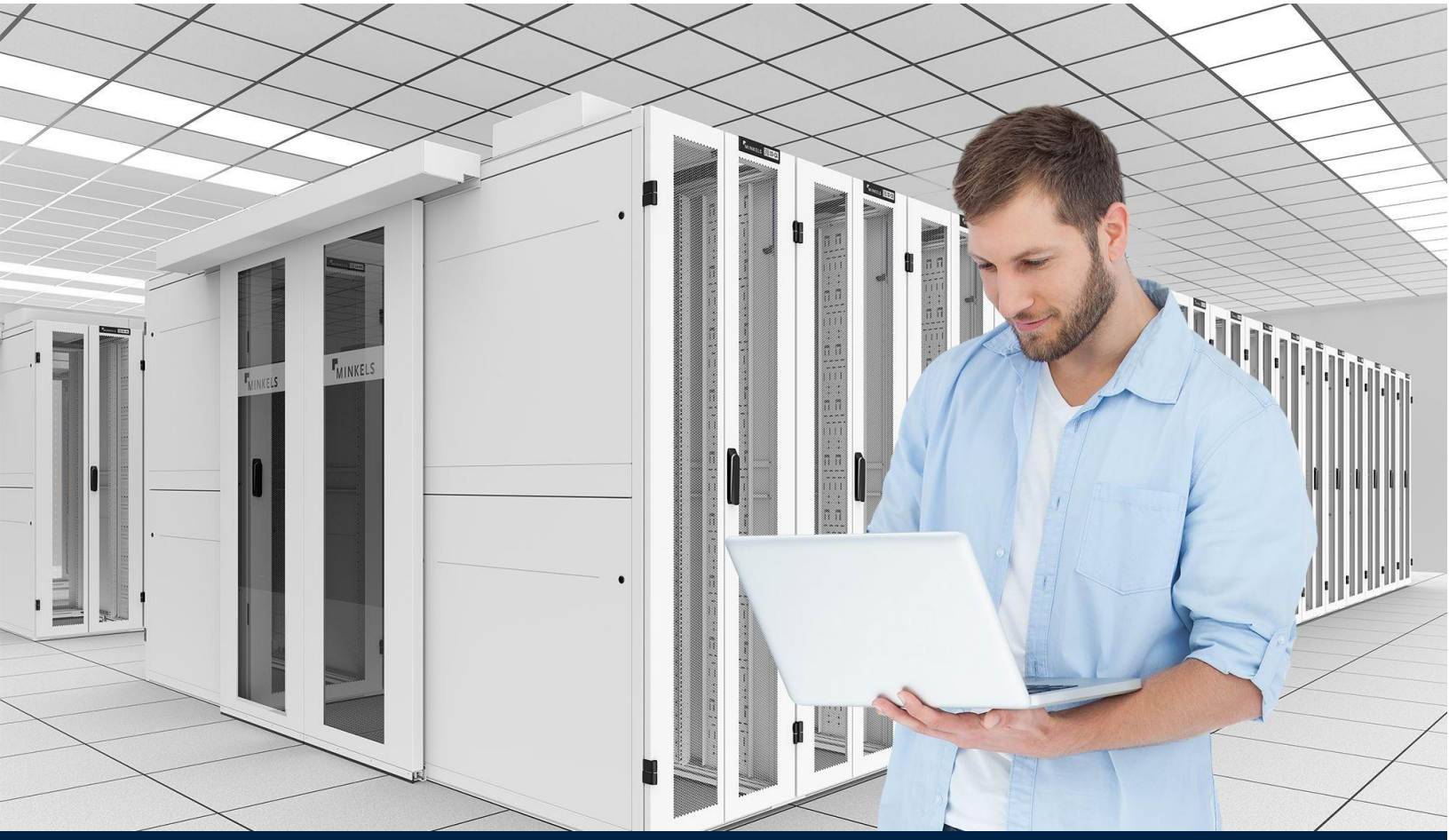
AIEP
DE LA UNIVERSIDAD ANDRES BELLO

SEGURIDAD DE CABLEADO Y DATACENTER



Unidad 1

Seguridad de Redes del Data center

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Eder Morán Heredia

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Emilia De la Cruz Barrés

VALIDACIÓN

Experto disciplinar: Gabriel Urra Varas

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Identifican infraestructura física de data center, considerando niveles y áreas funcionales.

Fuente: Ricoh-americalatina. (s/f). Recuperado en agosto del 2022, disponible en: https://bit.ly/3RYiXCn

Introducción

Cuando hablamos de datos center, nos realizamos las siguientes preguntas: **¿Bajo qué lineamientos se establecen el diseño en el data center?** o **¿Como se podría comprobar el nivel de un data center?**

En esta asignatura se abordarán temas referidos a la seguridad que engloba un data center, establecidas bajo un modelo de la norma Internacional ANSI/TIA 942. Sin embargo, hay otras regulaciones que están intrínsicamente ligadas en el sostenimiento de procedimiento de protección de un centro de datos o comúnmente llamado un data center. Para lo cual, debemos de recordar que la seguridad no solo está ligado al manejo de riesgos a todo nivel; por lo contrario, también se refiere al uso de procedimientos con el fin de establecer una continuidad del negocio, desde el más sencillo data center hasta el más complejo. Sin embargo, los estándares más desarrollados y la tecnología más importante que se ha generado a lo largo de la actividad computacional ha establecido los mejores procedimientos, los cuales seguiremos en el transcurso de la unidad.

En síntesis, establecer un data center perfecto no será permisible en la medida que se tenga conciencia en la seguridad, desde la decisión de la alta gerencia hasta la opinión de los últimos colaboradores, nivel de responsabilidad baja.

1. Seguridad de data center: Estándar ANSI/TIA-942

Actualmente en el mundo de la tecnología intrínsicamente en TI, se encuentran algunas características relacionadas con el manejo de la información, siendo uno de los ideales de la triada de la información la disponibilidad, también está la integridad de los datos, los cuales se deben preservar para asegurar la continuidad de las operaciones y del negocio, y por último la confidencialidad, el cual nos indica que solo las personas autorizadas deben de acceder a la información; en este capítulo nos centraremos en la disponibilidad. En este mundo convergen algunos factores de riesgo externos a la organización, como: el fuego, el cual puede destruir y causar a la organización grandes pérdidas. Sin embargo, solo este riesgo que tomamos como ejemplo, es un riego físico; si analizamos en profundidad podemos decir que el fuego es un riesgo critico porque ataca directamente a la infraestructura física, ya que esta debe de funcionar 24 horas del día y los 7 días de la semana. Si mantenemos el principio de la propiedad de la disponibilidad en el ejemplo mencionado, el data center debe tener la capacidad de interrelacionar de una serie de subsistemas de infraestructura que den respaldo al equipamiento crítico (*hardware*) para mantener la disponibilidad del sistema.

Así como se visibiliza este tipo de casos, no todas las actividades requieren el mismo nivel de disponibilidad y esto surgirá después de un análisis previo llamado *BIA (Busines Impact Analisis)* que cuantifica económicamente la viabilidad que produce alguna acción en contra de una indisponibilidad del data center, en un empresa u organización.

En líneas generales podemos establecer principalmente una clasificación aproximada de la criticidad de los sistemas.

1.1. La Infraestructura y el Estándar TIA-942 secundario

En abril del 2005, la organización *Telecomunication Industry Asociation* (TIA) publica sus estándar TIA-942 con el fin de unificar los criterios en el diseño de áreas de tecnología y comunicación, el principio se basa en un grupo de especificaciones para comunicaciones y cableado estructurado, estos generan los lineamientos que se deben seguir para clasificar estos subsistemas, en función de la distinta gradualidad que se pretende alcanzar.

En el Anexo G (informativo) y basado en recomendaciones del *Uptime Institute*, establece cuatro niveles de redundancia (TIERS) que pueden alcanzar en porcentajes de medición en un 99.995% de disponibilidad.

1.2. *Uptime Institute Tier Certification*

Al igual que el estándar TIA 942, también posee un sistema de clasificación por Tiers, para evaluar el rendimiento de la infraestructura en cuanto a disponibilidad. Actualmente, *Uptime Institute* ofrece 3 diferentes tipos de certificaciones:

- ***Design:*** reconoce excelencia de planeación del diseño de infraestructura.
- **Facility:** reconoce el cumplimiento de objetivos de la instalación física.

- ***Operations:*** reconoce excelencia operacional y mitigación de errores operacionales.

Todas clasificadas en un sistema de 4 Tiers, donde las primeras 2 están enfocadas a la topología e infraestructura física, y la última a la administración y mantenimiento; la cual, además, está separada en las categorías Gold, Silver y Bronze.

Si bien tanto el estándar TIA 942 como el sistema de clasificación de *Tiers de Uptime Institute* catalogan la infraestructura con Tiers de I a IV, ambas clasificaciones presentan diversas diferencias. Es por eso que entre ellas han llegado a un acuerdo, con tal de diferenciar claramente sus clasificaciones, en donde TIA 942 elimina la palabra Tier de su sistema de clasificación.

El estándar TIA 942 es uno de los estándares más importantes dentro de los diseños de los data center, ya que describe especificaciones para variados elementos dentro del diseño de la infraestructura física, como son el diseño de redes, sistemas redundantes de energía y enfriamiento, sistemas de seguridad, protección contra desastres naturales, etc.

El estándar es mundialmente reconocido debido a que establece una topología de Data Center modificable, la cual puede ser aplicable a cualquier Data Center de cualquier tamaño en cualquier lugar.

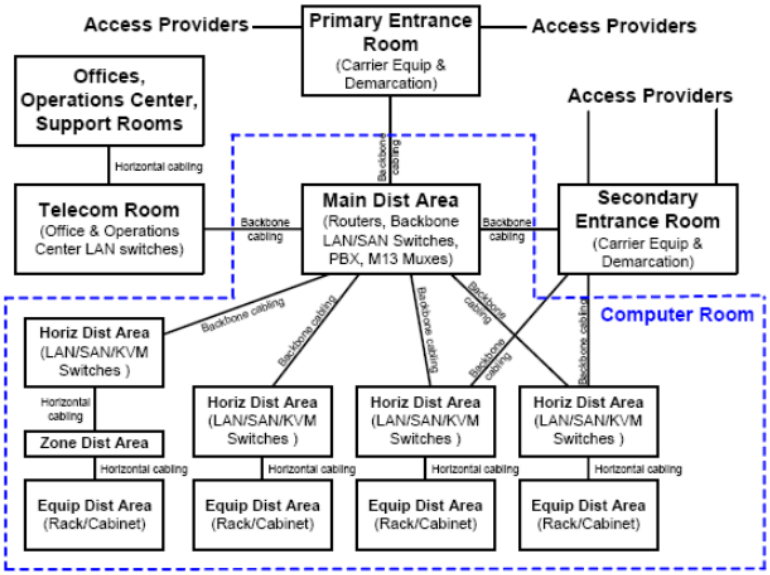


Figura 1: Topología básica de un Data center.

Fuente: https://bit.ly/3J6doOb

A su vez divide la infraestructura soporte de un data center en cuatro subsistemas a saber:

- **Telecomunicaciones.**
- **Arquitectura.**
- **Sistema eléctrico.**
- **Sistema Mecánico.**

Esta forma de clasificación es aplicable en forma independiente a cada subsistema de la infraestructura (telecomunicación, arquitectura, eléctrica y

mecánica.) También hay que considerar que la clasificación global del data center tiene todos los subsistemas TIER IV excepto el eléctrico que es TIER III.

Es importante considerar cuando se pretende la adecuación de data center actuales a TIER IV, en lugares como Sudamérica, hay ubicaciones difíciles de salvar en los emplazamientos o edificios que alojaran a la data center. Entonces se lograrán mediante el diseño desde cero con el estándar como guía. La norma describe, resumidamente, los distintos tiers de la manera que sigue.

1.2.1. TIER I: Data center Básico

Un data center *TIER* I es susceptible a interrupciones tanto planteadas como planificadas, cuenta con los sistemas de extracción de aire, aire acondicionado y distribución de energía, cabe la posibilidad de contar con piso técnico, UPS o generador eléctrico; si posee este último dispositivo puede tener redundancia eléctrica, la carga máxima para sistemas críticos es del 100%. También deberá estar fuera de servicio al menos una vez al año, por razones de mantenimiento y/o reparaciones físicas. Cuando ocurran situaciones de urgencia pueden conllevar a paradas más frecuentes, generando errores de la operación o fallas en los componentes, el promedio de disponibilidad máxima es del 99.671% del tiempo.

1.2.2. TIER II: Componentes redundantes

Son ligeramente menos susceptibles a interrupciones, tanto planificadas como no planificadas, cuentan con piso falso, UPS y generadores eléctricos. Sin embargo, están conectados a una sola línea de distribución. Su diseño es "lo necesario más uno (N+1), lo que existe al menos un duplicado de cada componente. La carga máxima de los sistemas en situación crítica es del 100%,

El mantenimiento en la distribución eléctrica o en otros componentes de la infraestructura puede causar una interrupción del procesamiento. Su disponibilidad máxima de la data center es del 99.749% del tiempo.

1.2.3. TIER III: Mantenimiento Concurrente

Permiten realizar cualquier actividad planeada sobre cualquier componente de la infraestructura, sin interrupciones en la operación, está incluido el mantenimiento preventivo y programado, reparaciones o remplazo de componentes, agregar o eliminar elementos y realización de pruebas de componentes o sistemas entre otros.

Se deber de considerar una suficiente capacidad y doble línea de distribución de los componentes, de tal manera que sea posible realizar mantenimientos o pruebas en una línea, mientras que la otra atiende la totalidad de la carga. En este TIER, actividades no planeadas como errores de operación o fallas espontaneas pueden todavía causar interrupciones, la carga máxima en los sistemas en situaciones críticas es del 90%.

Muchos data center TIER III son diseñados para alcanzar el nivel IV, de tal manera que se prepara para el siguiente nivel cuando los costos del negocio lo justifiquen. La disponibilidad del data center máxima es del 99.982% del tiempo.

TIER	% Disponibilidad	% Parada	Tiempo anual de parada
TIER I	99,67%	0,33%	28,82 horas
TIER II	99,74%	0,25%	22,68 horas
TIER III	99,982%	0,02%	1,57 horas
TIER IV	100,00%	0,01%	52,56 minutos

Figura 2: TIERs de un Data center.

Fuente: https://bit.ly/3OY7FeQ

1.2.4. TIER IV: Tolerante a fallas

Provee la capacidad de realizar cualquier actividad planeada o no planificada sin interrupciones en las cargas críticas, pero además de la disponibilidad y su funcionalidad es tolerante a fallos y permite seguir operando ante un evento critico no planificado, esto se realiza en base a dos líneas de distribución simultáneamente activas, típicamente es una configuración *System + System*. Estos dos sistemas de UPS independientes, todos con el nivel de redundancia de N+1, la carga máxima es del 90% y persiste un nivel de exposición a fallas del 90%, también persiste frente a situaciones de incendio o por que una persona active una alarma de evidencia o por un apagado de emergencia, también conocido como: *Emergency Power Off* (EPO). Los cuales deben de existir para cumplir con los códigos de seguridad contra incendios o eléctricos. Su disponibilidad es del 99.995%.

Hay que tener en cuenta que para un TIER IV se contempla la única parada que se produce por la actividad de un EPO y sucede solo una vez cada cinco años.

No obstante, para la exigencia que demanda un TIER IV algunas empresas u organizaciones manifiestan la necesidad de una disponibilidad de cinco nueves ósea del 99.999%, esto quiere decir de 5 minutos al año de interrupción.

2. Seguridad de áreas funcionales y espacios operacionales

Las empresas en todo el mundo están inteligentemente interconectadas digitalmente y muy dependientes de internet de la red y la nube, manipulando gran cantidad de información, lo que hace una necesidad de un espacio físico donde procesan y almacenan los datos.

2.1. Riesgos de seguridad

Si hablamos de incidentes de seguridad en la red lo primero que pensamos es hablar de ciberseguridad, piratería informática, falta de copias de seguridad, instalación de un antivirus, configuración de firewall, contar las ultimas actualizaciones de seguridad, entre otras.

Pero con esa seguridad lógica no estamos cien por ciento seguros que estamos protegidos y acá nace la pregunta: **¿Y qué sucede con la seguridad física?**

No disponer de una buena seguridad vuelve vulnerable y hay pocas áreas donde las interrupciones en los negocios sean tan costosas como en el almacenamiento de datos. No importa el tamaño del centro de datos de la organización ya que tienen todos los riesgos de ser vulnerable, ya sea de forma intencionada o de manera accidental. Por ello, se debe tomar las mayores medidas de seguridad que permitan a las organizaciones crear un entorno robusto con el único fin de proteger los datos.

Los CPD (centro de procesamiento de datos) están expuestos a riesgos físicos de otra naturaleza, como:

- Subida o caída de tensión.
- Temperatura incorrecta por fallos de quipos de climatización o de mal diseño.
- Incendios.
- Inundaciones y humedad.
- Humos, polvo y partículas en el aire que dañan los discos duros y los ventiladores de los dispositivos.
- Accesos de personal autorizado.
- Manipulaciones incorrectas de los equipos.
- Vandalismo, robos, etc.
- Movimientos sísmicos.

En el mundo de la seguridad física los data center se puede segmentar en cuatro niveles, en base a las capas de seguridad, los cuales son:

- Seguridad del perímetro.
- Seguridad de las instalaciones.
- Seguridad de las salas de Ordenadores.
- Seguridad a nivel de racks.

2.1.1. Seguridad Perimetral-Primera capa

El objetivo principal de esta capa es la protección del data center, se basa en las tres D´s: **Detener, Detectar, y Demorar.**

Existen diferentes tipos de sistemas para proteger el data center, desde el elemento más sencillos hasta el elemento más complejo, como, por ejemplo: se pueden mencionar desde las más simples hasta los métodos más sofisticados, como: alarmas infrarrojas y detectores de presencia, todo dependerá del enfoque y el tipo de empresa, así como el modelo de dato que maneja.

2.1.2. Seguridad de las Instalaciones-Segunda capa

El objetivo de esta segunda capa se basa en restringir el acceso, en caso de que se presente una situación en el perímetro, como: la vigilancia en los interiores, sistemas de identificación, métodos de verificación, uso de *fotochecks*, huellas dactilares, etc.

El tipo de instalación determinará los niveles necesarios de seguridad con relación al equilibrio que se debe considerar entre la seguridad requerida y la experiencia de las visitas; por ejemplo, un sistema con complejidades en su acceso tan estricto podría ser configurado en un data center donde acceden varias personas de forma continua.

2.1.3. Seguridad de las Salas de computadores-Tercera capa

EL fin de esta capa es restringir el acceso a través de múltiples métodos de verificación, el monitoreo de los accesos principales y contar con redundancia energética y de comunicaciones.

El acceso debe estar restringido al pequeño grupo de personas. Deberán cumplir con las restricciones de acceso a esta área y puede ser clasificado a nivel de confiabilidad, con las siguientes preguntas:

- **"Lo que sabes"**: Es la menos confiable y hace referencia principalmente a contraseñas.
- **"Lo que tienes"**: Categoría intermedia la cual engloba dispositivos como tarjetas o llaves de acceso.
- **"Lo que eres"**: Esta categoría es la más confiable y se basa en la autenticación biométrica.

2.1.4. Seguridad a Nivel de Racks-Cuarta capa

Es una de las más importantes y efectivas para minimizar las amenazas internas, la mayoría de los data center enfocan su atención en las tres primeras capas, pero la ausencia de control en los racks puede resultar una costosa fuga de información por un empleado con malas intenciones.

Algunas consideraciones importantes para esta cuarta capa de seguridad son:

- Se recomiendan sistemas de bloqueo electrónico para racks de servidores.
- Sistemas biométricos para acceso a los racks.
- Videovigilancia IP para captura de imágenes o clips de la actividad de las personas en los racks.

Para establecer lineamientos de seguridad en la construcción de un data center se sugiere la norma **EN 50600**, ya que establecen estándares de diseño para la "disponibilidad, seguridad y eficiencia de la energía para toda la vida útil del centro de datos". Para ello se debe establecer previamente un análisis de riesgo y de negocios, que debe ser conferida a la base del estándar y sobre la base de los requisitos estandarizados, se especifican los niveles de disponibilidad y protección para el funcionamiento del data center.

Uno de los principales puntos es el envolvente ya que nos asegura una seguridad estructurada contra cualquier riesgo que se avizore desde el exterior como: intrusiones, vandalismo, inundaciones, polvo, incendios, etc. Por ello, la norma establece lineamientos que deben cumplir una serie de requisitos mínimos que certifiquen ser efectivos contra las amenazas, evitando la penetración de elementos contaminantes, como: partículas, líquidos y gaseoso. Para ello las puertas, techo y tendido de cables debe garantizar que al menos cuente con un modelo IP55. Con respecto a la resistencia del fuego y la protección contra incendios, la construcción de los data center, es importante que cuente con una resistencia en un 90% en todo su conjunto de suelos, paredes y techos.

Otras de las normas que aportan en la estructura segura de un data center, son los requisitos establecidos en la norma EN1363, para la protección

estructural contra el manejo del fuego, utilizados en un centro de datos. Cuyo diseño debe seguir la norma EN1047-2. Por ejemplo, en caso de incendio interactúan algunos elementos constructivos considerados en la norma EN1363 como Pladur, Hormigón, piedra caliza, etc. Estos desprenden gran cantidad de humedad al ambiente, provocando averías en los servidores del CPD, en una sala de dimensiones 5 x6 x2.5m se estima una acumulación de hasta 870 litros de humedad.

En la seguridad antirrobo, las puertas deberían ser de una resistencia mínima de clase RC 3 (antigua WK3) según la norma **EN1627**. La seguridad de las puertas de acceso es para poder controlar que las personas que acceden al data center sean exclusivamente aquellas que hayan sido previamente autorizadas. También se requiere en las instalaciones un sistema de control de acceso y un sistema de videovigilancia en el interior y en sus inmediaciones. Deberá contar con sistemas de apertura segura, sensores en la puerta y dispositivos de autorización y grabación de imágenes, tanto del interior como el exterior de las instalaciones.

También es necesario implementar seguridad en el acceso a los racks de los servidores, ya sea mediante simples cerraduras con llave o lectores de control de acceso en las puertas, que permita un registro de las personas que han accedido a ellos, esto se debe a que todas las personas con acceso autorizado al CPD no tienen acceso a la zona de racks.

Otra de las disposiciones para un centro de datos es protegerlo contra uno de los actores más dañinos para los equipos electrónicos, como: humo o fuego. Por ello, resulta imperativo dotarlo de un buen sistema de detección y extensión de incendios.

Para poder garantizar una rápida respuesta y evitar cualquier conato de incendios, con el tiempo es conveniente implementar un sistema de tecnología de detección de humo por aspiración o ASD *(Aspirating Smoke Detection)* ya que estos son capaces de detectar un incendio con tanta antelación que se anticipa a la aparición de la llama.

Con un buen sistema de detección se hace necesaria la instalación de un sistema de extinción automático de incendios. Estos pueden variar en función de las instalaciones y el área de proteger, siendo principalmente sistemas mediante agentes extintores gaseosos o agua nebulizada. En el primero de los grupos de debe prestar especial atención a soluciones respetuosas con el medio ambiente y que no ocasionen daños a los equipos.

En el caso de la monitorización del centro de datos es posible detectar cualquier incidencia y actuar en consecuencia con rapidez, lo sistemas de monitoreo recogen las diferentes señales a controlar y son capaces de generar pre-alarmas y alarmas, asociados a través de SMS, emails u otros medios. Entre los principales parámetros a monitorizar se encuentran las condiciones ambientales (temperatura y humedad) de forma estratégica en el CPD, así como la detección de fugas de líquidos. También resulta interesante la recepción de alarmas de otros sistemas mediante su integración, tales como: UPS, unidades de climatización, sistemas de conmutación, cámaras auxiliares de protección en cuadros central de incendios, etc. Este tipo de integraciones se suelen realizar a través de contactos secos o protocolos de comunicaciones tipo SNMP.

2.2. Diagrama de Distribución

Las áreas funcionales en un centro de datos bien diseñado se deben plantear de manera que garantice lo siguiente:

- Se puede reasignar fácilmente el espacio para satisfacer necesidades cambiantes.
- Se pueden manejar fácilmente los cables de los tendidos y que no superen las distancias recomendadas.

2.2.1. Cuarto de Entrada

Alberga al equipo de operadores de telefonía y el punto de demarcación, puede estar dentro de la sala de cómputo, pero la norma recomienda que este en un cuarto aparte por razones de seguridad. Si está ubicado en el cuarto de cómputo, deberá estar consolidado dentro del área de distribución principal.

2.2.2. Área de Distribución Principal

El área de distribución principal alberga al punto de conexión cruzada para el sistema de cableado estructurado del centro de datos. Esta área debe estar ubicada en una zona central para evitar superar las distancias de cableado recomendados y puede contener una conexión cruzada horizontal para un área de distribución de un equipo adyacente.

2.2.3. Área de Distribución Horizontal

El área de distribución horizontal es la ubicación de las interconexiones horizontales, el punto de distribución para el cableado hacia las áreas de

distribución de equipos se debe de considerar que puede haber más de un área de distribución, ya sea horizontal según el tamaño del centro de datos y las necesidades.

2.2.4. Área de Distribución de Zonas

Es el área de cableado estructurado para los equipos que van en el suelo y no pueden aceptar paneles de parcheo. Como, por ejemplo, se puede citar a las computadoras centrales y los servidores.

2.2.5. Área de Distribución de los Equipos

Es la ubicación de los gabinetes y racks de equipos, la norma específica que los gabinetes y racks se deben colocar en una configuración *hot aisle/cold aisle* (pasillo caliente/pasillo frio) para que se disipen de manera eficaz el calor de los equipos electrónicos.

3. Distribución segura de equipamiento y hardware para montaje de un rack

Diferentes motivos determinan que tan grande o pequeños va a ser el ambiente de servidores los cuales incluyen:

- La cantidad de colaboradores que trabajaran ahí.
- El número y tipo de servidores, los equipos que el centro de datos hospedara.
- El tamaño de las áreas alrededor del cuarto de servidores que dependen de la infraestructura en planificación.

Dentro del centro de datos es obvio que cuanto más pequeño es el centro es menos costoso de operar y mantener que uno más grande. La mejor practica es diseñar el centro de datos con un tiempo de vida prologando e intentar expandir el entorno de los servidores cuando estos prácticamente llenen el centro de datos.

Para considerar el diseño de un centro de datos, se debe determinar la capacidad de este basado en el diseño de los RLU´s o *Rack Locations Units*, por sus siglas en inglés, y para calcular el espacio necesario en el cual aplicaremos dos métodos.

3.1. Diseño de los RLU´s

El sistema de los RLU su principio completamente escalable y flexible que puede ser usado para calcular las necesidades de los equipos de un data

center de cualquier tamaño, ya sea de 100 o 1000 metros cuadrados. En el centro de datos, diversos dispositivos son instalados en racks, este deberá ser ubicado en un lugar específico en el piso del centro de datos y los servicios como energía enfriamiento, conectividad, etc.; deben ser entregados en esta ubicación. A esto generalmente se lo llama "*Rack Location*" y todos los servicios que son entregados en esta ubicación tienen su unidad de medida, ya sea en vatios, metros, kilos, etc.

Existen requerimientos que ayudan en el diseño los cuales son:

- **Energía** (cantidad de solicitudes de energía por equipo suministrado)
- **Enfriamiento** (BTU por hora).
- **Espacio Físico** (cantidad de piso necesario para alojarlos).
- **Peso** (Peso de Rack).
- **Conectividad** (Como se conecta a la red).
- **Capacidad funcional** (cuanto poder de procesamiento tiene, memoria física, espacio de disco, etc.).

Los RLU´s basado en estas especificaciones, pueden ser usados para determinar qué cantidad de energía, enfriamiento, conectividad, espacio físico y peso, que el piso puede soportar para el rack, solo en grupos o en combinación con otros equipos. También para saber cuántos Racks y que configuraciones del data center y utilitarios externos pueden soportar.

EL RLU trabaja en ambas direcciones, determinando los usos necesarios para acomodar y alimentar los equipos, también ayuda en los cambios de

cantidades y configuraciones de los equipos, para aceptar cualquier limitación de recursos.

Para establecer los RLU´s se debe examinar los 6 criterios usados, como: espacio físico, conectividad, capacidad funcional, corriente, peso, enfriamiento.

3.1.1. Energía

La cantidad de energía, número de *breakers*, y como el centro de datos es cableado, son todos dependientes de las necesidades de los equipos planeados, para lo cual se necesita conocer lo siguiente:

- Necesidades de energía en el rack.
- Tipos de enchufe.
- El tipo de voltaje y el amperaje.
- Si es monofásico o trifásico.
- Que cantidad de energía ocupara el Rack.

3.1.2. Enfriamiento

El rack de dispositivos produce calor y requiere una cantidad especifica de enfriamiento para mantenerlo activo. Las solicitudes de los HVAC deben ser planeados con cuidado, para ello se debe considerar un numero especifico de BTU´s por hora, esto generalmente se obtiene de las especificaciones del fabricante y el área que ocupa cada Rack para considerar el enfriamiento de los diferentes componentes.

Estas dimensiones también denotan las áreas mínimas que deben ser dejadas por el otro equipo, para dejar fluir el aire. La figura 2.3 indica ejemplos de las dimensiones de enfriamientos generales de racks con direcciones de aire.

3.1.3. Conectividad

Se debe considerar la red y el cableado dentro de datos. Generalmente se hace con la categoría 5e, 6e o fibra multimodo. Cuando se determina la conectividad como parte del RLU; lo principal es determinar el número de conexiones para el rack, para permitir que otros periféricos se conecten y utilicen el canal.

3.1.4. Peso

Es importante considerar el peso del componente en su conjunto, partiendo desde el principio del rack y luego ir sumando los equipos conectados. Cada rack tiene su peso específico, pero varían entre un modelo y otro. Para ello, se debe considerar otros conceptos, como:

- **Carga total que soporta el piso:** es importante conocer la carga total que el piso y la estructura van a poder soportar. Y en caso de que exista una cámara de aire entre el piso y el suelo, es importante considerar el peso total.

- **Carga total del azulejo:** tiene que ver con el azulejo simple y la carga que debe soportar; en ocasiones hay azulejos sólidos, perforados y rayados, esto dependerá del fabricante.

- **Punto de Montaje del Azulejo:** puede ser escogido para soportar en el peor de los casos, los puntos de montaje del rack más pesado,

generalmente es ¼ del peso del rack, pero debe ser multiplicado por 2 y no debe exceder la carga total del azulejo.

3.1.5. Espacio Físico

Aquí solo el dimensionamiento es posible, el cálculo y el espacio que tendrá en el data center. Por ejemplo: el ancho(a) y la profundidad del rack(b); las dimensiones del sistema de enfriamiento en el rack y el espacio libre necesario para pasillos(c), también rampas de accesos libres de circulación de aire.

3.1.6. Capacidad Funcional

La capacidad funcional es requerida únicamente para determinar la cantidad y el tipo de RLU que se va necesitar para adaptarlo al proyecto y la realidad; es importante conocer esto y determinarlo junto con los requerimientos funcionales.

3.2 Método del Tamaño Basado en Empleados

Una manera de determinar el tamaño del centro de datos es la cantidad del número de empleados que se alojarán en el centro de datos, donde cada uno de ellos ocupará un lugar, solamente hay que considerar los colaboradores cuyos roles o actividades están asociados al centro de datos tanto con servidores o dispositivos de red.

Entender que proporción de piso del data center va a ocupar cada colaborador para determinar el tamaño. Lo ideal es establecer el número de empleados por

metro cuadrado, para una mínima cantidad de piso en cualquier centro de datos, se tiene que considerar aquellos espacios no funcionales y que son indiferentes si el sitio es grande o pequeño. Este espacio sin servidores incluye

áreas de la infraestructura de los equipos como unidades de poder, sistemas de ventilación, rampas de acceso o los pasillos, entre otros. Estas áreas no crecen proporcionalmente como el resto de los espacios del centro de datos,

Empleados	Tamaño Aproximado del Centro de Datos
Menos de 100	• 10 pies cuadrados por empelado. • 1 metro cuadrados por empelado.
200-250	• 5 pies cuadrados por empelado. • 5 metros cuadrados por empelado.
400-500	• 4 pies cuadrados por empelado. • 4 metros cuadrados por empelado.
1.500-6.000	• 2 pies cuadrados por empelado. • 2 metros cuadrados por empelado.
1.5000	• 1 pie cuadrado por empelado. • 1 metro cuadrado por empelado.

que si lo hacen para ello hay que considerar la siguiente tabla:

3.3. Método del Tamaño Basado en Equipos

En este caso se puede diseñar este criterio en base al número y tipo de servidores que va a hospedar el data center. La primera cosa a realizar es determinar las dimensiones peso y forma de lo equipos. La idea es obligar a los fabricantes fabricar los servidores más compactos, es decir más pequeños en altura, pero más largos que otros modelos; lo cual puede incrementar la profundidad que tengan las columnas de servidores en el data center, la figura mostrada a continuación ha realizado la adaptación de una pieza de hardware en un centro de datos, sin pensar en el resto de los componentes a ser usados.

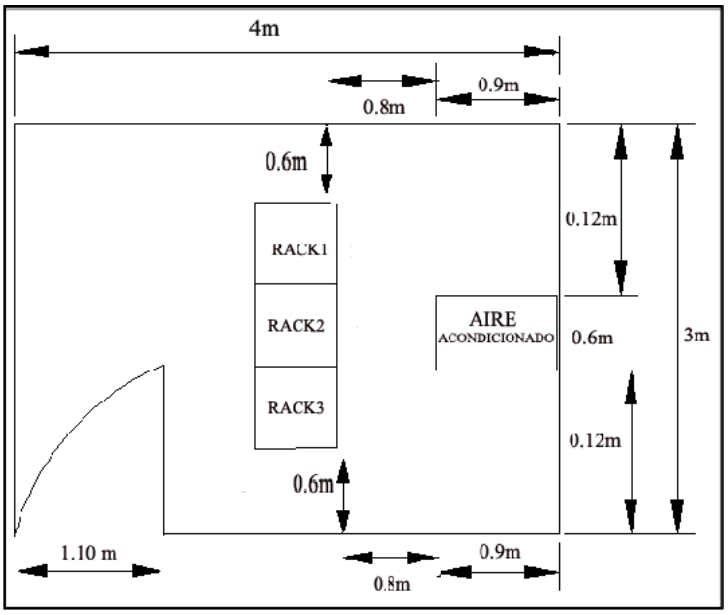


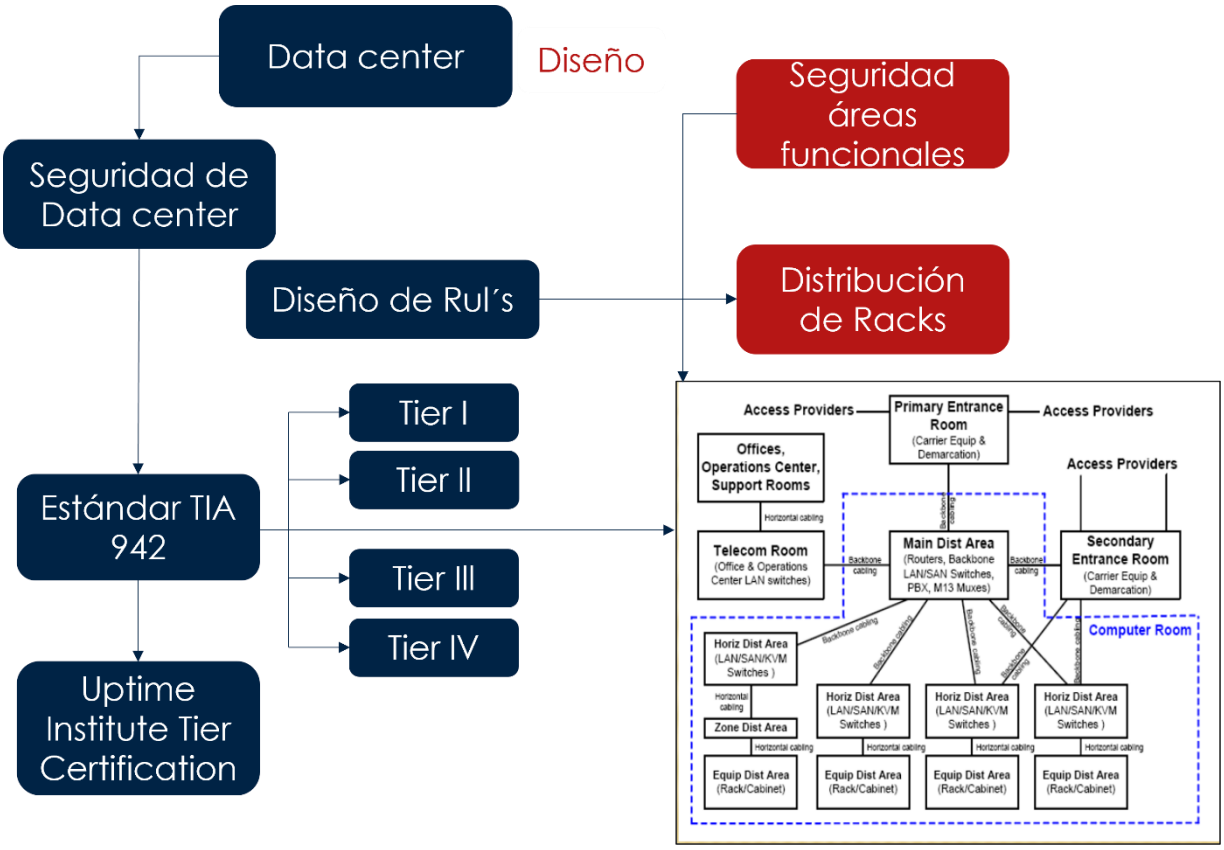
Figura 3: Racks ubicación en data center.

Fuente: https://bit.ly/3BHZxMC

Una vez encontrada el área deseada es importante destacar las diferentes áreas que va tener el centro de datos como cuarto eléctrico, cuarto de red, área de carga, cuarto de preparación de equipos, cuarto de almacenamiento, centro de comandos, áreas de medios de almacenamiento y áreas de servicio para vendedores.

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



¿Bajo qué lineamientos se establece el diseño en el data center?

Dentro de los diseños de la infraestructura de los data center y basado bajo normas establecidas como la TIA 942 , se establece que los lineamientos establecidos para cubrir cualquier dimensionamiento que se desee establecer, desde el más pequeño de los centros de datos hasta el más complejo, suponen características de seguridad complejas.

Referencias bibliográficas

- TIA Standard. (2005). *Telecommunications Infrastructure Standard for DataCenter*. Recuperado en agosto de 2022, disponible en: https://bit.ly/3bxb9XX

- Abts, Dennis. *High performance datacenter networks: architectures, algorithms, and opportunities*. ISBN: 9781608454020. Disponible en: https://bit.ly/3oWyGEF