Información Importante

MEJORES PRÁCTICAS PARA IMPLEMENTAR EN UN CENTRO DE CÓMPUTO SIGUIENDO LAS NUEVAS TENDENCIAS, NORMATIVA Y LOS ESTÁNDARES DE SEGURIDAD EN PRAGCON.

AUTOR DEL TRABAJO: ADRIANA LORENA CARTAGENA MUÑOZ

PROYECTO PARA OPTAR AL GRADO DE: INGENIERA INFORMÁTICA

PROFESOR DIRECTOR: CARLOS ALBERTO PUENTES PINTO

UNIVERSIDAD DE LA SABANA

FACULTAD DE INGENIERÍA

2014

CHÍA – COLOMBIA

Tabla de contenido

Tabla de figuras

Índice de tablas

Lista de abreviaturas

APC: American Power Conversion

ASHRAE: Sociedad Estadounidense de Ingenieros en Calefacción, Refrigeración y Aire Acondicionado

NCPI: Infraestructura física de red

NFPA: National Fire Protection Association

PUE: Efectividad del uso de la energía

TIA: Asociación de Industria de Telecomunicaciones

UPS: Sistema de alimentación ininterrumpida

Agradecimientos

Le doy gracias a mi familia que siempre me apoyo durante toda mi carrera y estuvo acompañándome en todo momento. Gracias a ellos logré cumplir mis metas y salir adelante durante este camino.

Agradezco a mi director de tesis, Carlos Puentes, que me guio y me apoyo a lo largo de este trabajo, mostrando su compromiso e interés por que todo saliera adelante.

Resumen

La disponibilidad y reguardo de la información es de vital importancia para el desarrollo de las organizaciones. Para llevar un control adecuado sobre la información de una compañía, una de las medidas a tomar, es la creación de un espacio físico especializado para el manejo de equipos informáticos. Dentro de este espacio, conocido como centro de cómputo, se llevan a cabo ciertas operaciones que permiten el monitoreo y la seguridad de la información de la compañía. Adicionalmente, se ejecutan y optimizan procesos críticos de la organización. De esta manera, se gestiona la continuidad de las actividades laborales, minimizando el riesgo de interrupciones y pérdida de información.

Al momento de diseñar e implementar un centro de cómputo, es importante tener en cuenta factores como: Seguridad de la información, seguridad física, optimización de los recursos y tendencias a futuro. Para cumplir estos aspectos, se deben entender los detalles más generales y relevantes de los estándares para un centro de cómputo. Se hace énfasis y se trata de cumplir con los principios básicos de la seguridad de la información (disponibilidad, confidencialidad, integridad). Adicionalmente, se analizan aspectos como las especificaciones ambientales y de seguridad dentro de un centro de datos como: Suministro de alimentación eléctrica, sistema de aires acondicionados, control de acceso, sistema de extinción de incendios, códigos de seguridad de construcción, entre otros. Por último, se estudian las tendencias de los centros de cómputo, enfocándose en el apoyo ambiental y a futuro una eficiencia energética. A partir de esto, se pretende cumplir con los niveles mínimos para un centro de cómputo. Del presente análisis, nace la idea de crear un documento de mejores prácticas para realizar las adecuaciones óptimas para el funcionamiento del centro de datos de una empresa mediana como Pragcon[1], llevando así un control interno de lo que ocurre en este espacio.

[1] Por políticas, no es posible compartir el nombre de la empresa. Pragcon, es el nombre ficticio que se le da a la empresa para realizar este estudio.

1. Descripción

1.1. Pregunta de investigación y su justificación

¿Cuáles son las mejores prácticas y metodologías a seguir para la adecuación del centro de cómputo de una empresa mediana como Pragcon en Bogotá?

Actualmente la mayoría de las empresas están adecuando un espacio físico para el almacenamiento de equipos informáticos y el control de los mismos, creando así un lugar especializado donde se alberga y maneja la mayor parte de la información de la compañía. Al momento de crear estos espacios, conocidos como centros de cómputo, existen unas normas y estándares a seguir. Entre estos temas, se tienen en cuenta los estándares de seguridad física, seguridad de la información y las tendencias a futuro a nivel de data center. Para evitar fallas en un centro de cómputo, se deben seguir unas recomendaciones y mejores prácticas para garantizar el funcionamiento actual y futuro de este centro. Al contar con una metodología de trabajo para la creación o modificación de un centro de cómputo, esta se puede aplicar a otras empresas similares o a sedes de la misma empresa que estén ubicadas en otra cuidad o país. En este momento, no se lleva un control ni un manejo adecuado sobre lo que ocurre en el centro de cómputo de Pragcon. Por esto, es de gran importancia implementar una metodología a seguir para dar una claridad y lineamientos en el tema. De esta manera, las personas que actualmente están involucradas en el manejo del centro, estén al tanto de los pasos a seguir para mantener en óptimas condiciones el lugar o para que en el momento que se presente alguna falencia, se actúe de la forma apropiada.

Inicialmente, se crea el centro de cómputo de Pragcon con un proveedor externo, el cual a partir de su experiencia, plantea un diseño. En ese momento, no se dejan en claro las buenas prácticas y metodologías a seguir, por esta razón a los 4 años de creado este centro, se encuentran múltiples falencias que causan un gran riesgo para la compañía. Para poder tener un centro de cómputo que se mantenga en el tiempo, en primera instancia, es necesario realizar las adecuaciones para cumplir con los

estándares mínimos. Adicionalmente, llevar un control a partir de ese momento para no caer nuevamente en las falencias actuales. Para esto, se van a identificar y extraer los aspectos generales y significativos de los estándares más utilizados para el desarrollo de un centro de cómputo, así como estándares de seguridad de la información, generando un valor agregado para la empresa. Este proceso consta de la validación de estándares amplios y documentos extensos que van a ser aplicados a las necesidades de la empresa. Con esto, se analiza el alcance que podemos tener en la empresa Pragcon en Bogotá y cuáles son los aspectos más relevantes a tener en cuenta de cada uno de ellos. Así, se crea un documento de fácil entendimiento que se adecue a las necesidades de la empresa y sirve de guía a las personas encargadas de administrar y gestionar el centro de cómputo para mantenerlo en óptimas condiciones.

1.2. Revisión de la literatura o estado del arte

"La combinación de la necesidad de monitorear los presupuestos operativos de los centros de datos (incluido el ahorro de energía) y la disponibilidad de la nueva tecnología obligará a las empresas a reconsiderar las arquitecturas de hardware de sus centros de datos" (Analistas de Gartner, 2012).[2]

Los centros de cómputo son uno de los activos más importantes de las compañías, pues representan una gran parte de la existencia de la misma. Por esta razón, es de vital importancia adecuar estos lugares, teniendo en cuenta los riesgos que se corren al tener la información en un lugar específico y sabiendo que las tendencias tecnologías siempre van en constante cambio. Anteriormente, los centros de cómputo eran salones muy grandes llenos de equipos, cables y dispositivos de red. En los últimos años, se ha notado un gran cambio en los centros de cómputo, pues "las proporciones físicas externas se han ido reduciendo a la vez que la capacidad de almacenamiento ha ido aumentando" (Fernández, 2009). Todo este cambio se da principalmente por la implementación de la virtualización que afecta el almacenamiento y procesamiento de la información. La innovación de los sistemas

[2] (Analistas de Gartner, 2012)

globales, permitiendo una mayor disponibilidad y eficiencia en los sistemas, se ve reflejada una evolución permanente de los centros de cómputo. Para poder llevar a cabo estas actualizaciones y tener un control sobre el cambio continuo, se deben tener unos estándares a seguir, para poder monitorear continuamente, detectar las falencias y solucionarlas tan pronto como sea posible.

Un caso puntual, es el centro de cómputo de la empresa Pragcon en Bogotá, el cual está generando un gran riesgo para la compañía por cuestiones de seguridad y organización. En los últimos meses, en este espacio se han estado guardando cajas, dándole un uso inapropiado y poniendo en riesgo la seguridad de la información y la disponibilidad de los recursos. Adicionalmente, el centro de cómputo cuenta con algunas falencias, aunque se cuenta con ciertas medidas de seguridad, estas no están siendo aplicadas correctamente debido a que no se tiene un estándar a seguir, no se realiza una gestión ni monitoreo adecuado.

Para poder aplicar las normas y los estándares necesarios, se realizará un estudio teniendo en cuenta centros de cómputo actuales e información relacionada del tema tomada de diferentes fuentes. Por otro lado, se revisaran las falencias actuales de este centro de cómputo y cuáles son las mejores decisiones a tomar para poder cumplir con las normatividades mínimas de un centro de datos. Se relacionaran todos los aspectos a evaluar en el documento: Mejores prácticas para implementar en un centro de cómputo siguiendo las nuevas tendencias, normativa y los estándares de seguridad en Pragcon. El documento incluirá la metodología y buenas prácticas a seguir con las normas y sus aspectos más relevantes que pueden ser aplicados al centro de cómputo de Pragcon. De esta manera, se podrá realizar un seguimiento constante y asegurarse que todas las exigencias mínimas necesarias se están cumpliendo. Por último, se evalúan las tendencias de los centros de datos y el proceso de mejora continua optimizando los recursos y el uso efectivo de la energía.

1.3. Marco teórico

En la actualidad, los centros de cómputo, acompañan y dan respuestas al día a día de una compañía, incorporando nuevas tecnologías y satisfaciendo las demandas de los usuarios. Para poder optimizar estos recursos y planear una estrategia a seguir para la revisión y mejora continua, se analizan diferentes aspectos, entre estos la seguridad física y de la información, sus tendencias y su constante evolución.

1.3.1. Introducción

Eric Slavinsky, director de informática de Louisville Gas and Electric and Kentucky Utilities Energy LLC (LG&E and KU) afirma que: "Uno no puede obligar a las personas a cambiar, hay que inspirar en ellas un sentido de pertenencia y participación. Además, uno debe mostrarles cómo el cambio puede tener consecuencias positivas en su trabajo. La idea es brindar más herramientas a la empresa mediante el uso de la tecnología" (Cisco, 2013). Dentro de la implementación de la tecnología en una empresa, uno de los temas más importantes a manejar es la forma en cómo se va a controlar la información, pues hoy en día, las personas esperan tener la información disponible las 24 horas del día. Según la norma de seguridad de la información UNE-ISO/IEX 17799, “La información es un activo que, como otros activos importantes del negocio, tiene valor para la empresa y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio elenco de amenazas para asegurar la continuidad del negocio, minimizar los daños a la empresa y maximizar el retorno de las inversiones y las oportunidades del negocio” (San Martín García, 2004, pág. 23).

“La virtualización del centro de datos y la computación en la nube están evolucionando como elementos fundamentales de las empresas, la educación, los gobiernos y las comunicaciones y redes domésticas", señaló Thomas Barnett, director del Grupo de Liderazgo en ideas para proveedores de servicios de Cisco (Cisco, 2013). Actualmente, dentro de las medianas y grandes empresas, el manejo de información se realiza dentro de un centro especializado que tiene como fin almacenar los equipos informáticos que van a estar implicados en el control de la

información de la compañía y las áreas de soporte (BICSI, 2011, pág. 8). Dentro de estos centros de datos, se lleva a cabo un control de múltiples factores garantizando la seguridad de la información y una seguridad física. Muchas de las empresas que comienzan a implementar estos centros de datos para el manejo de la información, no tienen en cuenta muchos de los estándares y la metodología adecuada que se debe llevar a cabo.

1.3.2. Seguridad de la información

En un negocio, la información debe ser administrada correctamente para que siempre esté protegida sin importar como ni en donde se encuentre, es decir, la seguridad de la información. Para proteger la información de la empresa, una de las principales soluciones es implementar un sistema de gestión de seguridad, creando así unas medidas de control en todos los niveles de la empresa mediante procedimientos, políticas de seguridad y funciones. (San Martín García, 2004, pág. 23). Adicionalmente, al planear la seguridad de la información se tienen en cuenta tres principios básicos: Confidencialidad, integridad y disponibilidad. En cuanto a la confidencialidad, se debe asegurar que la información sólo esté disponible para las personas autorizadas. Por integridad, se entiende que la información esté completa y sea confiable en todo momento. Por último, la disponibilidad garantiza que la información pueda ser consultada por un usuario en el momento que lo necesite (San Martín García, 2004, pág. 24).

1.3.3. Seguridad física

Según Cisco e Intel, la infraestructura de los sistemas de información en una empresa, es la base para que los negocios se realicen con agilidad y para que exista una eficiencia financiera en los centro de datos (Cisco, 2012). A medida que la tecnología va avanzando, los centros de cómputo se ven directamente afectados, pues cada vez demandan una mayor capacidad de almacenamiento y rendimiento. Al momento de construir un centro de cómputo, muchas empresas no valoran la inversión inicial que se debe realizar en la arquitectura de este sitio. Es de vital importancia valorar la infraestructura física del centro de cómputo para que en un futuro la empresa pueda

ser ágil, flexible y exitosa en un mercado que está en constante cambio (Torell, 2011, pág. 1).

De acuerdo al centro de seguridad nacional, (National Computer Science Center), la seguridad física que se debe aplicar a un centro de cómputo, se define como la aplicación de barreras físicas y el control de procedimientos como medidas preventivas contra las amenazas a los recursos y a la información sensible (SANS Institute, 2001, pág. 2). La seguridad física es uno de los puntos más importantes a la hora de diseñar la infraestructura física para redes críticas (NCPI), pues con esta, se maximiza el tiempo productivo del sistema, reduciendo así el tiempo que puede estar inactivo por causa de accidentes o errores humanos (Niles, Seguridad física en instalaciones de misión crítica, 2006, pág. 3).

En general, las amenazas de los centro de datos se pueden clasificar en dos grupos. Primero, las amenazas digitales que se dan por software informático y redes, las cuales son ocasionadas por hackers, virus, ataques maliciosos, entre otros; segundo, las amenazas por infraestructura física (Tecnológico Dominicano, 2011). Entre los aspectos más importantes a tener en cuenta dentro de la infraestructura de física para las redes, se encuentra el suministro eléctrico, la refrigeración del lugar, los racks, el cableado y el sistema de control de incendios (Niles, Seguridad física en instalaciones de misión crítica, 2006, pág. 2).

Para clasificar los riesgos físicos que se pueden tener en un centro de cómputo, se definen dos secciones, la primera se enfoca hacia la propiedad, es decir, el edificio, los equipos informáticos, la infraestructura general y la información; la segunda es el personal tanto interno como externo a la empresa (SANS Institute, 2001, pág. 3). En cuanto a los riesgos físicos, algunos de los factores a tener en cuenta son: La ubicación general del centro de cómputo, analizando desde la ubicación el centro de cómputo con respecto a las oficinas de trabajo hasta la posibilidad de desastres naturales en la zona.

En cuanto al perímetro del sitio, es recomendable tener un sistema cerrado de cámaras desde el cual se monitoree el sector y los movimientos que ocurran cerca al centro de datos. Para minimizar estos riesgos, lo primero que se realiza es un plano de las instalaciones para saber qué se debe proteger. En este plano, se identifican: El perímetro del edificio, el área para los equipos (Niles, Seguridad física en instalaciones de misión crítica, 2006, pág. 5) y los puntos de acceso. A continuación en la Figura **1**, se muestra un mapa especificando la profundidad de la seguridad que se debe tener dentro del centro de cómputo (Niles, Seguridad física en instalaciones de misión crítica, 2006, pág. 6).

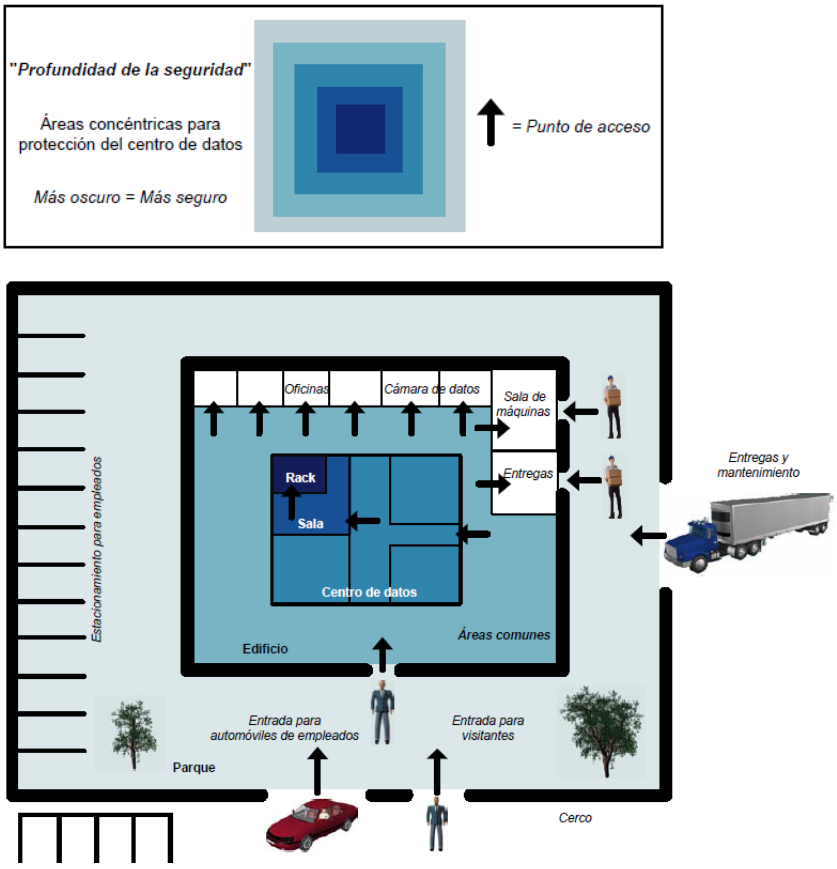


Figura 1. Mapa con profundidad de la seguridad

1.3.4. Diseño del centro de datos

Actualmente, existen múltiples centros de cómputo donde se han implementado buenas prácticas y los cuales se pueden tomar como referencia. Entre ellos, está la

empresa APC por Schneider Electric, la cual documenta buenas prácticas y medidas a tener en cuenta a la hora de realizar u organizar un centro de cómputo. Para comenzar, es de gran ayuda contar con un diseño de referencia para así simplificar la implementación física que se va a realizar, evitando procesos innecesarios y minimizando los posibles riesgos que el sistema esté inactivo.

En general, un diseño que se toma como referencia, es una lista de atributos que incluye las especificaciones del nivel de desempeño y el listado de componentes del sistema (Donovan, 2012, pág. 2). Algunos de los aspectos mínimos a tener en cuenta son: La implementación de un diseño, ubicación de los racks (Estructuras donde los equipos de tecnología se organizan), sistema de refrigeración, sistema contra incendios, sistema de control de acceso por medio de cámaras de seguridad, cableado adecuado y disponibilidad de los elementos. En primera instancia, al definir la capacidad de la infraestructura física, se garantizan procesos como la refrigeración y alimentación adecuada para el espacio (Rasmussen, Administración de capacidad de energía y refrigeración para centros de datos, 2012, pág. 2).

Según Giuliano Di Vitantonio, vicepresidente de marketing de centros de datos y virtualización global de Cisco, "El diseño determina el grado de intervención humana y de aplicaciones que se necesitan, que son factores que definen la complejidad y el costo, y afectan la agilidad real" (Cisco Systems e Intel, 2012, pág. 4). Es recomendable diseñar el centro de cómputo para así tener en cuenta primero las limitaciones por espacio antes que las limitaciones por potencia y temperatura (American National Standard, 2011, pág. 31). Dentro de este estudio que se realiza para el diseño del centro de cómputo, se planea la ubicación de los equipos, teniendo en cuenta el espacio disponible y la conectividad entre los mismos (Alarcón, 2011, pág. 16). Adicional a esto, se debe tener un diseño con la ubicación de los racks, pensando en posibles errores humanos (Avelar, Opciones prácticas para implementar equipos IT en sucursales y salas de servidores pequeñas, 2013, pág. 7). Por otro lado, se debe tener en cuenta la obstrucción que se pueda realizar por causa del piso falso,

es decir las canales y tuberías que se encuentren en el piso. Igualmente, las placas del piso falso, cómo están acomodadas y los cortes que se deben realizar a algunas de ellas para permitir el paso de los cables, altura del piso falso y del techo (Alarcón, 2011, pág. 40).

1.3.4.1. Sistema de control de acceso

Dentro de las principales prevenciones, está el acceso limitado de personal, evitando así una acción inadecuada dentro del centro de datos (Tecnológico Dominicano, 2011). Para esto, se cuenta con unos controles de acceso relacionados a unos métodos de identificación. Estos métodos se clasifican en tres categorías, a medida que se va aumentando la seguridad, aumenta el costo de implementación.

El primer nivel consta de lo que la persona tiene, esto se puede clasificar como un dispositivo de seguridad, como una llave o una tarjeta de control de acceso. Este es el mínimo nivel de confiablidad, pues estos artículos pueden ser compartidos o robados y no se asegura que la persona que esté usando el artículo, sea la que debe tener acceso. En segundo nivel, se tiene lo que la persona conoce, es decir una clave o un procedimiento que se debe realizar para acceder. En este caso, se cuenta con una mayor confiabilidad, pues no puede ser robado pero si compartido. Por último, el nivel de seguridad más confiable se logra por medio de la identidad de la persona. Esto implica un reconocimiento físico; este método es llamado biometría. Algunas de las características físicas que se utilizan en la biometría son: Las huellas digitales, el iris, la retina o la voz (Niles, Seguridad física en instalaciones de misión crítica, 2006, pág. 8). A continuación, en la **Figura 2** se hace una relación entre los 3 niveles de seguridad que se tienen para el acceso a los centros de datos y el nivel de confiabilidad (Niles, Seguridad física en instalaciones de misión crítica, 2006, pág. 9).

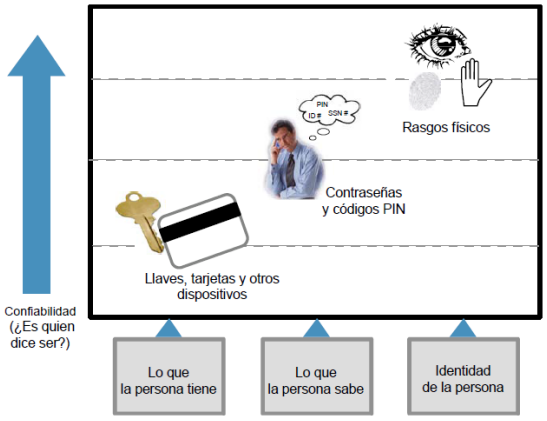


Figura 2. Niveles de seguridad en un centro de cómputo

1.3.4.2. Control de temperatura

Teniendo este diseño físico inicial, se estudia el sistema de enfriamiento para el centro de datos. Debido a que los fallos por temperatura en un centro de cómputo pueden ocasionar un gran impacto, es necesario llevar un control. Al momento de implementar un sistema de aires acondicionados se analiza el flujo del aire. En el 2011, el comité técnico 9.9 de ASHRAE, establece unos límites de temperatura de servicio recomendables que están entre 18°C a 27°C y un rango permisible que van de 15°C a 31 °C (Avelar, Opciones prácticas para implementar equipos IT en sucursales y salas de servidores pequeñas, 2013, pág. 5). Es de gran importancia cumplir con estos límites, pues según un estudio realizado en el Laboratorio Nacional Los Alamos sobre los fallos del calor, se sabe que: “La tasa de fallos se duplica por cada 10°C de incremento en la temperatura” (Bayle, 2010, pág. 11). En la **Figura 3**, se ve un gráfico que compara el riesgo de fallo que se tiene a medida que va aumentando la temperatura en el centro de cómputo.

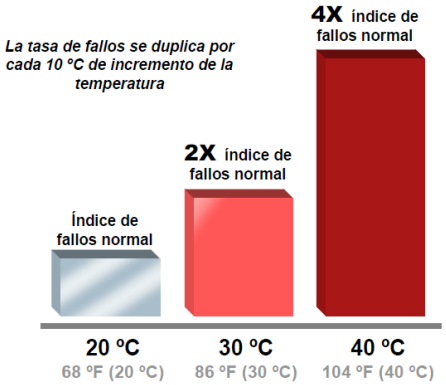


Figura 3. Estudio del Laboratorio Nacional Los Alamos sobre fallos por calor

1.3.4.3. Distribución de racks

En cuanto a la ubicación de los racks y los armarios, se analiza el flujo del aire caliente o frío que generan los equipos. En la parte delantera de los racks, se encuentran los pasillos fríos, en el piso falso de este pasillo se ubican los cables para la distribución de energía. En la parte trasera de los racks, se crean los pasillos de flujo de aire caliente, en el piso falso de estos pasillos, se organizan las bandejas de cables para telecomunicaciones.

A continuación en la **Figura 4**, se encuentra un diagrama de los pasillos calientes o fríos de un centro de cómputo que dependen de la organización de los equipos en los racks. Los cuadros grises equivalen a los racks y los blancos a las baldosas del piso falso, que pueden ser levantadas para el control del cableado. Los racks deben alinearse a las baldosas para que al momento de levantar el piso falso, este pueda ser removido sin ningún inconveniente. Para un mejor acceso a los equipos y conectividad de hardware, los racks no deben superar una altura de 2,1 metros (Telecommunications Industry Association, 2005, págs. 38-40).

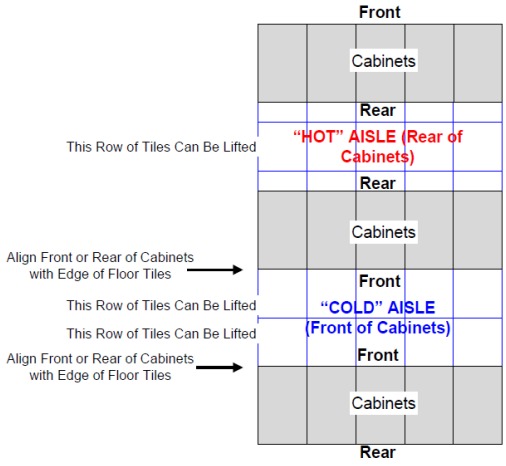


Figura 4. Distribución de pasillos según racks o armarios[3]

1.3.4.4. Sistema de control y extinción de incendios

En un centro de cómputo, se considera necesario un sistema de detección y extinción de incendios. La asociación nacional de protección contra incendios, NFPA, creada en 1896, es la encargada de minimizar los incendios mundialmente basándose en códigos, normas e investigaciones (Avelar, Mitigating Fire Risks in Mission Critical Facilities, 2011, pág. 2). Específicamente, para los centros de cómputo, se crea una norma, NFPA 75, para la protección de equipos electrónicos y de procesamiento de información. Los incendios se clasifican en 4 categorías como se muestra en la **Tabla 1**.

Tabla 1. Tipos de incendios [4]

Clase	**Tipo de incendio**	**Símbolo**
A	Incendios que se relacionan con materiales combustibles ordinarios como: Papel, madera, tela y algunos plásticos.	
B	Incendios por líquidos o gases como aceite, pintura inflamable, petróleo o gasolina.	
C	Incendios por equipos eléctricos, generalmente son de clase A o B y tienen presente electricidad.	

[3] (Telecommunications Industry Association, 2005, pág. 38)
[4] (Avelar, Mitigating Fire Risks in Mission Critical Facilities, 2011, pág. 3)

D	Incendios por metales combustibles como magnesio, sodio o potasio.	
K	Incendios por elementos de cocción como aceites y grasas.	

Para minimizar el riesgo de incendio, existen varios de sistemas de detección, entre ellos, el mejor sistema a implementar en un centro de cómputo es detección por humo, pues la detección por calor o llama, no genera una alerta con anterioridad, la cual es necesaria para evitar el daño de los equipos **(Avelar, Mitigating Fire Risks in Mission Critical Facilities, 2011, pág. 4)**. Los detectores de tipo punto, son de gran utilidad para un centro de cómputo pequeño, pues otros detectores más costosos, agregan sólo un poco de valor a la detección dentro de estos espacios pequeños.

Existen dos tipos de detectores tipo punto, los fotoeléctricos que usan una luz y un sensor de luz perpendicular a esta, así cuando haya humo en la cámara del sensor, la luz se vuelve algo difusa y es reflejada al sensor causando así una alarma. Por otro lado, existen los detectores iónicos, que usan una cámara de ionización y una pequeña radiación para detectar el humo, la cámara está ionizada por la radiación causando un flujo de corriente constante; cuando existe humo, esta radiación deja de ser constante y genera una alarma. Al momento de detectar la alarma de humo, se debe reaccionar implementando métodos para apagar el fuego como: Espuma, polvo químico seco, sistema de rociadores de agua o un extintor de incendios **(Avelar, Mitigating Fire Risks in Mission Critical Facilities, 2011, págs. 4-8)**.

Es vital llevar un mantenimiento en el sistema contra incendios que es implementado en un centro de cómputo; para esto, existe una norma, NFPA 25, la cual regula la inspección, pruebas y el mantenimiento de este sistema y de los aspersores usados; la norma se basa en un sistema contra incendios basado en agua **(Niemann, Brown, & Avelar, 2013, pág. 13)**.

1.3.4.5. Mantenimiento preventivo

Una de las mejores prácticas a realizar, es un mantenimiento preventivo, por medio una inspección de las fallas para evitarlas antes que ocurran. Con esto, se crea una estrategia para asegurar la disponibilidad de los equipos en un centro de cómputo (Bayle, 2010, pág. 3). Existen cinco opciones cuando se realiza la inspección: Primero, encontrar una falla antes que ocurra y solucionarla. Segundo, se puede encontrar una falla ya ocurriendo, solucionarla y así evita una mayor indisponibilidad. Tercero, encontrar una tendencia en la que está cayendo la red y solucionarla de manera definitiva. Cuarto, no encontrar ninguna falla y reprogramar el siguiente mantenimiento preventivo sin ninguna acción. Por último, encontrar una falla la cual genera un tiempo de inactividad que debe ser tomado en cuenta e informado a las personas afectadas por esta caída del sistema (Bayle, 2010, pág. 5).

Por medio de estudios realizados, el mantenimiento preventivo en un centro de datos tiene un impacto muy positivo. En los últimos años, se han tenido grandes avances en las tecnologías que se implementan para un centro de cómputo y cada vez, los fabricantes esperan lanzar un equipo mejor y con menos errores que el anterior, lo que permite que en la actualidad, la infraestructura física sea más fácil de controlar y de mantener a lo largo de los años. (Bayle, 2010, pág. 7).

1.3.4.6. Monitoreo de personal y equipos

Actualmente, las amenazas que se presentan en un centro de cómputo, son causadas en su mayoría por errores humanos. Según el instituto UpTime[5], más del 70% de las caídas de alimentación, se dan por errores humanos. Generalmente, están relacionados con falta de entrenamiento, mantenimiento y rigor en la operación (UpTime Institute , 2010, pág. 2). Un sistema de monitoreo que se puede incorporar dentro del centro de cómputo, es un circuito cerrado de cámaras el cual cuenta con sensores y videovigilacia. En caso de notar algún movimiento poco común dentro de este espacio, se genera una alerta para que el administrador detenga este evento y así

[5] Centro de investigación, educación y consultoría, enfocado en la mejora de centros de datos en cuanto a eficiencia y rendimiento, a través de la colaboración e innovación.

evite una falla (Bouley, 2012, pág. 6). Adicional a esto, se lleva un control sobre las personas que ingresan al centro de cómputo y sobre sus acciones dentro de este.

Por otro lado, debe existir una supervición permanente del estado de los equipos principales. Para esto, cada equipo cuenta con una configuración inicial que al ser programada, genera unas alertas para que las personas encargadas del manejo del centro de cómputo, estén al tanto cuando hay una falla. Entre las funciones que se tienen en este sistema de supervisión, están las alertas, el estado actual de los equipos, informes y configuración de control. Con esto, se definen unos límites permitidos, cuando estos niveles no están dentro del rango, se genera una alerta que puede ser enviada por correo electrónico, mensaje de texto o alertas dentro del mismo sistema y de ser necesario, se puede crear una conexión para reiniciar los equipos remotamente (Bouley, 2012, pág. 9).

1.3.5. Normas de un centro de cómputo

Hoy en día, existen normas aplicables a un centro de datos las cuales se deben seguir para poder cumplir con los niveles mínimos necesarios dentro de este espacio. En la **Figura 5**, se encuentra una gráfica con las áreas a tener en cuenta y los estándares a aplicar en cada una de ellas dentro de un centro de cómputo.

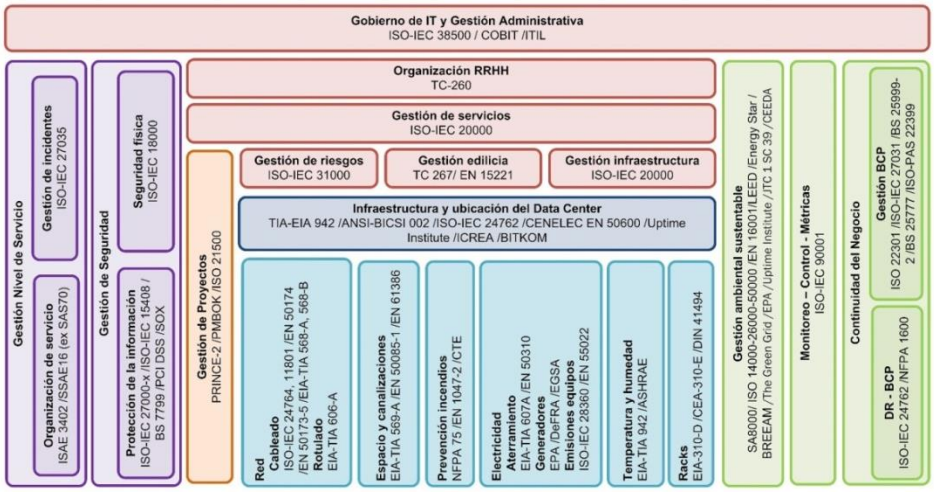


Figura 5. Estándares en el Data Center [6]

[6] (Pacio, 2013)

1.3.5.1. Nivel Tier

El instituto UpTime es un centro de investigación, educación y consultoría, enfocado en la mejora de centros de datos en cuanto a eficiencia y rendimiento, a través de la colaboración e innovación (Uptime Institute , 2014). Este propone un estándar a seguir que abarca algunas de las normas a tener en cuenta en cuanto a la infraestructura y ubicación de un data center. El estándar mundial dice que por medio del sistema de clasificación Tier, se establecen los comportamientos y riesgos que impactan a largo plazo en un centro de cómputo. Esto se mide según la disponibilidad del centro de cómputo con 4 niveles (UpTime Institute , 2010, pág. 6). A medida que va incrementando el nivel de Tier, el tiempo de actividad de un centro de cómputo debe aumentar.

El nivel Tier I se le asigna a un centro de cómputo cuando se tiene un espacio especializado para almacenamiento de equipos de tecnología, este debe ser diferente al espacio de la oficina de trabajo. Adicional a esto, se debe tener un sistema de alimentación ininterrumpida (UPS) que filtre los picos de voltaje y caídas de energía momentáneas, un sistema de enfriamiento las 24 horas del día y un generador de energía para asegurar la actividad de los equipos (UpTime Institute , 2010, pág. 6).

Un centro de cómputo de nivel Tier II, debe contar con las características del Tier I. Adicional a esto, cuando existan fallas de los equipos de infraestructura, se cuenta con un sistema que controla las caídas constantes de energía y que evita la interrupción del enfriamiento. Para esto, se implementan componentes como: UPS, enfriadores, equipos que reaccionen al calor, entre otros. En este caso, al momento de que un equipo presente una falla o se realice un mantenimiento con previo aviso, los equipos de tecnología dejan de funcionar, perdiendo así su capacidad (UpTime Institute , 2010, pág. 6).

Para el nivel III de Tier, se debe asegurar que todos los equipos que entran a mantenimiento, con previo aviso, no deben afectar el ambiente de tecnología. Por otro lado, se debe tener un suministro redundante para la energía y el enfriamiento del centro de cómputo, asegurando que al momento de realizar un mantenimiento en

estos sistemas, el sitio sigua funcionando normalmente (UpTime Institute , 2010, pág. 6).

Por último, en el nivel Tier IV, la infraestructura del sistema debe ser tolerante a fallas, soportando operaciones del equipo de tecnologías. Estos centros de cómputo permiten la falla o mantenimiento de cada uno de los equipos sin previo aviso. Además, contemplan las fallas de varios equipos simultáneamente, de sus componentes y sistemas, sin que esto afecte la operación del centro de cómputo (UpTime Institute , 2010, págs. 6-7).

1.3.5.2. TIA-942

El estándar TIA-942 fue desarrollado en 2005 por la Asociación de Industria de Telecomunicaciones, TIA; una asociación comercial que representa las tecnologías de comunicación e información globales por medio de normas, políticas, oportunidades de negocio, e inteligencia de mercados (Asociación de industria de telecomunicaciones, 2014). Este estándar se basa en el instituto UpTime y se fundamenta en especificar la estructura para las telecomunicaciones y el cableado en cualquier centro de cómputo.

A continuación, en la **Figura 6**, se presenta el arreglo físico o lógico de un sistema de telecomunicaciones, más conocido como topología, presentado en el estándar TIA-942 para un centro de cómputo reducido.

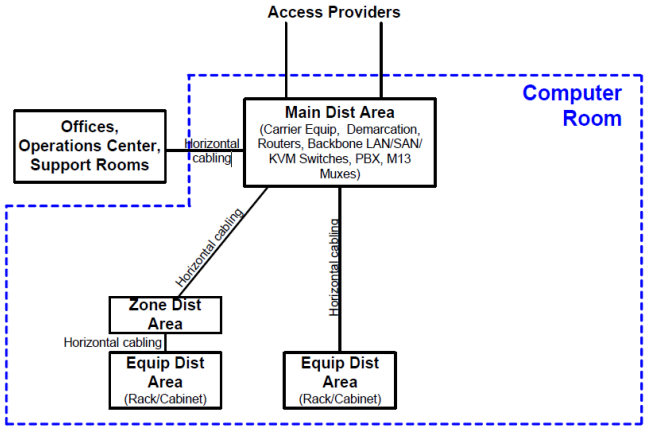


Figura 6. Ejemplo de una topología de un centro de cómputo reducido[7]

El área principal de distribución, es el espacio donde se encuentra la conexión cruzada principal, es decir, el esquema de conexión entre equipos o subsistemas utilizando cables que conectan algún tipo de hardware en cada extremo. Por otro lado, el área de distribución de zona, es dónde se encuentra un punto de salida o de distribución, es decir, un equipo que da por concluidas las conexiones de cableado horizontal permitiendo una conexión al área de distribución de equipos. Ésta se implementa para servir a las áreas de equipos cuando la conexión horizontal no está localizada en el área principal. Una conexión horizontal es la que existe entre el área principal y las áreas de distribución o áreas de zona. Por último, el área de distribución de equipos, se ocupa por racks o armarios y los equipos de tecnología que se almacenan dentro de estos (Telecommunications Industry Association, 2005, págs. 13-16).

Teniendo en cuenta el diseño arquitectónico del centro de cómputo, algunas de las recomendaciones que presentan el estándar TIA-942 son las siguientes: En el espacio designado para este fin, se debe tener en cuenta el espacio que requieren los equipos actuales y los equipos pensando a futuro. Además, la altura del techo debe ser de mínimo 2,6 metros; desde el piso hasta la primera barrera de techo que se encuentre. Los pisos, paredes y techos deben ser creados en un material que evite el polvo y los acabados se deben realizar de un color claro para generar más iluminación dentro de la sala. También, los pisos deben tener propiedades antiestáticas según la norma IEC 61000-4-2 y las puertas deben tener al menos 1 metro de ancho y 2,13 metros de alto (Telecommunications Industry Association, 2005, págs. 27-29).

Por otro lado, el control de ventilación, calor y aires acondicionados debe funcionar las 24 horas del día, asegurándose de tener una operación continua. De ser necesario, se debe tener una planta eléctrica propia en caso que el edificio no cuente con este requerimiento y un generador especializado para este tema. Además, los parámetros de temperatura y humedad de la sala para operar correctamente, deben estar entre 20

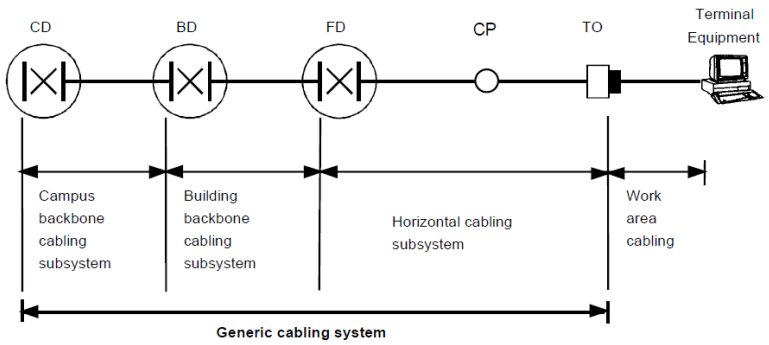
[7] (Telecommunications Industry Association, 2005, pág. 25)

a 25°C y una humedad relativa del 40 al 55%, teniendo una máxima tasa de cambio en la temperatura de 5°C por hora. Estos controles se deben realizar cada 3 a 6 metros, a no una altura mayor de 1,5 metros del piso. (Telecommunications Industry Association, 2005, págs. 28-29). Es de gran importancia tener en cuenta el factor de la humedad pues un nivel muy alto de esta en el centro de cómputo, permite que se acumule gran cantidad en la parte interna de los equipos, creando un daño en estos. En caso que la humedad sea muy baja, se generan descargas de electricidad y cortos en los circuitos (IT Watch Dogs).

Adicional a la distribución dentro del centro de cómputo, el estándar TIA-942, cuenta con unos requerimientos generales basados en el estándar NFPA 75. En general, el estándar recomienda que la ubicación del centro de cómputo no sea en edificios con restricciones de acceso como: Ascensores pequeños, paredes que interrumpan el ingreso o limitaciones para ingresar equipos grandes. Además, este no debe estar cerca de salas con fuentes electromagnéticas como: Salas de transmisión de radio o rayos X y no debe tener ventanas al exterior pues reducen la seguridad y generan más calor (Telecommunications Industry Association, 2005, pág. 27).

1.3.5.3. ISO/IEC 24764

En términos del cableado que se debe utilizar para la conexión de los equipos, existe la norma internacional ISO/IEC 24764, enfocada en el sistema de cableado de cobre y fibra óptica de un centro de cómputo **(TE Connectivity, 2012, pág. 3)**. El estándar incluye la estructura y los configuraciones mínimas del cableado, los requerimientos de desempeño de los canales y componentes, implementación, procedimientos y verificación de los mismos **(Maguire, 2013)**. Este estándar se basa en los requisitos de la norma ISO/IEC 11801, la cual identifica los elementos funcionales de los cables y su conexión para formar subsistemas **(ISO/IEC, 2002, pág. 26)**. En general, en un edificio, la estructura general de conexión es la siguiente:



CD: Cabling Distribution
BD: Building Distribution
FD: Floor Distribution
CP: Consolidation Point
TO: Telecommunications Outlet

Figura 7. Estructura genérica de cableado[8]

A partir de esto, se crea la estructura y distribución de cableado en un edificio. En uno de los pisos está el centro de cómputo, aquí es donde se tiene el punto de consolidación de todo el cableado externo. A continuación, en la **Figura 8**, se muestra como se acomodan los elementos en un edificio.

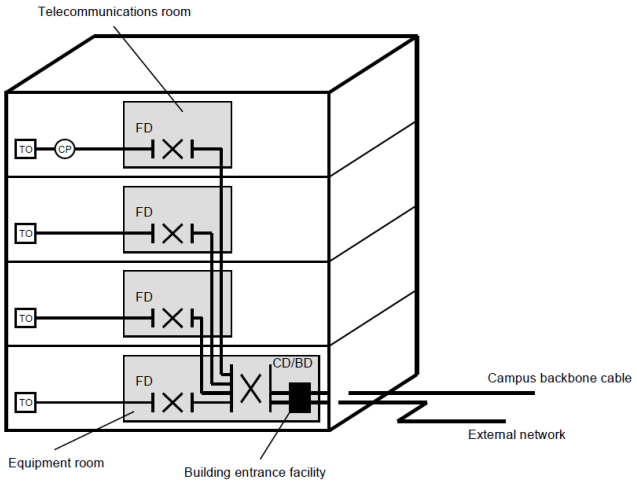


Figura 8. Distribución de elementos en un edificio[9]

El cableado organizado a lo largo de un edificio, cableado estructurado, permite conectar diferentes dispositivos, integrando así todos los servicios. Los componentes del cableado estructurado son: El área de trabajo, el cableado horizontal, los racks, el cableado vertical y el centro de cómputo (Laboratorio de comunicaciones 66.79, 2009, pág. 14). El cableado horizontal es el que inicia en el centro de cómputo y va

[8] (ISO/IEC, 2002, págs. 26-27)
[9] (ISO/IEC, 2002, pág. 30)

hasta el área de trabajo (ANSI/TIA/EIA-569-A, 2006). Se tienen 3 medios la conexión de cableado horizontal: El cable de 4 pares 100 Ohm UTP, cables de 2 pares 150 Ohm y cable de fibra óptica 2 Fibras 62.5/125 um. (Universidad Nacional , pág. 1). El cableado horizontal debe tener una topología en estrella y los elementos eléctricos no deben ser instalados como parte de este cableado.

El estándar, define los canales y vínculos que se deben tener en un centro de cómputo. Los cables de par trenzado de cobre se clasifican en clase A, B, C, D, E, E_A, F y F_A (TE Connectivity, 2012). A continuación en la **Tabla 2**, se relaciona el tipo de cable de par trenzado de cobre y la frecuencia máxima que este alcanza, definiendo su desempeño. Cada tipo de cable, se implementa para una aplicación diferente, la clase A, genera el menor desempeño para soportar aplicaciones, esta es la menor clase (ISO/IEC, 2002, pág. 39).

Tabla 2. Clase de cable de cobre y su frecuencia máxima

Clase de cable	**Frecuencia Máxima**
A	100KHz
B	1MHz
C	16MHz
D	100MHz
E	250MHz
E_A	500MHz
F	600MHz
F_A	1000MHz

Los cables de fibra óptica se clasifican en OM1, OM2, OM3, OM4, OS1 y OS2. La fibra óptica puede ser multimodo o monomodo, es decir, la cantidad de líneas que se tienen para la transmisión. Si es monomodo, solo se tiene una línea y sólo se puede transmitir la información; si es multimodo, se puede transmitir y recibir información simultáneamente. Estos al igual que el cable de par trenzado de cobre, se implementan dependiendo de la aplicación que se tenga. Como mínimo en un centro de cómputo, se debe contar con un cable de par trenzado de cobre de clase E_A y un cable de fibra óptica de tipo OS1 u OS2 para transmisiones monomodo y un cable de fibra óptica de tipo OM3 para transmisiones multimodo (Aldama, 2012).

Dentro del cableado estructurado, también se hace referencia al cableado vertical (backbone), que corresponde a la conexión entre los pisos, los cables del centro de cómputo al cableado del edificio y los cables de edificio a edificio. Para estas conexiones, se utilizan diferentes cables dependiendo de la distancia y el tipo de aplicación. A continuación, en la **Tabla 3**, se encuentra el tipo de cableado con su máxima distancia.

Tabla 3. Tipos de cableado y distancias[10]

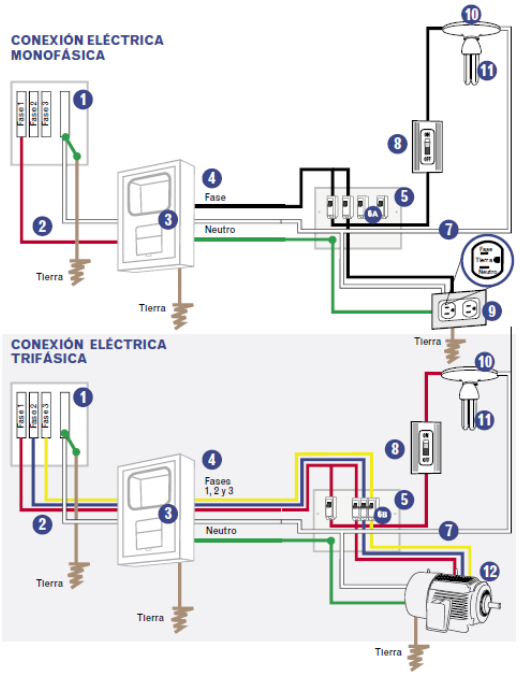
Tipo de cable	Máxima distancia
100 Ohm UTP	800 metros para transmisión de voz
150 Ohm STP	90 metros para transmisión de datos (Ancho de banda 20Mhz a 300Mhz)
Fibra óptica 62.5/125 um multimodo	2000 metros
Fibra óptica 8.3/125 um monomodo	3000 metros

1.3.6. Eficiencia energética y apoyo al medio ambiente

Cuando se planea el diseño de un centro de cómputo, no se tienen en cuenta el consumo de energía que este va a generar y cómo se puede optimizar. Muchas veces este costo puede superar el valor de la inversión en equipos e infraestructura general. Algunos de los problemas que causan un consumo muy elevado son: La factura llega después de consumido el servicio, el consumo está incluido en una factura general por lo cual no se puede medir el consumo de sólo el centro de cómputo (Rasmussen, Implementación de centros de datos con eficiencia energética, 2012, pág. 1). Según Neil Rasmussen[11], "Con decisiones sencillas y sin costo alguno tomadas durante el diseño de un centro de datos nuevo, es posible ahorrar entre un 20 y un 50% del monto de la factura de electricidad, y con un esfuerzo sistemático, ese porcentaje podría ascender hasta un 90%." [12]

[10] (Universidad Nacional , pág. 2)
[11] Vicepresidente senior de innovación en Scheider Electric
[12] (Rasmussen, Administración de capacidad de energía y refrigeración para centros de datos, 2012, pág. 2)

Para poder tener una medida, se debe conocer el consumo en cuanto a energía y potencia. El consumo de energía es la relación con el costo de la factura del servicio público; mientras que el consumo en potencia se mide con respecto a los sistemas que ofrecen energía, entre estos el sistema de aire acondicionado, las UPS, generadores, entre otros (Rasmussen, Implementación de centros de datos con eficiencia energética, 2012, pág. 4). A continuación en la **Figura 9**, se presenta un diagrama con los componentes básicos de las instalaciones eléctricas internas que se tienen en una compañía.



Componente
1: Transformador
2: Acometida
3: Caja de medidor
4: Parcial
5: Tablero de distribución
6: Interruptores automáticos
7: Circuito eléctrico
8: Interruptores manuales
9: Toma corriente
10: Portalámparas
11: Luminarias
12: Motor

Figura 9. Componentes de las instalaciones eléctricas internas[13]

Para mejorar la cantidad de energía y potencia que se consume en un centro de cómputo, existen varias recomendaciones. Una de ellas es el retiro de equipos informáticos que no están en uso, que siguen en funcionamiento y están consumiendo energía; esto disminuye la potencia consumida aproximadamente en un 20% (Rasmussen, Implementación de centros de datos con eficiencia energética, 2012, pág. 6). Por otro lado, se puede administrar de la potencia de los equipos informáticos cuando la carga computacional es menor, generando un menor consumo de energía

[13] (Codensa, 2006, págs. 10-11)

(Rasmussen, Implementación de centros de datos con eficiencia energética, 2012, págs. 6-7).

Adicionalmente, para el ahorro de energía, se analiza el flujo del aire dentro del centro de cómputo. Según Bruce Myatt de EYP Mission Critical, la separación del aire caliente del aire frío "es una de las medidas de mayor eficiencia energética disponible hoy en día para centros de datos nuevos y existentes"[14]. Entre las buenas prácticas, existen dos metodologías: La primera, es la contención de pasillos fríos en donde el aire caliente viaja libremente por toda la sala y se cierra el pasillo frio como se muestra en la **Figura 10**, para esto es necesario que las filas de los racks estén acomodadas de forma que se alternen los pasillos fríos y los calientes (Niemann, Brown, & Avelar, 2013, pág. 3).

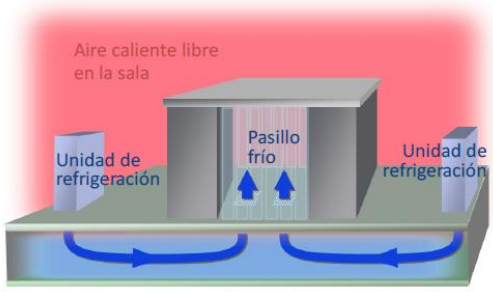


Figura 10. Contención de pasillos fríos[15]

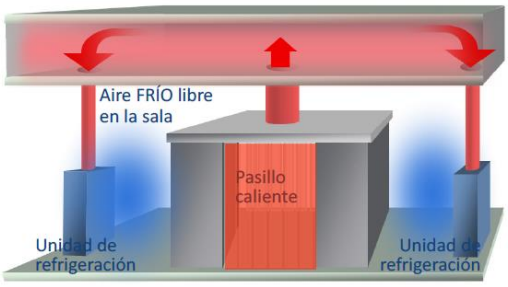


Figura 11. Contención de pasillos calientes[16]

La segunda técnica que se puede aplicar, es la contención de pasillos calientes, es decir que todo el aire caliente de salida de los equipos se contiene y el aire frío viaja libremente, como se muestra en la **Figura 11**. Entre las dos opciones, la que proporciona una mejor eficiencia y ahorro de energía para el centro de cómputo es la contención de pasillos calientes, pues este consume un 43% menos de energía de refrigeración cuando la temperatura en el área de aire frio se encuentra a 24°C (Niemann, Brown, & Avelar, 2013, pág. 10). De igual manera, las dos opciones generan un ahorro de energía, por lo cual es necesario contemplar cuál es la mejor

[14] (Niemann, Brown, & Avelar, 2013, pág. 2)
[15] (Niemann, Brown, & Avelar, 2013, pág. 4)
[16] (Niemann, Brown, & Avelar, 2013, pág. 5)

solución a implementar dependiendo de las características actuales del centro de datos (Lin, Avelar, & Niemann, 2013, págs. 3-5).

1.3.7. Tendencias a futuro

1.3.7.1. Virtualización

Una de las tendencias más influyentes para los centros de cómputo es la virtualización, la cual se refiere a "la creación de equipos, basados en software, que reproducen el ambiente de una máquina física en sus aspectos de CPU, memoria, almacenamiento, entrada y salida de dispositivo".[17] La virtualización trae múltiples beneficios en un centro de cómputo, entre ellos, aprovechar más los recursos, reducir el espacio que es ocupado por los equipos, menos consumo de energía, una menor necesidad de enfriamiento, reducción del costo total de las operaciones, entre otras (Hernandez Brito, 2011, págs. 23-24).

En general, la virtualización reduce el consumo de energía de los equipos, pero al mismo tiempo aumenta la densidad del centro de datos. A medida que se van virtualizando las máquinas, el procesamiento del servidor aumenta (Niles & Donovan, Virtualización e informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios, 2012, págs. 2-3). Adicionalmente, al tener altas densidades de potencia, se debe analizar la capacidad de enfriamiento del centro de datos para evitar una carga alta en un solo rack. Para esto, se debe tener en cuenta la distribución de los equipos y la concentración de esta carga, ya sea en un bloque de alta densidad o una distribución equitativa a lo largo de todo el centro de datos.

Por otro lado, la efectividad del centro de datos se ve afectada con la virtualización de los equipos. A medida que se genera una menor carga informática, se tiende a tener una peor efectividad del uso de la energía, PUE, pues a pesar que se mejora la carga informática, los sistemas de enfriamiento y potencia no se optimizan como se observa en la **Figura 12**.

[17] (Hernandez Brito, 2011, pág. 7)

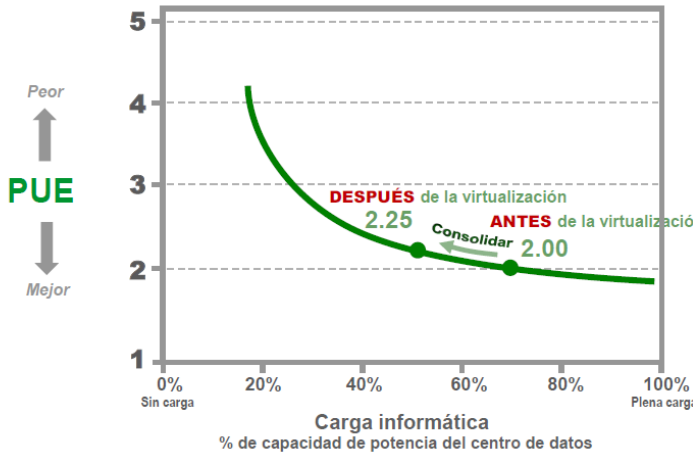


Figura 12. Carga informática contra PUE[18]

Para evitar que esto ocurra, se pueden tomar ciertas medidas después de implementar la virtualización, entre ellas, la separación de aire frio de aire caliente para reducir la mezcla de aire. Por otro lado, se pueden organizar los racks de manera que no sea necesario contar con múltiples sistemas de enfriamiento, solo en las áreas necesarias. Además se pueden remover, apagar UPS que ya no sean necesarias o quitar módulos de potencia del sistema UPS (Niles & Donovan, Virtualización e informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios, 2012, pág. 8).

Igualmente, una de las grandes ventajas de la virtualización del software, es que a pesar que exista una falla en el software, esta puede ser solucionada rápidamente creando así la mínima latencia o retardos temporales en la red para el usuario (Niles & Donovan, Virtualización e informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios, 2012, pág. 10). Asimismo, los sistemas virtualizados cuentan con la capacidad de reubicación automática en una zona segura cuando se causa una falla. Esto permite que a pesar de una falla, el sistema sigue arriba y está disponible sin tener que contar con sistemas físicos redundantes que aseguren la continuidad (Niles & Donovan, Virtualización e

[18] (Niles & Donovan, Virtualización e informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios, 2012, pág. 6)

informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios, 2012).

1.3.7.2. Tendencias según Datacenter Dynamics

Algunos especialistas afirman que para el 2014, los centros de datos van a seguir creciendo progresivamente como lo han venido haciendo en los últimos 5 años. Entre las tendencias principales, las empresas van a entender los centros de cómputo como una prioridad alta, pues los datos van creciendo cada minuto y estos deben ser procesados y almacenados en un centro especializado. Adicionalmente, el crecimiento de algunos centros de cómputo, llevará a los otros centros a aumentar su disponibilidad y eficiencia para llegar a un nivel similar. Por otro lado, se espera que la continuidad en la operación del sistema, se tome como una tendencia administrativa y se comience a entender el valor agregado que ofrecen estos centros. Por último, se tiene en cuenta la eficiencia energética como un factor que afecta el sustento de la empresa a pesar que la mayoría de las economías se declaren autosuficientes (Sánchez, 2014).

Una tendencia de las empresas para el 2014 es virtualizar los laptops y equipos de escritorio, permitiendo a los usuarios tener una movilidad y control sobre las aplicaciones que necesitan. Para esto, se tiene la idea de un auto servicio donde los usuarios descargan, instalan y actualizan las aplicaciones sin necesidad de un equipo de soporte. Esta idea va ligada a servicios de la actualidad como el Apple Store o el Play Store. Esto se logra mediante la virtualización de la oficina en el centro de cómputo. Adicionalmente, se espera la implementación de la nube híbrida que permite una infraestructura de cloud privada que cuente con los mismos servicios que una cloud pública como los que ofrecen las grandes empresas Amazon y Google (Toledo, El futuro es de la cloud híbrida, según Nutanix, 2014).

1.3.7.3. Casos de empresas

A continuación, se presentan algunos casos de empresas que han implementado mejoras en centros de datos y alianzas entre ellas para mejorar sus servicios. El primer caso es la alianza de Toshiba y NTT donde NTT ofrece su plataforma

Enterprise Cloud para los servicios de cloud y centro de datos a Toshiba proporcionando la expansión y gestión de operaciones en cloud accesible desde cualquier parte del mundo. En paralelo, Toshiba ofrece un sistema de almacenamiento de alta calidad y rendimiento (Villarrubia, Toshiba y NTT firman una alianza cloud global, 2014).

El segundo caso, es la empresa chilena Mas Errázuriz, la cual implementa la solución Dynamic Enterprise Computing de Level 3 que tiene como objetivo la virtualización y al mismo tiempo el respaldo de los recursos físicos. Con este cambio de sistemas, se minimizan los tiempos de indisponibilidad y se espera una mejora del 35% (Villarrubia, La chilena Mas Errázuriz optimiza su infraestructura TI con Level 3, 2014).

Por otro lado, un caso interesante es el de IBM, que prioriza el análisis de grandes volúmenes de datos. Para esto, la presidenta de IBM en España, Portugal, Grecia e Israel, afirma que la nube es uno de los factores que impulsa el progreso de una empresa. En cuanto a la implementación de la nube, IBM invierte en SoftLayer, el proveedor de infraestructura para cloud computing más grande del mundo; todo esto con el objetivo de implementar una red de 40 centros de datos alrededor del mundo (Toledo, IBM prioriza el análisis de grandes volúmenes de datos, 2014).

1.3.7.4. Cumbre de Gartner 2014

Gartner, la compañía líder en asesoramiento e investigación de la tecnología en el mundo, en la cumbre de centros de cómputo de Diciembre de 2013, realizada en Las Vegas, define las 8 fuerzas para dar forma a las estrategias de los centros de cómputo para los siguientes años. Definen que históricamente, los centros de cómputo se han visto como centros de prestación de servicios dónde se asegura el riesgo y el costo; de ahora en adelante, la agilidad, también va a ser un factor a tener en cuenta. La agilidad para Gartner es la velocidad a la que el equipo de tecnologías, responde a las necesidades de la empresa (Gartner, Inc., 2013).

A partir de esto, Gartner plantea 8 factores a considerar cuando se crea una estrategia para el desarrollo de un centro de datos, balanceando el riesgo, costo y la agilidad. Esto va a estar basado en la necesidad del uso tecnológicos de las 4 fuerzas Nexus: Social, móvil, nube e información (Gartner, Inc., 2013).

1. Mejorar la arquitectura de los procesadores y la memoria; la memoria principal de va a ser la ubicación para la información de las aplicaciones, soportada por memorias flash más económicas. Además, se usarán procesadores que consuman menos energía reduciendo así los costos.
2. La implementación del servicio de cloud y el rango de proveedores de este servicio seguirá incrementando, cambiando así los gastos de capital a gastos por funcionamiento.
3. Se invertirá en procesos operacionales y en herramientas mejoradas; si actualmente se necesita contar con un servicio de soporte, documentación, seguridad y manejo de la información, cuando la agilidad se comience a tener en cuenta, estos procesos van a ser aún más importantes.
4. Es importante contar con plan de continuidad de la información donde se incluyan planes de continuidad de la empresa y recuperación de desastres, reduciendo así el costo y la mejora en la agilidad.
5. Debido a la necesidad de crear aplicaciones basadas en las 4 fuerzas Nexus, se manejará la capacidad de crecimiento en hardware a través del análisis de la información. Esto afecta a la capacidad de almacenamiento, servidores y la red, por lo cual aumenta el tráfico en la red, el espacio en el centro de cómputo, la energía y la refrigeración.
6. Plan para el cambio del sistema operativo y las aplicaciones cambiando de UNIX a Linux, Windows seguirá creciendo e IBM O/S va a tener una expansión en ciertos lugares. Esta migración de aplicaciones comienza en el 2014 y para aplicaciones con condiciones extremas de disponibilidad y tiempo de respuesta, se comenzará en 2017.

7. Realizar planes para el cambio continuo optimizando continuamente el hardware y el sitio físico, evitando que esto se vea sólo como un plan a término definido, mejorando así la infraestructura y operaciones a un costo óptimo.
8. Obtener herramientas que manejen la infraestructura del centro de cómputo, pues las nuevas tendencias necesitan mayor capacidad de energía y enfriamiento que debe ser controlada para no generar gastos mayores.

1.3.7.5. Cloud Computing

La virtualización es la base para el cloud computing, este servicio ofrece ventajas económicas, velocidad, flexibilidad y agilidad cumpliendo con las características de la innovación. En el momento de realizar el cambio a la tecnología cloud, se deben tener en cuenta 3 factores: Primero, la manera en cómo se maneja, cambiando de la idea actual al despliegue de la misma; esto afecta la velocidad, agilidad e innovación. Por otro lado, se debe tener en cuenta el ambiente que se va a implementar ya sea nube pública, privada o híbrida. Por último, se debe analizar la seguridad, privacidad y el control que se le va a aplicar a la nube (Gartner, Inc., 2014).

Entre las 10 tendencias de estrategias tecnológicas planteadas por la empresa Gartner, se plantea el efecto que tiene una nube personal en una empresa y cómo esto impacta a los usuarios que tienen la necesidad de acceder a esta nube desde diferentes dispositivos, teniendo así como prioridad, la calidad de servicio que se le presta. Por otro lado, se define la nube híbrida como la visión a futuro, donde las empresas deben diseñar una nube privada con opción de incorporar los beneficios de la nube pública (Gartner, Inc., 2013).

1.4. Objetivos

- Identificar los estándares actuales y normas para los centros de cómputo.
- Crear un documento con las mejores prácticas a seguir para los centros de cómputo del tamaño de Pragcon.
- Aplicar la metodología y mejores prácticas definidas en el centro de cómputo de Pragcon.

- Encontrar las falencias y hacer las recomendaciones necesarias para contar con las adecuaciones óptimas para el funcionamiento de un centro de cómputo (en este caso Pragcon).
- Identificar cómo aumentar la eficiencia, la flexibilidad y vida útil de un centro de cómputo.
- Plantear una propuesta a futuro teniendo en cuenta la tendencia de los centros de cómputo de optimizar la energía y ahorrar costos mediante el uso eficiente de los recursos.
- Realizar las adecuaciones necesarias al centro de cómputo de la sede de Pragcon en Bogotá cumpliendo con las normas y mejores prácticas dedicando este espacio solamente para este fin (Estará limitado y definido a los recursos y disposición de la organización).

1.5. Metodología propuesta

A la hora de realizar el proyecto se van a tener en cuenta varias fases. La primera de estas, es la identificación del problema, en dónde se encuentran fallas de un sistema y la necesidad de la mejora continua. En este caso, se identifican las falencias de manera general que tiene el centro de cómputo de la empresa Pragcon en Bogotá y la necesidad de realizar e implementar unas mejoras.

La segunda fase, es la investigativa en donde se plantea una idea inicial para la mejora y solución de este problema. Para este caso, se van a consultar múltiples fuentes de información de las cuales se pueda extraer la información más relevante en cuanto a metodología, normas y buenas prácticas para un centro de cómputo. Para esto, se realizan consultas en artículos, revistas, manuales de buenas prácticas, documentos físicos, entrevistas e investigación en internet. Aquí se tendrán en cuenta aspectos como: Disponibilidad de los recursos, protección física, seguridad de la información, entre otros.

La tercera fase, es donde se realiza un estudio de factibilidad teniendo en cuenta el diseño y el sitio. Para esta fase se utilizará la documentación existente del centro de

datos de la empresa Pragcon. Esta información es muy limitada pues nunca se plasmó en un documento y los datos que se tienen, deben ser recuperados de correos electrónicos e información proporcionada por las personas que estuvieron a cargo del centro de cómputo en el 2008 y que siguen trabajando en la compañía.

Después de realizar estas investigaciones, se realizará un análisis de los resultados y se planteará una metodología y buenas prácticas a seguir a partir del estudio de normas y estándares relevantes e información general que pueda ser aplicada a este sitio. La implementación de esto, debe tener en cuenta el presupuesto de la compañía. En este proceso, se realizará una inspección del centro de cómputo para así poder plantear los cambios a lograr teniendo en cuenta las falencias actuales y que es lo más conveniente para prolongar el ciclo de vida de este centro. Aquí, se deben tener en cuenta dos principios básicos: "Crear diseños que contemplen la posibilidad de cambios futuros y asegurarse de contar con una estrategia eficaz de auditoria y actualización" (Schneider Electric Colombia, 2013).

Teniendo en cuenta que este cambio es cíclico y se debe estar realizando constantemente hasta llegar al punto de optimizar y ahorrar costos para la compañía; se plantea como recomendación, una metodología que incluye las buenas prácticas a seguir en un centro de cómputo y las revisiones que se deben realizar periódicamente para que los estándares siempre se estén cumpliendo. De esta manera, se garantiza que no se vuelvan a cometer las mismas fallas, que el centro de cómputo siempre está en mejora continua y que las normas y estándares principales se están cumpliendo. Esto se va a llevar a cabo con una lista de chequeo que se realizará periódicamente y en donde se podrán tomar medidas a seguir en caso de que exista una falencia; adicionalmente se implementarán los controles y se aplicará lo estudiado.

2. Resultados y discusión

2.1. Resultados

La empresa de Pragcon Bogotá[19], cuenta con un centro de cómputo que necesita ciertas adecuaciones. A continuación se presentan las características de este espacio. En el **Anexo 2**, se encuentran algunas imágenes que describen el estado del centro de datos.

2.1.1. Ubicación

El centro de cómputo está localizado en un edificio donde se encuentran las oficinas de la sede principal de la empresa Pragcon en Bogotá. En el **Anexo 9**, se encuentra un plano con el diseño general de la oficina.

2.1.2. Sistema de control de acceso

El edificio cuenta con un sistema de vigilancia y un sistema de control de acceso por medio de una tarjeta. Al ingresar a las oficinas de Pragcon en el piso 5, se cuenta con un sistema de control de acceso por medio de tarjeta. Después, se encuentra la recepción, donde están los vigilantes de la empresa; para ingresar a los puestos de trabajo, camino al centro de datos, se encuentra otro sistema de control de acceso por medio de tarjeta. Por último, para ingresar al centro de cómputo, se debe contar con la tarjeta de control de acceso debe tener los permisos necesarios. Adicionalmente, al momento de ingresar al centro de datos, se debe tener una carta de autorización por parte de alguien de Pragcon y una inscripción en la bitácora de ingresos.

2.1.3. Sistema de monitoreo

En el edificio se cuenta con un sistema de cámaras de seguridad para llevar un control sobre las personas que ingresan al edificio, ya sea en carro o a pie. Adicional a esto, Pragcon cuenta con un sistema de cámaras de seguridad interno; dentro del centro de cómputo, se cuenta con una cámara de seguridad que permite visualizar quién ingresa al centro de cómputo y así monitorear las acciones que realiza dentro de esta sala.

[19] Estos resultados son tomados de una empresa real que por cuestiones de seguridad no se revela el nombre de la compañía. Para relacionar la compañía en el estudio, se implementa el nombre ficticio Pragcon.

2.1.4. Espacio físico

El centro de cómputo, es un salón especializado para el almacenamiento de equipos informáticos. Este espacio cuenta con un piso falso, techos en concreto, paredes en concreto y en dry wall. El centro de cómputo mide 6,27 metros de largo, 3,7 metros de ancho y 2,54 metros de alto. Adicionalmente, el alto del piso falso es de 28 centímetros. Las imágenes de este espacio se encuentran en el Anexo 2.A

2.1.5. Ubicación de los racks

Se cuenta con 4 racks, 3 de ellos acomodados a 90 centímetros de la pared, organizados uno al lado del otro. El cuarto rack, está acomodado de frente a los 3 racks anteriores, a 90 centímetros de la pared, a 1,20 metros de la otra y a 1 metro de los otros 3 racks. En el **Anexo 2**, se encuentra el diagrama del centro de cómputo y la ubicación de los racks.

2.1.6. Aire acondicionado

El sistema de aires acondicionados, está conformado por dos equipos, uno de ellos tiene la tarjeta y el compresor dañado, por lo cual necesita ser sustituido. Aunque se cuenta con un equipo de refrigeración, este no está cumpliendo con los requerimientos mínimos para el funcionamiento adecuado, pues la sala no cuenta con la temperatura adecuada que es en promedio 18°C.

2.1.7. Sistema eléctrico

El sistema de energía con el que se cuenta actualmente, se contrata con el proveedor Codensa. Este servicio de electricidad llega al edificio por medio de un cable del exterior del proveedor y se va dividiendo la capacidad necesaria para cada uno de los 17 pisos del edificio. Cuando este entra al piso 5 a las oficinas de Pragcon, llega a una entrada UPD de 12 KVA y la de corriente es distribuida en 3 fases en donde se cuenta con una capacidad máxima de 20 amperios por fase. Actualmente, se está realizando una distribución errónea de estas fases; la primera de ellas está siendo sobre cargada, pues en esta fase, se tiene conectado el rack con las cámaras de seguridad, 2 servidores y un router, mientras que en la segunda fase, solo se tiene conectado un rack con 2 routers y otros equipos pequeños. Pragcon cuenta con una UPS que

funciona las 24 horas del día y regula los picos de voltaje que se tengan y una planta de baterías. Adicionalmente, el edificio cuenta con una planta eléctrica.

2.1.8. Cableado

El cableado del centro de cómputo necesita una revisión, pues muchos de los cables que estaban conectados en los equipos de los racks, están cruzados, es decir, que el cable marcado con un número no está conectado en ese punto. Adicionalmente, los cables no tienen una organización y muchos de ellos están fallando, pues el conector está partido o conectado incorrectamente. Las imágenes se encuentran en el **Anexo 2.B.** Adicionalmente, se realiza una nueva marcación para cada uno de los puntos identificando al punto de red al que corresponde con la siguiente nomenclatura: "DATOS09". Por otro lado, se crean marquillas para cada uno de los equipos con la siguiente nomenclatura "SW 07", como se puede ver en el **Anexo 2.D.**

2.1.9. Monitoreo de elementos

Cuenta con un sistema de monitoreo para el servidor primario y secundario, cuando alguno de estos dos genera alguna alarma, se notifica por medio de correo electrónico que el equipo está fallando. Por otro lado, el sistema de incendios, no cuenta con una notificación al administrador del centro de datos cuando se genera una alarma.

2.1.10. Documentación

Cuando se crea el centro de cómputo hace 5 años, se deja poca documentación sobre este, sólo se tiene un plano inicial y las especificaciones de algunos de los equipos. Este documento no se vuelve a actualizar a medida que se van realizando los cambios durante estos 5 años.

2.1.11. Sistema de control de incendios

Se cuenta con un sistema basado en 4 detectores fotoeléctricos, dos de ellos ubicados en el piso falso y los otros 2 en el techo. El cilindro contiene gas FM 200 y tiene una capacidad de 48,5 libras. Las imágenes del sistema se encuentran en el **Anexo 2.C.**

2.1.12. Capacitación en el sistema de extinción

El personal que está las 24 horas del día rotando en la oficina, no está al tanto del funcionamiento de este sistema y de cómo se debe activar o desactivar en caso que se cree alguna falla.

2.2. Discusión de resultados

A continuación, se realiza un análisis de la información obtenida de la empresa Pragcon, plasmada en la sección de resultados, comparándola con la información recopilada de estándares, revistas, artículos que se encuentra en el marco teórico. A partir de este análisis, se plantea la metodología a seguir para la creación de un centro de datos de pequeño y mediano tamaño, se plasman los cambios a realizar en el centro de datos de la empresa Pragcon y se plantean las mejores prácticas que se deben tener en cuenta para mantener y mejorar el centro de datos continuamente. En Anexo 5, se encuentran algunas imágenes del centro de datos, después de que esta información fue analizada y los cambios necesarios fueron aplicados.

2.2.1.Puesta en marcha

A la hora de construir o remodelar un centro de cómputo, es necesario realizar el plan de acción que se va a tener para todo el proyecto. La planeación, investigación y desarrollo previo de las ideas, evita múltiples fallas a la hora de estar ejecutando el proyecto. Con esto, no se logra evitar el 100% de los errores, pero si la mayoría de las fallas. En caso de no realizar un planeación previa, es muy probable que los costos y el tiempo de ejecución del proyecto, sean mucho mayores a lo que se esperaba. Para poder llevar a cabo un plan de acción, según el APC en su informe “proyectos de centros de datos: La planeación del sistema”, se necesitan 2 etapas; la primera en donde se realiza la planeación y la segunda en donde se construye esta propuesta. A continuación, en la **Figura 13**, se muestra el diagrama de etapas para la planeación y construcción del centro de datos según APC.

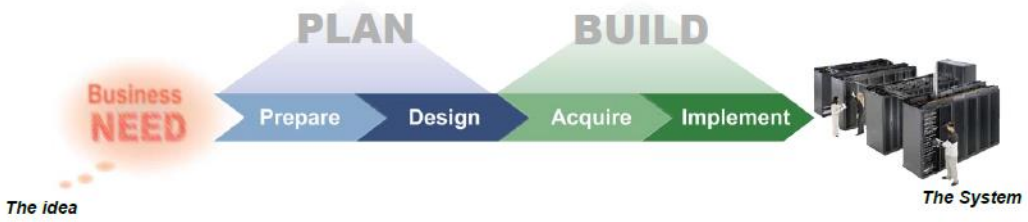


Figura 13. Planeación del proyecto para un centro de cómputo[20]

Entre la primera fase de planeación, se encuentra la preparación y el diseño del proyecto teniendo en cuenta los aspectos más relevantes y las normas actuales para el diseño del centro de cómputo. Dentro de esta fase, se tiene en cuenta la infraestructura física y se analiza cada uno de los aspectos que esto conlleva. En la segunda fase de construcción, se adquieren los equipos e implementos necesarios ya estipulados en la primera fase y después se realiza la implementación y construcción del proyecto. Para todo tipo de empresas, es necesario contar con este plan de acción, asesorándose con los especialistas para cada uno de los temas evitando los riesgos más comunes. Adicionalmente, se puede planear el futuro del centro de cómputo, permitiendo que este sea flexible al cambio teniendo en cuenta las nuevas tendencias. En el Anexo 1, se puede encontrar un cronograma con las actividades realizadas durante estas fases.

2.2.2.Normas más significativas para un centro de cómputo

Un centro de cómputo, es un lugar especializado para la ubicación y manejo de los equipos informáticos en una empresa. Estos, son de gran importancia para todas las empresas, pues aquí es en donde se asegura uno de los activos más importantes que es la información. Dependiendo del tipo de empresa en la cual se implementa un centro de cómputo, es necesario tener en cuenta ciertas características que van variando de acuerdo a las aplicaciones e información a manejar. Para poder llevar a cabo la construcción o modificación de un centro de datos, se tienen unos estándares a seguir, en los cuales se validan los diferentes aspectos; la mayoría de estos se basan en estándares ya creados por diferentes entidades. A continuación en la **Tabla 4**, se

[20] (Rasmussen, Proyectos de centros de datos: La planeación del sistema, 2010, pág. 4)

presentan algunos de los estándares mínimos a tener en cuenta a la hora de crear o modificar un centro de cómputo.

Tabla 4. Normas en los centros de cómputo

Norma	Descripción
UNE-ISO/IEX 17799	La información como uno de los activos más importantes de la empresa.
TIA-942	Infraestructura y ubicación del data center: Se especifica la estructura para las telecomunicaciones y el cableado en cualquier centro de cómputo.
ISO-IEC 24764	Enfocada en el sistema de cableado de cobre y fibra óptica de un centro de cómputo, la estructura y los configuraciones mínimas del cableado, los requerimientos de desempeño de los canales y componentes, implementación, procedimientos y verificación de los mismos.
ISO/IEC 11801	Identifica los elementos funcionales de los cables y su conexión para formar subsistemas.
NFPA 75	Prevención de incendios: Protección de equipos electrónicos y de procesamiento de información.
NFPA 25	Mantenimiento de un sistema contra incendios implementado en un centro de cómputo que esté basado en agua. El procedimiento se realiza mediante la inspección y pruebas de los aspersores y el sistema en general.
ANSI/TIA/EIA-569-A	Estándar comercial de construcciones para espacios y caminos de telecomunicaciones: Relaciona temas del acceso a los pisos, caminos de los cables, instalaciones de la entrada, caminos al interior del edificio, área de trabajo, entre otras.
TIA-569	Estandarizar el camino específico, el diseño del espacio y las buenas prácticas en la construcción para edificios con equipos de telecomunicaciones.
ANSI/BICSI-002	Mejores prácticas para el diseño e implementación en un centro de cómputo.
ISO 20071	El derecho informático y gestión de la seguridad de la información.

ISO 20071 A.10.10	Sistema de monitoreo del centro de cómputo detectando de actividades no autorizadas en la información.
ISO 27001 A.9.1	Seguridad física y ambiental: Prevenir el acceso a personal no autorizado que pueda dañar o interferir en las premisas e información de la compañía. En esta norma se tiene en cuenta la seguridad física perimetral, controles de acceso, seguridad de las oficinas, protección contra amenazas externas y trabajo en áreas seguras.
ISO 27001 A.10.5.1	Mantener la integridad y disponibilidad de la información y las facilidades para procesarla. Esta norma exige que se realicen backups de la información y del software realizando pruebas periódicas de acuerdo a las políticas de copia.
ISO 27001 A.14	Definir un plan de continuidad para el negocio protegiendo los procesos críticos dela empresa de las grandes fallas de los sistemas de información de la empresa y desastres asegurando el levantamiento de la información en poco tiempo.
IEC 61000-4-2	Define las propiedades antiestáticas de los pisos y dimensiones de las puertas.

2.2.3.Niveles Tier

A partir de estas recomendaciones y características de un centro de cómputo, se crea una segmentación por tipo de centro de cómputo basándose en la disponibilidad del mismo. Estos niveles, se clasifican en cuatro grupos llamados Tier. A continuación en la **Tabla 5**, se establecen algunas de las características de cada uno de estos niveles y se observa como a medida que se va aumentando de nivel Tier, el centro de cómputo debe contar con una mayor disponibilidad en cada uno de sus equipos informáticos.

Tabla 5. Características de niveles Tier

Nivel	Características
Tier I	• Se tiene un espacio especializado para el almacenamiento de los equipos. • Se cuenta con un sistema de alimentación ininterrumpida que filtre los picos de voltaje y las caídas momentáneas de energía. • Sistema de enfriamiento las 24 horas del día.

Tier II	• Sistema que controle las caídas constantes de energía. • Cuenta con UPS, enfriadores, equipos que reaccionan al calor. • Se permite que un equipo deje de funcionar mientras sea por un mantenimiento con previo aviso o falla inesperada.
Tier III	• El mantenimiento de los equipos con previo aviso no debe afectar la disponibilidad de los servicios prestados por los equipos de tecnología.
Tier IV	• Tolerante a fallas o mantenimientos sin previo aviso de todos los equipos. • Permite la falla de varios equipos simultáneamente sin afectar su disponibilidad.

A partir de estos niveles, se crean centros de cómputo en cada una de las empresas dependiendo de la necesidad y la información que se esté manejando. Por ejemplo, en una empresa mediana de distribución e importación de materiales, no es de vital importancia contar con un centro de datos Tier IV, pues aunque es importante tener la información de la compañía disponible, este servicio puede tener fallas y no generar un impacto tan contundente en la compañía. Por otro lado, una empresa que presta servicios de telecomunicaciones, debería contar con un centro de cómputos mínimo Tier III, pues si el servicio que se está prestando, llega a tener alguna falla inesperada, se debe contar con un plan de contingencia y unas medidas básicas de seguridad del flujo de la información y disponibilidad de la misma, pues muchas personas se ven afectadas.

En el caso específico de la empresa Pragcon, el centro de cómputo cuenta con características del nivel Tier II. Aunque para la empresa es de gran importancia contar con un centro de datos, el cual debe asegurar la disponibilidad de los equipos y servicios las 24 horas del día, una falla puede ocurrir y esta no tiene un impacto que defina la estabilidad de la compañía.

2.2.4. Seguridad de la información

A partir de estas normas y los niveles Tier, se deben tener ciertas características en cuenta a la hora de crear o remodelar un centro de cómputo. Cuando se realiza un

centro de datos, generalmente, nace por la necesidad de la compañía de asegurar los servicios y contar con las condiciones para su adecuado funcionamiento. Muchas de las empresas asignan un espacio sin tener en cuenta que se está manejando toda la información y que a un largo plazo, va a ser necesario adecuar un lugar especializado.

En el caso específico de Pragcon, en el centro de cómputo, se cuenta con múltiples servidores que alojan el software e información de la compañía como las ventas de los productos. En el día a día, es necesario acceder a esta información para asegurar que los diferentes productos están siendo distribuidores, legalizados, están disponibles en las cadenas y finalmente están siendo vendidos. Con esta información, se miden los objetivos anuales de la compañía; pues el software alojado en estos servidores, permite a los usuarios acceder diariamente a la información. Se recomienda que para un futuro virtualizar los servidores.

Adicionalmente, es necesario que se proteja esta información, pues el personal externo, no debe tener acceso, ya que partir de estos datos, se pueden crear estrategias de ventas que afectan directamente al desarrollo de la compañía. Por otro lado, es obligatorio que la información no pueda ser modificada por alguien externo. Teniendo en cuenta las razones mencionadas anteriormente, la información debe cumplir con los tres principios básicos de la seguridad de la información que son disponibilidad, integridad y confidencialidad. Asegurando esto, se está teniendo en cuenta la norma UNE-ISO/IEX 17799, donde se explica que la información es uno de los activos más importantes de la compañía.

2.2.5. Ubicación y estructura

Una de las primeras decisiones que se toma para el diseño del centro de datos, es la selección del sitio y el tipo de construcción en el que este va a estar ubicado. En la actualidad, muchos edificios cuentan con un sistema anti sismos que permite que en caso que exista un terremoto, el edificio siga en pie. Adicionalmente, el sitio seleccionado, debe estar lo más lejos posible de grandes estructuras hidrográficas, evitando el riesgo por inundación.

En el momento de hacer la remodelación en Pragcon, la ubicación del centro de datos no se cambió. En este caso, no se recomienda cambiar el sitio, pues este es un espacio que está separado de las oficinas y está especializado en el almacenamiento de los equipos informáticos y ya cuenta con algunas de las recomendaciones mínimas para estos espacios. Adicionalmente, Pragcon cuenta con una sala donde se almacena la UPS y las baterías, por lo cual también se está cumpliendo con esta norma. Se recomienda que se identifique el centro de datos pues al estar en este lugar especializado, un personal limitado sabe dónde se encuentran todos los equipos informáticos de la compañía.

2.2.6.Diseño

Es importante tener en cuenta la seguridad física del centro de cómputo desde el diseño externo hasta el diseño interno y ubicación de cada uno de los equipos, pues esta infraestructura es la que asegura la disponibilidad de la información. La mayoría de los centros de cómputo pequeños, son inseguros, desorganizados, no tienen una supervisión adecuada y cuentan con un tamaño muy reducido. En gran parte, los errores que se comenten, se crean por falta de conocimiento y por errores humanos.

Es vital contar con una base sólida para el diseño inicial, en donde se analiza no sólo la necesidad actual de la empresa, sino también la flexibilidad de cambio a futuro. Además, se evitan fallas ya mencionadas por otras empresas y se aplican las soluciones estándares para los centros de cómputo. Asimismo, se debe llevar un control en el manejo de los equipos y los cambios realizados en el centro de cómputo. El objetivo de realizar el seguimiento continuo en un centro de datos, es evitar que se esté sobre utilizando o esté siendo implementado para un fin diferente a su propósito.

En Pragcon, se da este caso, pues a los 5 años de construido el centro de cómputo, no se lleva un monitoreo continuo y parte de este espacio es implementado como bodega, causando un riesgo para los equipos y la compañía en general. Como se sabe, para tener un centro de cómputo nivel Tier I, se debe tener un espacio especializado para estos equipos y este requerimiento básico se estaba incumpliendo.

Para solucionar esto, se implementa una división de vidrio dentro de este espacio, separando así el espacio que utilizan los equipos y los racks, del espacio en donde se el equipo de tecnologías almacena y deja algunos equipos ejecutando ciertos procesos. Las cajas y equipos antiguos no permitían monitorear adecuadamente los equipos de los racks y creaban un riesgo en caso de incendio o terremoto. Se realiza esta división de vidrio, pues al separar el espacio que existe para el almacenamiento de los equipos del área de trabajo del centro de datos, se consigue una mayor seguridad para los equipos, aislamiento de los mismos y un mayor control sobre el manejo de los mismos. Se recomienda que este espacio siga siendo utilizado sólo para el almacenamiento de los equipos que actualmente están activos y que los equipos que salgan de funcionamiento, sean desechados de manera adecuada y no almacenados en esta sala.

2.2.7. Backup

En un centro de cómputo, se debe tener en cuenta el efecto de las catástrofes naturales, contando con un plan de contingencia. Para Bogotá, se está lejos de un mar o fuente hidrográfica amplia que pueda causar una inundación o maremoto, pero no se está exento de un terremoto, por lo cual es importante tener esto dentro de las fallas sin previo aviso. Una recomendación es tener una copia de la información más relevante en un servidor ubicado en otro país u otro lugar diferente al centro de datos. Teniendo presente este backup de información, se tiene en cuenta la norma ISO 27001 A.10.5.1 manteniendo la integridad, disponibilidad de la información y las facilidades para procesarla por medio de copias de seguridad (Ministry of Gender Quality, 2006, pág. 9).

Actualmente, Pragcon genera una copia del día a día en unas cintas de seguridad que son controladas por IBM y que son almacenadas en una bodega aparte de la sede principal. Estas copias se realizan de esta manera, pues dos veces a la semana, se entregan estas cintas y se asegura que en caso de necesitar un backup, este va a estar disponible en las cintas que son almacenadas por IBM. Adicionalmente, muchos de los servidores, están alojados en otros países y en caso que ocurra un desastre natural,

sería necesario adquirir nuevamente el hardware para la conexión a estos servidores remotamente, pero la información podría ser recuperada. Una recomendación, es realizar pruebas de restauración y verificación de los backups periódicamente.

2.2.8. Acceso físico

Para asegurar el lugar, se debe tener un sistema de control y registro de las personas que ingresan a la edificación y al centro de cómputo. Este no basta para asegurar el acceso al personal autorizado, pues estos sistemas a pesar de ser muy robustos, no tienen una inteligencia propia, por lo que no pueden evitar que usuarios no autorizados implementen alguno de los sistemas de acceso para ingresar sin permiso. En este caso, es indispensable contar con un personal de vigilancia que controle el ingreso.

Un sistema de control de acceso puede ser tan robusto como se desee, dependiendo de las necesidades de la empresa y del presupuesto de la compañía. Muchas veces, esta es una de las características más vulnerables porque en la mayoría de los casos, el acceso depende de un dispositivo que puede ser utilizado por una persona no autorizada. A medida que el sistema se va volviendo más complejo, es más difícil vulnerarlo, pero cada vez, va siendo más costoso. Para una mayor seguridad, está el reconocimiento por medio de un sistema biométrico, el cual de cierta manera, asegura que la persona que está ingresando al sistema, cuenta con ciertos rasgos físicos únicos. Generalmente, estos sistemas de control de acceso, son un riesgo para las compañías, pues no todos los sistemas son confiables y los más avanzados, no están 100% desarrollados y son susceptibles a fallas.

En Pragcon, se cuenta con un personal de seguridad; cumpliendo así con uno de los requerimientos mínimos y que en términos generales, el acceso a personal no autorizado está siendo controlado. Después del estudio, se instala un equipo para visualizar todas las cámaras de la empresa desde la recepción, garantizando que se va a tener un monitoreo continuo de los movimientos de toda la empresa. En total se cuenta con 19 cámaras ubicadas en diferentes zonas de la oficina, son cámaras de movimiento. Este sistema cuenta con un sistema de monitoreo por medio de una

dirección IP lo cual permite tener un monitoreo de la empresa estando dentro o fuera de las oficinas.

En este caso, se recomienda que se siga realizando un monitoreo continuo y que periódicamente, se revise el sistema de cámaras de seguridad. Actualmente, no se realiza un monitoreo continuo del sistema de vigilancia, sólo se está en contacto con el proveedor en caso de falla. Adicionalmente, se sugiere contar con una política para la retención de videos, así como pruebas y verificaciones periódicas.

Después del análisis realizado, en Pragcon, no se hace ningún cambio en cuanto al control de accesos por tarjeta. De igual manera, se recomienda revisar quién tienen acceso a este espacio y limitar la entrada para las personas que realmente deben ingresar pues actualmente se da un acceso permanente a los usuarios. Se recomienda que en un futuro, se implemente un mejor sistema de control de accesos como un sistema biométrico. Además, se recomienda seguir la bitácora de ingreso al centro de datos y el control por medio de cartas de autorización de ingreso. Con esto, se cumple con la norma ISO 27001 A.9.1 donde se previene que el personal no autorizado ingrese, dañando o interfiriendo en las premisas e información de la compañía (Ministry of Gender Quality, 2006, pág. 5). Por otro lado, se recomienda realizar una validación periódica del registro de personas que ingresan al centro de datos por medio de tarjetas.

2.2.9.Personas

En todas las empresas, debe existir un administrador del centro de cómputo o un equipo de infraestructura, que van a ser los encargados de toda la administración y gestión de los elementos que integran el centro de datos. Adicionalmente, se debe contar con un personal certificado y capacitado para tener una buena gestión de los recursos y tener un óptimo tiempo de respuesta en caso de fallas. En cuanto a las capacitaciones para el personal de la empresa, se recomienda realizar una capacitación semestral en donde el personal que está rotando en la empresa, sepa manejar el sistema en general y sepa las políticas de la empresa.

Después del estudio realizado al centro de datos, se sabe que existe un equipo de infraestructura. También, se cuenta con un personal especializado de IBM, que es el encargado de controlar el acceso, hacer un seguimiento de los cambios y asegurar que el proceso de backup de la información se está llevando a cabo. Se recomienda revisar los acuerdos de confidencialidad y seguimiento del trabajo diario que se tiene con la empresa IBM.

Por otro lado, se tiene una capacitación en el sistema de incendios para los usuarios que están en contacto constante con el centro de cómputo y con el equipo de vigilancia de Pragcon, de esta forma, en caso que ocurra alguna emergencia o sea necesario activar o desactivar el sistema, el personal esté en capacidad de realizar este procedimiento.

2.2.10. Refrigeración

A pesar de que el centro de cómputo es un lugar especializado para el almacenamiento, monitoreo y procesamiento de información, es necesario regular el ambiente que se tiene dentro de la sala. Para esto, se hace un estudio sobre los elementos o recursos que se encuentran dentro del centro de datos.

El flujo del aire dentro del centro de cómputo, afecta directamente al funcionamiento de los equipos, pues si no se cuenta con la temperatura adecuada, existe un alto riesgo de falla. Adicionalmente, al tener el ambiente controlado, se genera un ahorro en el consumo de energía. A medida que se toman las prevenciones necesarias, como la separación de aires en los diferentes pasillos, buena práctica incluida dentro de la norma TIA-942, se reduce el uso de equipos extra para regular cada una de las zonas del centro de cómputo.

Para muchas empresas, basta el simple hecho de implementar un sistema de aires acondicionados dentro del centro de cómputo que mantenga este espacio en una temperatura promedio y no se tiene en cuenta que puede estar generando un mayor consumo de energía, un desgaste de los equipos por falta de planeación y un riesgo para la disponibilidad de la información. Este tema es de gran importancia, ya que la

tendencia de los centros de cómputo es reducir su espacio cada vez más implementando equipos con mayor capacidad. Al tener un menor espacio, el calor se concentra más fácilmente y es más difícil regularlo.

En Pragcon, se cuenta con un sistema de aire acondicionado que se mejora después del análisis realizado. Se cambia del aire acondicionado que estaba fallando, sustituyéndolo por uno referencia Mini Split pared de 24.000 Btuh R 410ª. Al mismo tiempo, se hace el cambio de las tuberías de líquido, las tuberías de succión, se realiza un aislamiento tipo rubatex y se obtiene el refrigerante R-410ª. Adicionalmente, se cambia la tubería PVC y la bomba de condensado; este nuevo equipo usa gas freón y es capaz de regular automáticamente la temperatura del sitio para que siempre esté en un promedio de 18°C.

En este caso, se crea una zona de flujo aire frio, que es separada por la división de vidrio mencionada anteriormente. En esta sección, están ubicados los 4 racks, esto con el fin de que la zona de los equipos informáticos siempre esté en una temperatura promedio de 18°C regulada automáticamente por el nuevo equipo. Este equipo de aire acondicionado fue seleccionado, pues al controlar la temperatura del ambiente, se asegura un ahorro de energía, pues solo se emite aire frio cuando la sala, cambia la temperatura promedio. Adicionalmente, la implementación de este equipo, asegura que los niveles de temperatura siempre estén dentro del rango establecido evitando que las fallas se dupliquen por causa del aumento de la temperatura. El sistema cuenta con una revisión mensual por parte de la empresa Aire Service; se recomienda seguir con esta revisión mensual y realizar los cambios necesarios sugeridos a lo largo de estas revisiones.

2.2.11. Sistema de monitoreo y funcionamiento de elementos del data center

A pesar que los equipos tienen la capacidad de operar sin necesidad de una supervisión constante, es necesario contar con un monitoreo de los mismos. Para esto, hoy en día se cuenta con sistemas de notificación a los usuarios cuando uno de los equipos informáticos genera una alarma. Esto es de gran importancia, pues los

equipos en el momento de tener una falla, no cuentan con la capacidad de tomar una decisión para encenderse de nuevo o arreglar la falla que tienen.

Es una muy buena práctica detectar cuando un equipo está fallando para así poder accionar y solucionar el problema antes de tener un mayor impacto. Para Pragcon, es de gran importancia continuar con este seguimiento en el servidor primario y secundario. Para este caso, se realiza un monitoreo continuo del sistema de tal manera que al momento de presentar una falla, se notifica de inmediato al equipo de infraestructura. Por otro lado, el sistema de incendios no contaba con una notificación al administrador en momento de alarma, para esto, se instala un marcador telefónico, que informa al administrador por el celular cuando el sistema está fallando. Es recomendable seguir con este monitoreo y llevar un control sobre las personas a las que se les está informando sobre esta falla, para asegurarse que son las personas que pueden reaccionar en caso que se presente una alarma.

2.2.12. Protección contra incendios

Actualmente, existen varios métodos para identificar un riesgo por incendio antes que ocurra y en caso que acontezca evitar un problema mayor. Para implementaciones básicas se debe contar con un extintor cerca al centro de cómputo que pueda ser accionado manualmente en caso de incendio; sin embargo, esta no es la mejor práctica para un sitio como estos, pues no se cuenta con la precaución las 24 horas del día. Muchas veces, tener un sistema actualizado, con supervisión esporádica y mantenimiento periódico, no es fácil, pues es un poco costoso, pero pensando a futuro, la detección automática de una falla, puede ser solucionada al instante y causar pérdidas mucho menores. Cuando se tiene una prevención sobre la posibilidad de incendios en un centro de cómputo, se aplican los principios básicos de la norma NFPA 75. Adicionalmente, se debe tener en cuenta que en estos espacios no es permitido el uso de fuego y está prohibido fumar, esto se puede enmarcar por medio de señalización dentro del centro de datos. Por otro lado, los materiales para la construcción se seleccionan de acuerdo a las normas establecidas, evitando que los

materiales puedan generar un incendio o que el peso de los pisos y techos no sea el adecuado.

Después del análisis, es necesario desinstalar el cilindro y retirar libras de gas, pues según los cálculos hidráulicos, la cantidad de gas debe ser menor para que este no sea tóxico, pues el volumen que ocupa en nuevo centro de cómputo es menor. Por otro lado, se suministra la nueva tubería, se cambian algunos detectores fotoeléctricos que estaban fallando y se reinstalará la tubería eléctrica y el cableado. Se selecciona este sistema de extinción de incendios pues este es el estándar para implementar en un centro de datos, pues en caso de requerir apagar un incendio, el tipo de gas implementado debe cumplir con las características necesarias para no dañar los equipos, permitiendo que estos puedan seguir funcionando a futuro.

Además, se revisa el panel de control y se le hace un mantenimiento, pues una de las baterías de 12 voltios, estaba fallando y estaba generando una alarma. Este sistema no tenía un mantenimiento hace 2 años, por esto, de ahora en adelante, se contrata un servicio de revisión trimestral en donde se realizan los mantenimientos preventivos a los equipos, contando así con un soporte continuo del sistema. Se recomienda que a medida que se realice el mantenimiento, se tengan en cuenta las recomendaciones realizadas por parte de la empresa Incoldext, con la cual se está trabajando actualmente.

A medida que se va estructurando un centro de cómputo, va aumentando la prioridad para cada uno de estos sistemas. Por ejemplo, en el centro de cómputo de un banco, es necesario tener un sistema contra incendios que permita una acción inmediata en caso de una alerta; mientras que en el centro de cómputo de una sucursal que se usa como bodega de los pedidos, no es necesario un sistema tan robusto como el caso de la bodega de Pragcon en Bogotá, que sólo se cuenta con un extintor como medida preventiva en caso de incendio.

2.2.13. Telecomunicaciones

El cableado a implementar en un centro de datos es de gran importancia porque este es el medio físico con el cual se conectan los diferentes dispositivos y es la forma como realmente se crea la arquitectura de la red. La transmisión de la información requiere cada vez más velocidad y por esto en los últimos 20 años, se ha tenido un cambio tan drástico en el cableado vertical de un centro de datos. Anteriormente, se implementaban topologías de anillo de aproximadamente de 16 megabytes y actualmente podemos contar con tecnologías hasta de 100 gigabytes para el cableado vertical; afectando el tamaño y diseño de la red. Además, los equipos que se implementan y el tipo de cable han cambiado de cobre a fibra óptica. Este cambio continuo se da por la necesidad de los usuarios de aumentar la velocidad de conexión a los servicios que se ofrecen día a día. Es necesario que el centro de datos sea flexible; permitiendo así la mejora progresiva y la implementación de nuevos equipos y tipos de conexiones para que se cumpla con las necesidades de los usuarios.

Después del estudio realizado, se hace una reacomodación de los racks, donde se desconecta todo el cableado del centro de cómputo y se acomodan nuevamente los cables organizadamente y se revisa que cada punto esté funcionando correctamente. Las dimensiones actuales del centro de cómputo son las siguientes: 3,19 metros de ancho por 3,7 metros de largo. La altura del techo y del piso falso se conserva. En el Anexo 4, se encuentra el diagrama del nuevo diseño del centro de cómputo.

Adicionalmente, según las normas de marcación del cableado, se cambia la marcación por medio pines a adhesivos para cada uno de los cables especificando a qué punto deben ir conectados y a qué número de equipo dentro de ese rack. Este cambio se implementa para evitar el daño de los cables por causa de los pines. Por otro lado, se cambian los cables que estaban fallando y se compran unos nuevos cables que cumplen con las normas actuales para el cableado del centro de cómputo. Se recomienda que de ahora en adelante, se controle el acceso al centro de cómputo para evitar que cualquier persona intercambie la conexión de uno de estos puntos para habilitar otro que esté fallando. Esta era una de las prácticas que se tenía

anteriormente y por esto era que muchos de los cables estaban conectados en el punto incorrecto, causando así un desorden en el cableado.

Para generar una mayor organización en el cableado y siguiendo las políticas establecidas, se crea un documento donde se anexan todos los puntos de red que tiene la oficina, especificando a que número de punto corresponden en el centro de cómputo. Con esto se asegura que se tiene una documentación adecuada de la distribución del cableado de la oficina, en caso de necesitar algún cambio o revisión de un punto, se cuenta con un plano permitiendo solución más fácil y rápida. Por otro lado, se recomienda contar con un equipo de red redundante que permita la disponibilidad de la red en caso que el equipo principal presente alguna falla.

2.2.14. Sistema eléctrico

Es de gran importancia evaluar todos los riesgos en las instalaciones eléctricas con el fin de asegurar las personas y el ambiente. Entre las posibles fallas, se encuentra la ausencia de energía, cortocircuitos, rayos, equipos fallando, sobrecarga, entre otros (Codensa, 2006, págs. 12-13). El sistema eléctrico que se implementa en un centro de cómputo, genera un impacto tanto económico como de disponibilidad de la información en la compañía. Uno de los mayores riesgos que se tiene al momento de instalar un equipo es no contar con un sistema eléctrico adecuado.

En Pragcon, para poder solucionar problema de la distribución errónea en las 3 fases del sistema, se hace una nivelación de las cargas que se tenían en el centro de cómputo, dejando cada una de ellas consumiendo aproximadamente 15 amperios por fase. Estos cambios afectan positivamente, pues al nivelar las cargas, las fases son más estables permitiendo que exista un flujo constante de la corriente. Se tiene como recomendación disminuir el consumo de amperios por fase 12 aproximadamente. Además, es importante validar que se cuenta con un sistema de UPS adecuado que puede soportar la carga por un tiempo de falla del sistema eléctrico y con una planta eléctrica.

2.2.15. Documentación

Para tener una mejora continua del centro de datos, es vital contar con la documentación apropiada que defina una estructura, el diseño y las configuraciones de los equipos, permitiendo así que la información no sólo quede en manos una persona. Es necesario que la información quede protegida contando con un backup de todas las configuraciones. Esto es de gran importancia pues sirve como elemento de auditoría para cada uno de los equipos.

A partir de estos cambios realizados en Pragcon, se crea un documento con la información básica y más relevante del centro de cómputo. Adicionalmente, se actualiza la carpeta con las cartas de autorización de ingreso al centro de datos, la cual es administrada por el equipo de infraestructura. Por otro lado, se realiza la marcación adecuada de todos los equipos del centro de cómputo con un adhesivo especificando a qué equipo corresponde, pues anteriormente, sólo se podían identificar los equipos por medio del serial y en muchos equipos, no era fácil encontrar este número; esto se deja documentado en un archivo anexo. La buena práctica, es realizar una documentación adecuada y que a medida que se realice algún cambio, se evidencie para efectos de seguimiento.

2.2.16. Optimización de recursos

Los beneficios al realizar la optimización de los recursos son tanto económicos como administrativos dando unos mejores tiempos de respuesta. Muchas veces, la empresa cuenta con software y hardware que no está en uso o que está siendo subutilizado. Ligado a esto, está el consumo de energía del centro de datos, pues se asegura que los únicos equipos que van a estar generando un consumo son los que están activos. Para este caso, en Pragcon, dos de los servidores que estaban en el centro de cómputo, estaban inactivos y ya no estaban siendo usados por ningún usuario, pero estaban encendidos y consumiendo energía. Se realizó la validación con el proveedor de este servicio, Verizon y se valida que efectivamente estos equipos no estaban en uso y se apagan para que dejen de consumir energía y así evitar un gasto innecesario para la compañía. Se recomienda realizar un monitoreo periódico de los equipos definiendo cuales están activos.

Otra validación para optimizar los recursos, es realizar una consolidación de servidores físicos, es decir, que se pueda reemplazar un servidor adicionando un complemento a un servidor ya existente. En el caso de Pragcon, se toma la decisión de adquirir una tarjeta PVDM64, esto con el fin de permitir que el tráfico de voz funcione en el router de backup cuando el primario falle; de esta manera, se enrutan las llamadas IP a través de la conexión WAN de backup si la conexión WAN primaria se cae. Con esta tarjeta incorporada, se retira el equipo del centro de cómputo que estaba cumpliendo esta función, así se obtiene en el espacio en el rack, un menor consumo de energía y se minimiza la emisión de aire caliente. Con este cambio, se tolera una falla en el servidor primario sin afectar la telefonía IP.

Paralelamente, es necesario aplicar el concepto de virtualización y las ventajas que esta trae para los usuarios y la empresa. Para esto, se realiza la virtualización de 35 equipos, cambiando de los equipos de escritorio a equipos thin client, que manejan una máquina virtual y todas las aplicaciones e información en un servidor. Es decir, que ahora los usuarios se conectan a su sesión virtual para poder acceder a su información día a día. Esta virtualización de los equipos trae grandes ventajas, pues al contar con una sesión virtual, se da una mayor movilidad a los usuarios, pues anteriormente no podían acceder a sus equipos empresariales desde fuera de la oficina, ahora sólo requieren una clave para una conexión remota y desde cualquier equipo personal pueden acceder a esta información tal y como si estuvieran en la oficina. Además, estos equipos apoyan la eficiencia energética pues consumen menor energía que un equipo de escritorio y cuentan con las mismas funcionalidades y aplicaciones para el día a día de los usuarios. Por otro lado, se recomienda a futuro, realizar una virtualización de los servidores para poder asegurar que la información está disponible y que se tiene una mayor flexibilidad en estos servidores.

2.2.17. Tendencias

En los últimos años, los cambios tecnológicos han generado una necesidad de mejora continua que va ligada a grandes volúmenes de información que requieren ser almacenados y procesados. Este es un proceso complicado pues requiere de un

respaldo económico de la empresa y no se cuenta con un estándar para aplicar estas nuevas tendencias. Para estos cambios, es necesario contar con un plan de acción, que no tenga una fecha de fin y que siempre esté abierto permitiendo una flexibilidad.

En cuanto a las tendencias, se puede realizar la virtualización de equipos y analizar el efecto de este cambio. Se debe tener en cuenta que en caso de no realizar la virtualización adecuada, se genera un mayor costo, menor disponibilidad, mayor consumo de energía y necesidad de equipos para enfriamiento. Otra tendencia es llevar un monitoreo automático de la infraestructura del sitio. Esto, se realiza a través de un software que revela datos de consumo de energía, capacidad disponible, calor emitido, entre otros. Con estos valores, se realiza un análisis de la infraestructura actual, permitiendo la mejora en términos de temperatura y consumo de energía. Ligado a esto, se espera un impacto ambiental por medio del uso eficiente de los equipos, pues al poder monitorearlos, el objetivo es distribuir equitativamente el consumo de energía, enfriamiento y procesamiento de datos en todo el centro de cómputo.

Es claro que no todo puede migrar a la nube, pues aunque se tienen grandes beneficios, no se cuenta con un sistema totalmente robusto. También esto genera un consumo en la red, un tiempo de procesamiento y que estos procesos cada vez se van volviendo más demandantes y exigen cada día mejores recursos.

En el caso específico de Pragcon, se tiene como plan a futuro, realizar la virtualización de la aplicación del correo electrónico, permitiendo una mayor capacidad de almacenamiento para cada uno de los usuarios.

2.2.18. Estadísticas

El instituto UpTime realiza anualmente una encuesta a las industrias de los centros de cómputo, la última encuesta fue realizada en de Febrero a Abril de 2013 a 1000 personas, entre ellos operadores, gerentes de tecnologías y ejecutivos alrededor del mundo. A continuación se presentan algunos de los resultados (Stansberry, 2013). En la **Figura 14**, se clasifican las 1000 personas que realizaron la encuesta por lugar en el

que se encuentran ubicados y área a la que pertenecen dentro de la compañía a la que se le está realizando el análisis en la encuesta.

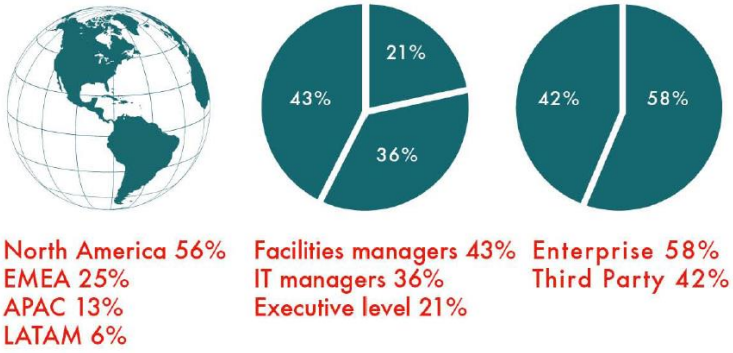


Figura 14. Demografía de la encuesta de centros de cómputo por UpTime en 2013[21]

En cuanto al caso específico de Latinoamérica, el costo por año que generó el centro de datos, incrementó en un 57%. Por otro lado, sólo el 57% de las empresas en Latinoamérica consideran que reducir el consumo de energía es muy importante, como se puede ver en la **Figura 15**.

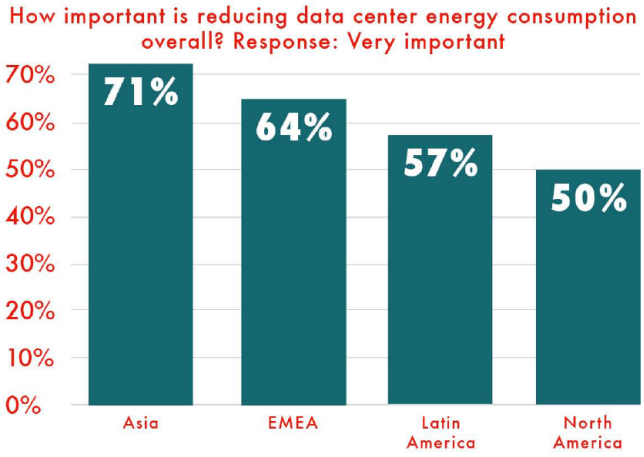


Figura 15. Importancia del consumo de energía por región[22]

En cuanto al nivel de temperatura, en la **Figura 16**, se muestra el promedio de temperatura de estos 1000 centros de cómputo. Estos rangos mencionados, cumplen

[21] (Stansberry, 2013, pág. 12)
[22] (Stansberry, 2013, pág. 15)

con los límites de temperatura establecidos en el 2011, por comité técnico 9.9 de ASHRAE.

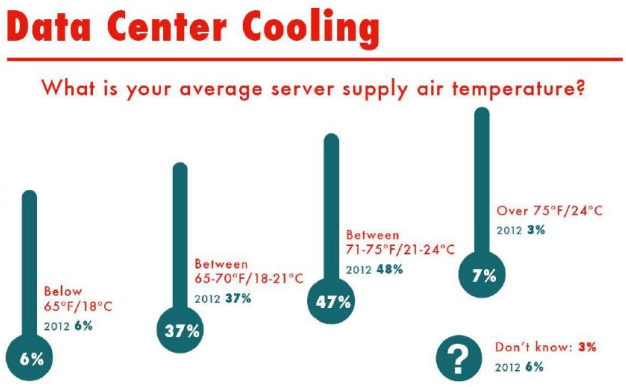


Figura 16. Promedio de temperatura en los centros de cómputo[23]

Por último, la implementación del servicio de cloud tanto público como privado en estas empresas se presenta en la **Figura 17**.

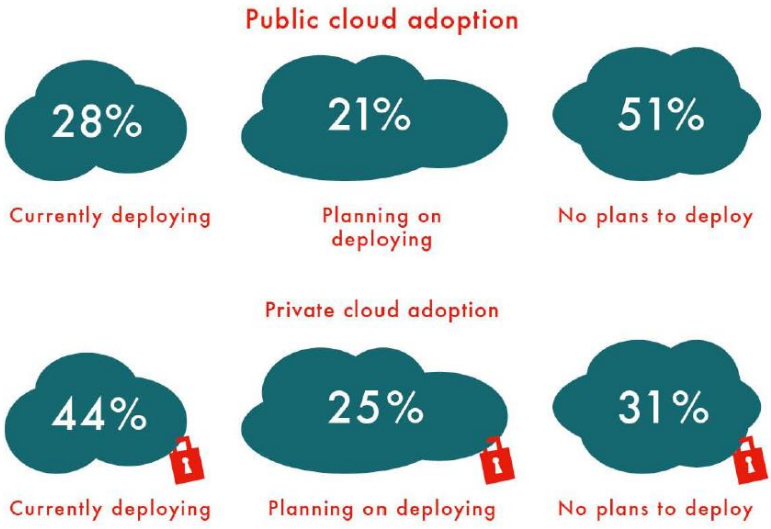


Figura 17. Adopción de cloud computing[24]

[23] (Stansberry, 2013, pág. 18)
[24] (Stansberry, 2013, pág. 23)

3. Conclusiones

A la hora de crear o modificar un centro de cómputo, es necesario realizar una investigación previa, pues a partir de esta información obtenida, se desarrolla el plan de trabajo y se tienen en cuenta las variables que pueden afectar durante este proceso. Para la ejecución de este proyecto, es necesario contar con un líder de equipo que va a ser el responsable de organizar adecuadamente las tareas a llevar a cabo y el que va a poner un tiempo límite de entrega en cada uno de los aspectos. Para esto, es necesario no sólo contar con un apoyo de un especialista de centros de datos, sino también, tener en cuenta casos similares en otras empresas para así evitar los errores a futuro.

Se debe tener en cuenta que el centro de datos, es el lugar en donde se controla y procesa toda la información de una compañía y por eso mismo es de gran importancia. Cada día, se genera más información que necesita ser procesada y almacenada adecuadamente evitando riesgos para la compañía y que esta información sea modificada o llegue a manos de la persona no correspondida. Con esta visión, los centros de datos cada vez toman más relevancia para las organizaciones.

El tipo de infraestructura y normas aplicables a un centro de datos están descritas en múltiples documentos, de los cuales se puede extraer la mejor información y aplicarlos a este espacio, sin embargo, es necesario que a partir de estos estándares, se realice un análisis más puntual teniendo en cuenta las necesidades de la empresa, la capacidad económica de la misma y las características con las que se espera cumplir. Para esto, es recomendable contar con un documento de buenas prácticas donde se pueda llevar un control del cambio continuo de este centro.

Es de gran importancia analizar la forma de implementar la virtualización, pues como puede traer muchas ventajas, una mala implementación puede afectar más que beneficiar el centro de datos y la disponibilidad de los equipos. A la hora de optimizar los recursos con los que se cuenta en el centro de cómputo, se deben tener en cuenta las recomendaciones implementadas en centros de cómputo existentes. Adicionalmente, se deben analizar y aplicar los cambios que vayan de acuerdo a las tendencias de eficiencia energética y mejoras tecnológicas.

El análisis realizado al centro de datos de la empresa Pragcon, genera un valor agregado para la compañía. El objetivo inicial de realizar las adecuaciones principales se cumplió. Ahora se están respetando y siguiendo las políticas para el manejo de equipos y del espacio. Es importante de ahora en adelante llevar un control y un seguimiento del espacio del para que sólo las personas que deban tener el acceso sean las encargadas del manejo de estos temas. Por otro lado, es importante llevar un seguimiento mensual del estado del centro de cómputo para no caer en el incumplimiento de las buenas prácticas y normas de un centro de cómputo. Para esto se recomienda llevar una lista de chequeo con las normas básicas para así realizar mejoras continuas y cambios necesarios en su debido momento.

Teniendo en cuenta las modificaciones implementadas en el centro de cómputo, realizar un centro de cómputo más pequeño, se enfoca hacia el objetivo de optimizar los equipos y de virtualizar de aplicaciones; reduciendo así la cantidad de equipos físicos y aumentando la capacidad de los equipos con los que se cuenta.

El proyecto de adecuaciones del centro de cómputo se logró satisfactoriamente, cumpliendo los objetivos y afectando a la menor cantidad de usuarios. Este cambio es de gran importancia pues se realiza una revisión del centro de cómputo, se hacen ciertas mejoras que no se ejecutaban desde hace un tiempo y se propone implementar una rutina para que esta revisión se esté realizando periódicamente.

Al contar un centro de datos que cumpla con los requerimientos mínimos planteados en las diferentes normas, existen grandes ventajas para la compañía. Entre ellas, un control sobre lo que se tiene y sobre las posibles oportunidades de mejora. Adicionalmente, permite una mejor operación en el día a día, garantizando una continuidad en los servicios prestados a la compañía.

4. Recomendaciones

4.1. Plan de continuidad

Dentro de las buenas prácticas a tener en cuenta en una empresa es implementar un plan de continuidad. Esto con el fin de levantar estos servicios en un sitio alterno en caso que los sistemas informáticos fallen. Esta implementación no se toma en cuenta en empresas pequeñas y medianas, pero es una recomendación a implementar y con la cual se estaría cubriendo la norma ISO 20071 A.14. En esta norma se define un plan de continuidad protegiendo los procesos críticos de las fallas de los sistemas de información de la empresa y de los desastres.

4.2. Auditorías

Adicionalmente, se recomienda establecer un proceso de auditorías periódicas en donde se realice un seguimiento de los equipos y su estado actual. Esto es de gran importancia pues se está analizando el riesgo operacional de la empresa y la disponibilidad con la que cuentan los equipos informáticos. A partir de este seguimiento, se estima la eficiencia actual de los equipos y si estos necesitan ser reemplazados para que la calidad de la red y la disponibilidad de la misma permanezcan y de ser posible mejoren.

4.3. Mantenimiento preventivo y correctivo

Dentro de una empresa, es recomendable contar con un mantenimiento preventivo y correctivo, no sólo para el centro de datos, sino para todos los aspectos en general. Para el centro de datos es de gran importancia pues siempre se va a llevar un control de todos los equipos y un registro para saber cuándo necesitan ser cambiados o actualizados antes que fallen. Para esto, es de vital importancia, contar con unos acuerdos de servicio que garanticen el funcionamiento de los equipos. Este proceso, se debe realizar con los proveedores externos por medio de contratos en donde se especifique un soporte continuo y un mantenimiento en caso de falla. Además, en este proceso, se deben tener en cuenta las actualizaciones necesarias para los equipos y la forma de implementarlas en cada uno de ellos.

4.4. Políticas

Dentro de la planeación de un centro de datos, siempre se debe contar con unas políticas. Entre estas, las más relevantes son el control de acceso, asegurando que las personas que puedan acceder y conceder estos permisos, estén al tanto del funcionamiento general de la sala y sepan los riesgos que se tienen permitiendo el acceso a personal no autorizado. Adicionalmente, se debe establecer una política de cambio de equipos que va a depender del equipo que se tenga y de las revisiones periódicas que se le realicen. Para esto, el administrador del centro de cómputo, debe estar al tanto de cada uno de los equipos y de su funcionamiento.

Por otro lado, se debe establecer una política de limpieza del centro de datos, con la cual, se asegura que este espacio está siendo implementado para el almacenamiento de equipos activos. Además, se asegura que los equipos están organizados y que están ubicados en la posición establecida. Igualmente, se debe realizar una limpieza semanal en donde el personal de aseo es acompañado al centro de datos, evitando así que por falta de conocimiento, se genere una falla. Por último, se debe establecer una política de mantenimiento de los equipos permitiendo que estos siempre estén operando de la mejor manera posible y asegurando que la capacidad del centro de datos se va a mantener a lo largo del tiempo.

4.5 Plan de mejoras faltantes

De acuerdo a los cambios realizados en el centro de datos, se sugiere que para poder tener un mejor espacio, un mejor desempeño y capacidad de los equipos es necesario tener en cuenta algunas mejoras faltantes. En cuanto al cableado con el que se cuenta, se recomienda cambiar los cables de red a categoría 6, con esto mejoraría el desempeño de la red. Adicionalmente, se recomienda implementar servidores virtuales con el fin de permitir un mejor manejo de los servidores y en caso de una falla, poder levantar los servicios en mejor tiempo y reducir el tiempo de indisponibilidad del sistema. Por otro lado, se recomienda contar con un monitoreo por medio de un software que genere alertas automáticas antes que se presente el

error. Este monitoreo permitiría contar con un sistema centralizado que controle diferentes aspectos dentro del centro de datos como: Humedad, temperatura, luminosidad, entre otros. Por otro lado, en cuanto al sistema de control de acceso puede mejorarme implementando un sistema biométrico, esto con el fin de mejorar la seguridad de acceso al centro de datos. En cuanto al sistema de control de incendios, se recomienda cambiar de los sensores del sistema de incendios a iónicos, pues estos cuentan con una mejor tecnología y detección al momento de alerta.

Bibliografía

Alarcón, R. (2011). *Data Center Eficiente.* APC Schenider Electric.

Aldama, M. (2012). *Especificaciones más relevantes de las normas para CPD ISO/IEC 24764 y ANSI/TIA-942-A.* Siemon Latinoamérica.

American National Standard. (2011). *ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices.* Florida, USA: BICSI.

Analistas de Gartner. (30 de Noviembre de 2012). Predicts 2013: Data Center Infrastructure.

ANSI/TIA/EIA-569-A. (2006). *Commercial Building Standard for Telecommunication Pathways and Spaces.* Hochiminh: QUANG DUNG TECHNOLOGY.

Asociación de industria de telecomunicaciones. (2014). *About TIA.* Recuperado el Enero de 2014, de TIA Advancing Global Communications: http://www.tiaonline.org/about/

Avelar, V. (2011). *Mitigating Fire Risks in Mission Critical Facilities.* APC Schneider Electric.

Avelar, V. (2013). *Opciones prácticas para implementar equipos IT en sucursales y salas de servidores pequeñas.* APC Schneider Electric.

Bayle, T. (2010). *Estrategia de mantenimiento preventivo para centros de datos.* APC Legendary Reliability.

BICSI. (2011). Data Center Design and Implementation Best Practices. En *ANSI/BICSI 002-2011* (págs. 1-36). Tampa, FL 33637-1000 USA: BICSI.

Bouley, D. (2012). *Cómo los sistemas de supervisión reducen los errores humanos en las salas de servidores distribuidas y los armarios de cableado remotos.* APC Schneider Electric.

Cisco. (2012). Visión común para infraestructura. *Liberando Potencial IT*.

Cisco. (Julio de 2013). La tecnología como agente de cambio cultural y promotora de la eficiencia. *Liberando el potencial de TI*.

Cisco. (Septiembre de 2013). Proyecciones de crecimiento del tráfico en la nube y del centro de datos. *Liberando el potencial de TI*.

Cisco. (Septiembre| de 2013). Proyecciones de crecimiento del tráfico en la nube y del centro de datos. *Liberando el potencial de TI*.

Cisco Systems e Intel. (Octubre de 2012). Visión común para infraestructura. *Liberando el potencial de TI*, pág. 4.

Codensa. (2006). *Manual de seguridad eléctrica.* Bogotá: Codensa.

DC Consultores. (2010). *Normas, estándares y auditoría en un datacenter.*

Diageo. (s.f.). *Sobre Nosotros*. Recuperado el 25 de 09 de 2013, de Diageo: http://www.diageo.com/es-es/ourbusiness/aboutus/Pages/default.aspx

Donovan, P. (2012). *Data Center Projects: Advantages of Using a Reference Design.* APC Scheneider Electric.

Fernández, J. G. (2009). Data Centers: tendencias y seguridad. *Seguridad Pública* , 86-88.

Gartner, Inc. (2013). *Gartner Outlines Eight Critical Forces to Shape Data Center Strategy.* Stamford: Gartner.

Gartner, Inc. (2013). *Top 10 Strategic Technology Trends for 2014.* Gartner.

Gartner, Inc. (2014). *10 cloud computing trends.* Gartner.

Hernandez Brito, C. (2011). *Virtualización como una estrategia para reducir costos de operación en centros de cómputo.* México DF: Instituto Politécnico Internacional.

ISO/IEC. (2002). *International Standard ISO/IEC 11801 Generic cabling for customer premises.* Switzerland.

IT Watch Dogs. (s.f.). *Importance of using humidity monitoring equipment.* Recuperado el 19 de Febrero de 2014, de IT Watch Dogs: http://www.itwatchdogs.com/humidity-monitoring

Laboratorio de comunicaciones 66.79. (2009). *Cableado estructurado.* FIUBA.

Lin, P., Avelar, V., & Niemann, J. (2013). *Implementing Hot and Cold Air Containment in Existing Data Centers.* APC Schneider.

Maguire, V. (2013). *ISO/IEC 11801 Edition 2.2: Information Technology – Generic Cabling For Customer Premises.* Obtenido de Standards Informant: http://blog.siemon.com/standards/isoiec-11801-edition-2-2-information-technology-%e2%80%93-generic-cabling-for-customer-premises

Ministry of Gender Quality. (2006). *ISO 27001 Controls and Objectives.* Ministry of Gender Quality.

Niemann, J., Brown, K., & Avelar, V. (2013). *Impacto de pasillos calientes y fríos en la eficacia y la temperatura del centro de datos.* APC Schneider Electric.

Niles, S. (2006). *Seguridad física en instalaciones de misión crítica.* American Power Conversion - Schneider Electric.

Niles, S., & Donovan, P. (2012). *Virtualización e informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios.* Schneider Electric.

Pacio, G. (7 de Febrero de 2013). *Protección y administración de datos en la empresa.* Recuperado el 9 de Febrero de 2014, de Data Centers Hoy: http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html

Rasmussen, N. (2010). *Proyectos de centros de datos: La planeación del sistema.* APC.

Rasmussen, N. (2012). *Administración de capacidad de energía y refrigeración para centros de datos.* APC Schneider Electric.

Rasmussen, N. (2012). *Implementación de centros de datos con eficiencia energética.* Schneider Electric.

San Martín García, J. M. (Enero - Febero de 2004). La Seguridad de la Información. Norma UNE de Seguridad de la Información. *La Seguridad de la Información. Nueva ventaja competitiva en la empresa (I/IV).*

Sánchez, R. (2014). *2014 Tendencias en Recintos de Mison Critica.* México: Datacenter Dynamics.

SANS Institute. (2001). *Data Center Physical Security Checklist.* Sean Heare.

Schneider Electric Colombia. (2013). Aumente hoy la eficiencia, la flexibilidad y la vida útil de su centro de datos. *Uptime ¡No pierda tiempo!*, pág. 6.

Stansberry, M. (2013). *Data Center Industry Survey 2013.* UpTime Institute.

TE Connectivity. (2012). *Data Centre Applications Reference Guide Networking & Storage.* Tyco Electronics Corporation.

Tecnológico Dominicano. (Octubre de 2011). Evolución en el monitoreo de centros de datos.

Telecommunications Industry Association. (2005). *Telecommunications Infrastructure Standard for Data Centers.* Arlington, VA: TELECOMMUNICATIONS INDUSTRY ASSOCIATION.

Toledo, V. (2014). *El futuro es de la cloud híbrida, según Nutanix.* Datacenter Dynamics .

Toledo, V. (2014). *IBM prioriza el análisis de grandes volúmenes de datos.* Datacenter Dynamics.

Torell, W. (2011). *Data Center Physical Infrastructure: Optimizing Business Value.* APC Schneider Electric - Data Center Science Center.

Universidad Nacional . (s.f.). *Normas ISO/IEC 11801 y Estandar EIA/TIA568.* México: UDG.

UpTime Institute . (2010). *Data Center site infrastructure Tier Standard: Operational Sustainability.* New York: UpTime Institute, LLC.

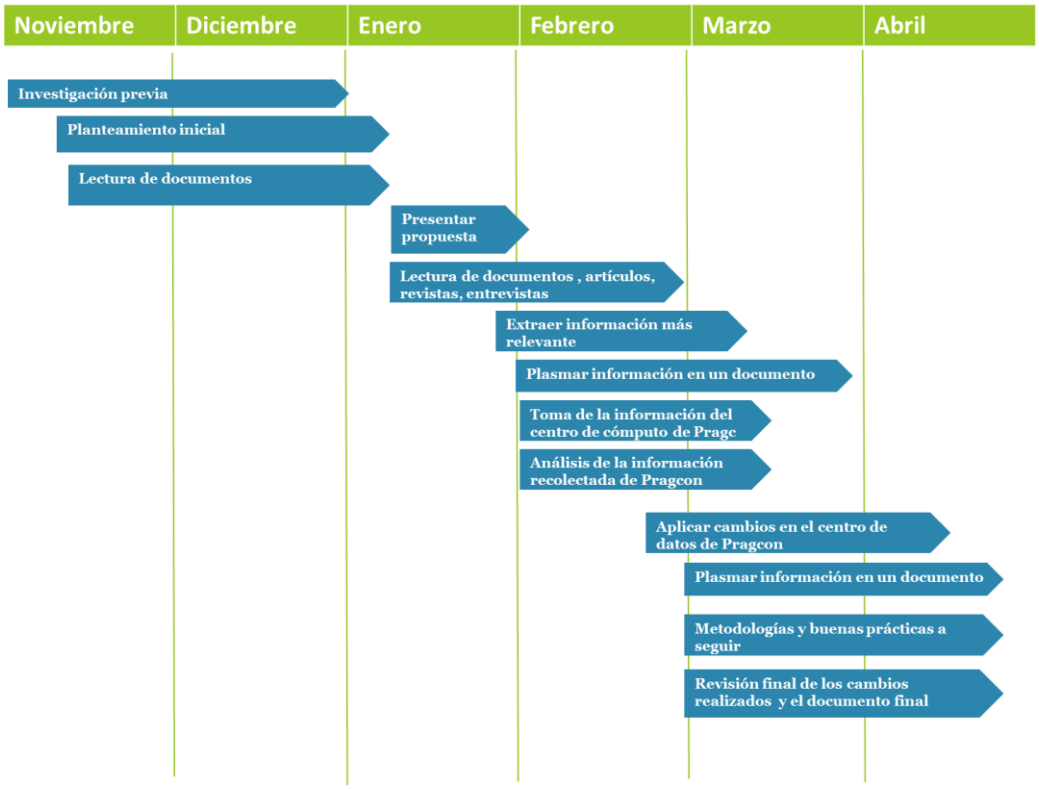
Uptime Institute . (2014). *About Uptime Institute* . Recuperado el 9 de Enero de 2014, de UpTime: http://uptimeinstitute.com/about-us

Villarrubia, C. (2014). *La chilena Mas Errázuriz optimiza su infraestructura TI con Level 3.* Datacenter Dynamics.

Villarrubia, C. (2014). *Toshiba y NTT firman una alianza cloud global.* Datacenter Dynamics.

Anexos

Anexo 1. Cronograma de actividades realizadas en Pragcon



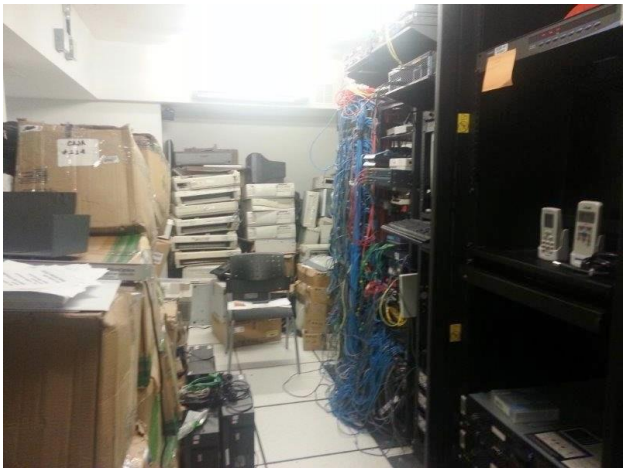
Mes 1 / Mes 2	ANÁLISIS PREVIO
1 semana	Plantear la necesidad de cambio
2 semanas	Análisis del cambio a realizar
1 semana	Aprobación del cambio a realizar y definición del proyecto
Mes 2	**PLANEACIÓN Y DISEÑO DEL PROYECTO**
3 semanas	Listado de activos que están de baja en el sistema
2 semanas	Verificar activos a retirar
1 semana	Realizar cotización inicial para los cambios requeridos
2 semanas	Limpieza inicial del centro de cómputo
2 semanas	Realizar planos con el diseño a implementar en el centro de cómputo
Mes 3	**CONSTRUCCIÓN DEL PROYECTO**
1 semana	Realizar cotización para cambio de aires acondicionados
2 días	Retirar del centro de cómputo los activos a dar de baja y desechar las cajas
1 día	Remover planta de teléfonos del centro de cómputo
1 día	Inspección de piso falso

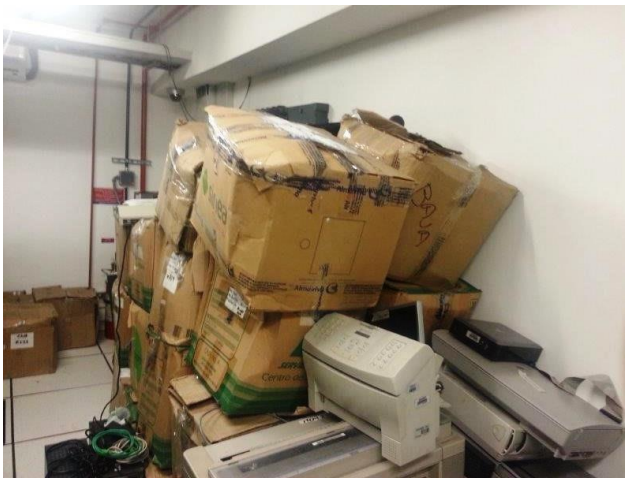
1 día	Enviar la orden de compra de aires acondicionados para aprobación
1 semana	Instalación de aires acondicionados
1 semana	Balanceo de carga eléctrica e instalación de nuevos circuitos
3 semanas	Organización y redistribución de racks de comunicaciones y organización del cableado
1 semana	Marcación de los switches y routers
1 semana	Realizar cotización para la nueva ubicación de la tubería de extintores
3 días	Mantenimiento del piso falso
2 semanas	Estabilización de servicios después del movimiento de los racks
Mes 4	**CAMBIOS FINALES Y REVISIÓN**
2 semanas	Instalación del sistema de extinción y reubicación de la tubería
1 semana	Realizar división de vidrio
3 días	Instalar dry wall y división de vidrio
1 día	Pintura y detalles finales del centro de cómputo
1 día	Revisión final

Anexo 2. Imágenes centro de cómputo de Pragcon antes del análisis

2.A Almacenamiento de equipos no activos dentro del centro de datos

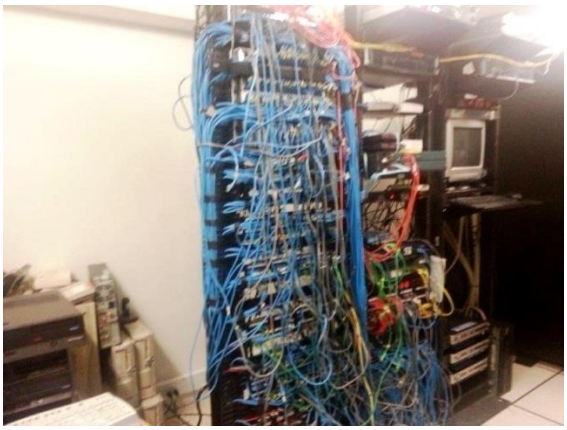
Se incumple con la norma ANSI/BICSI-002 que especifica las mejores prácticas y diseño en un centro de cómputo.





2. B Cableado

Se incumple con la norma ISO-IEC 24764 en donde se especifican las características mínimas con las que debe contar el cableado y la estructura con la que se debe contar

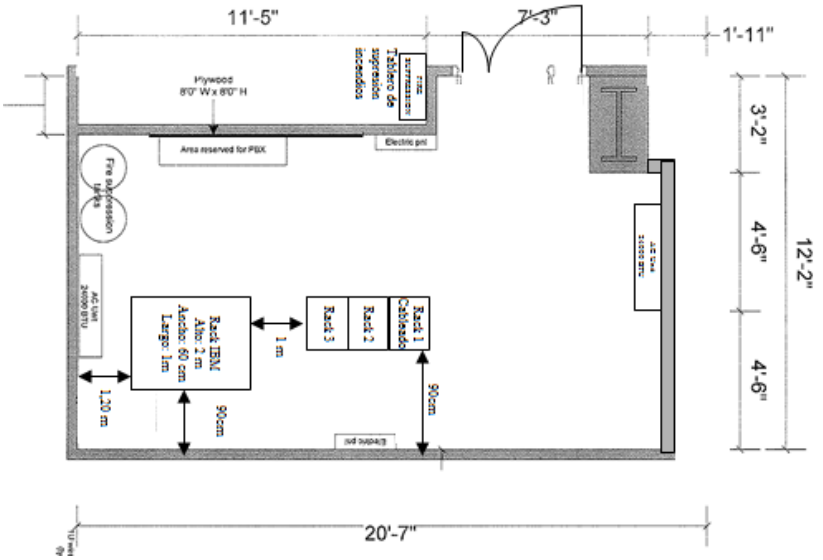


2.C Sistema de extinción de incendios

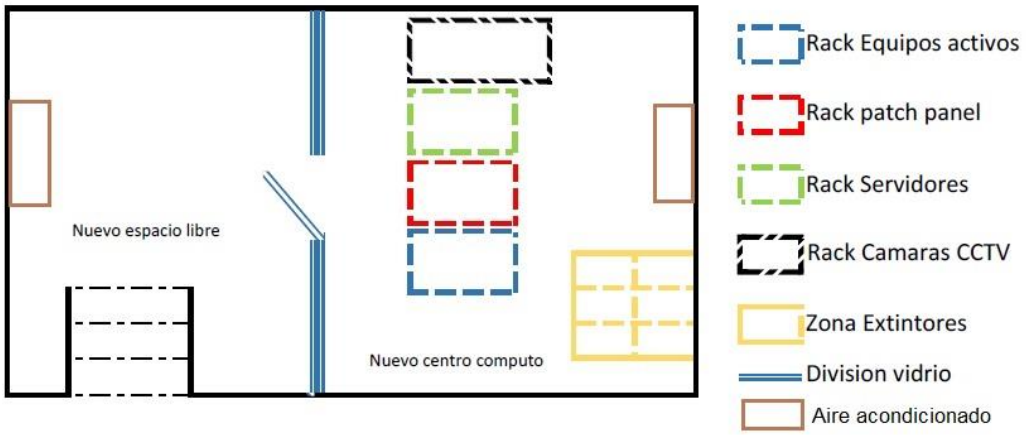
Se incumple con la norma NFPA 75, no se cuenta con un acceso adecuado sistema de extinción de incendios pues está rodeado de cajas y equipos no activos.

2.D. Marcación de cables

Anexo 3. Diseño centro de cómputo de Pragcon



Anexo 4. Nuevo diseño del centro de cómputo



Anexo 5. Centro de cómputo de Pragcon después del análisis

Anexo 6. Guía de chequeo

2. A Seguridad física externa

Característica	Si	No
¿Se cuenta con un sistema cerrado de cámaras?	☐	☐
¿Se cuenta con vigilancia las 24 horas del día?	☐	☐
¿Se cuenta con un sistema de seguridad que impida el acceso a áreas restringidas?	☐	☐
¿Se cuenta con un sistema de seguridad para evitar que se retiren equipos de la empresa sin autorización previa?	☐	☐

2.B Infraestructura del centro de cómputo

Característica	Si	No
¿Se cuenta con un espacio físico especializado para el almacenamiento de equipos informáticos activos?	☐	☐
¿Se cuenta con un sistema de control de incendios?	☐	☐
¿Se realiza un mantenimiento preventivo periódico al sistema de control de incendios?	☐	☐
¿Los detectores del sistema de control de incendios se encuentran en óptimas condiciones?	☐	☐
¿Existe un soporte de garantía para el sistema de control de incendios?	☐	☐
¿Se cuenta con un sistema de refrigeración?	☐	☐
¿Se realiza un mantenimiento preventivo mensual al sistema de aires acondicionados?	☐	☐
¿La temperatura del centro de datos se encuentra dentro del rango permisible (18°C – 27°C)?	☐	☐
¿Existe un soporte de garantía del sistema de refrigeración?	☐	☐

¿Se tiene una iluminación adecuada en el centro de cómputo?	☐	☐
¿Se cuenta con señalización para las salidas de emergencia?	☐	☐
¿Se cuenta con una UPS?	☐	☐
¿Se realiza un mantenimiento preventivo a la UPS?	☐	☐
¿Existe un soporte de garantía de la UPS?	☐	☐
¿El edificio cuenta con una planta eléctrica?	☐	☐
¿Se realiza un mantenimiento preventivo a la planta eléctrica?	☐	☐
¿Existe un soporte de garantía de la planta eléctrica?	☐	☐

2.C Seguridad de control de acceso

Característica	Si	No
¿Se cuenta con un sistema de control de acceso al edificio?	☐	☐
¿Se cuenta con una bitácora de ingreso?	☐	☐
¿Se cuenta con un sistema de control de acceso al centro de cómputo?	☐	☐
¿El acceso al centro de cómputo se realiza por medio de un dispositivo físico (Ej.: Llave, tarjeta)?	☐	☐
¿El acceso al centro de cómputo se realiza ingresando una contraseña?	☐	☐
¿Se cuenta con un sistema biométrico de control de acceso (Reconocimiento por medio de rasgos físicos)?	☐	☐
¿Se realiza una actualización periódica de las personas que pueden ingresar al centro de datos?	☐	☐
¿Se cuenta con políticas de ingreso?	☐	☐

2.D Control de los equipos

Característica	Si	No
¿Se cuenta con un inventario de los equipos activos?	☐	☐
¿Se realiza una revisión periódica para estos equipos?	☐	☐
¿Se tiene un control de los cambios realizados a los equipos?	☐	☐
¿Se tiene un control de la garantía de los equipos?	☐	☐
¿Se cuenta con un servicio de mantenimiento de los equipos?	☐	☐
¿Se cuenta con un sistema de notificación de fallas por medio de envío de alertas (Correo electrónico, vía telefónica)?	☐	☐

2.E Organización del centro de datos

Característica	Si	No
¿Se realiza una limpieza periódica?	☐	☐
¿Esta limpieza es acompañada por alguien que conoce el procedimiento para evitar errores humanos?	☐	☐
¿Se realiza un seguimiento periódico al uso que se le está dando al centro de	☐	☐

cómputo y que este espacio no esté almacenando equipos o materiales diferentes a los activos?		

2.F Plan de acción

Característica	Si	No
¿Se cuenta con un sistema de contingencia en caso que fallen los equipos?	☐	☐
¿Se tiene un plan de mejora continua?	☐	☐
¿Se realiza un plan previo para los cambios programados?	☐	☐

2.G Alertas por falla

Característica	Si	No
¿Se cuenta con un monitoreo las 24 horas para los sistemas del centro de datos?	☐	☐
¿Se cuenta con un sistema que alerte las fallas de los equipos de red?	☐	☐
¿Se tiene un sistema de notificación para el sistema de control de incendios?	☐	☐
¿Se tiene un sistema de notificación para el sistema de refrigeración?	☐	☐

Anexo 7. Base documental

1. Villarrubia, Celia. Toshiba y NTT firman una alianza cloud global. Datacenter Dynamics, 2014.
2. La chilena Mas Errázuriz optimiza su infraestructura TI con Level 3. Datacenter Dynamics, 2014.
3. Toledo, Virginia. IBM prioriza el análisis de grandes volúmenes de datos. Datacenter Dynamics, 2014.
4. El futuro es de la cloud híbrida, según Nutanix. Datacenter Dynamics , 2014.
5. Uptime Institute . About Uptime Institute . UpTime. [En línea] 2014. [Citado el: 9 de Enero de 2014.] http://uptimeinstitute.com/about-us.
6. Asociación de industria de telecomunicaciones. About TIA. TIA Advancing Global Communications. [En línea] 2014. http://www.tiaonline.org/about/.
7. Sánchez, Roberto. 2014 Tendencias en Recintos de Mison Crítica. México : Datacenter Dynamics, 2014.
8. Gartner, Inc. 10 cloud computing trends. Gartner, 2014.
9. Top 10 Strategic Technology Trends for 2014. Gartner, 2013.
10. Cisco. Proyecciones de crecimiento del tráfico en la nube y del centro de datos. Liberando el potencial de TI. Septiembre de 2013.

11. Pacio, Germán. Protección y administración de datos en la empresa. Data Centers Hoy. [En línea] 7 de Febrero de 2013. [Citado el: 9 de Febrero de 2014.] http://www.datacentershoy.com/2013/02/estandares-en-el-data-center.html.
12. Avelar, Victor. Opciones prácticas para implementar equipos IT en sucursales y salas de servidores pequeñas. APC Schneider Electric, 2013.
13. Cisco. La tecnología como agente de cambio cultural y promotora de la eficiencia. Liberando el potencial de TI. Julio de 2013.
14. International Data Group . Consolidating Remote Servers and Storage for Security, Efficiency. Riverbed, 2013.
15. Maguire, Valerie. ISO/IEC 11801 Edition 2.2: Information Technology – Generic Cabling For Customer Premises. Standards Informant. [En línea] 2013. http://blog.siemon.com/standards/isoiec-11801-edition-2-2-information-technology-%e2%80%93-generic-cabling-for-customer-premises.
16. Lin, Paul, Avelar, Victor y Niemann, John. Implementing Hot and Cold Air Containment in Existing Data Centers. APC Schneider, 2013.
17. Start with the end in mind. UpTime Institute, 2013.
18. Niemann, John, Brown, Kevin y Avelar, Victor. Impacto de pasillos calientes y fríos en la eficacia y la temperatura del centro de datos. APC Schneider Electric, 2013.
19. Gartner, Inc. Gartner Outlines Eight Critical Forces to Shape Data Center Strategy. Stamford : Gartner, 2013.
20. Stansberry, Matt. Data Center Industry Survey 2013. UpTime Institute, 2013.
21. Panduit. Transforme su Centro de Datos, de básico a estratégico. Panduit, 2013.
22. Prime Energy IT. Infraestructura y hardware informático energéticamente eficiente. Prime Energy IT, 2013.
23. Schneider Electric Colombia. Aumente hoy la eficiencia, la flexibilidad y la vida útil de su centro de datos. Uptime ¡No pierda tiempo! 2013, pág. 6.
24. Cisco Systems e Intel. Visión común para infraestructura. Liberando el potencial de TI. Octubre de 2012, pág. 4.
25. Cisco. Visión común para infraestructura. Liberando Potencial IT. 2012.
26. Niles, Suzanne y Donovan, Patrick. Virtualización e informática en la nube: la optimización de potencia, enfriamiento y de la administración maximizan los beneficios. Schneider Electric, 2012.

27. Analistas de Gartner. Predicts 2013: Data Center Infrastructure. 30 de Noviembre de 2012.
28. Rasmussen, Neil. Implementación de centros de datos con eficiencia energética. Schneider Electric, 2012.
29. UpTime Institute. Data Center Site Infraestructure Tier Standard: Topology. UpTime Institute, 2013.
30. Aldama, Miguel. Especificaciones más relevantes de las normas para CPD ISO/IEC 24764 y ANSI/TIA-942-A. Siemon Latinoamérica, 2012.
31. TE Connectivity. Data Centre Applications Reference Guide Networking & Storage. Tyco Electronics Corporation, 2012.
32. Donovan, Patrick. Data Center Projects: Advantages of Using a Reference Design. APC Scheneider Electric, 2012.
33. Avelar, Victor. Practical Options for Deploying IT Equipment in Small Server Rooms and Branch Offices. Schneider Electric, 2012.
34. Bouley, Dennis. Cómo los sistemas de supervisión reducen los errores humanos en las salas de servidores distribuidas y los armarios de cableado remotos. APC Schneider Electric, 2012.
35. Rasmussen, Neil. Administración de capacidad de energía y refrigeración para centros de datos. APC Schneider Electric, 2012.
36. Niles, Suzanne and Donovan, Patrick. Virtualization and Cloud Computing: Optimized Power, Cooling, and Management Maximizes Benefits. Schneider Electric, 2012.
37. Brown, Kevin and Bouley, Dennis. Classification of Data Center Infrastructure Management (DCIM) Tools. Schneider Electric, 2012.
38. Hernandez Brito, César. Virtualización como una estrategia para reducir costos de operación en centros de cómputo. México DF : Instituto Politécnico Internacional, 2011.
39. Avelar, Victor. Mitigating Fire Risks in Mission Critical Facilities. APC Schneider Electric, 2011.
40. Tecnológico Dominicano. Evolución en el monitoreo de centros de datos. Octubre de 2011.
41. Torell, Wendy. Data Center Physical Infrastructure: Optimizing Business Value. APC Schneider Electric - Data Center Science Center, 2011.

42. Alarcón, Rafael. Data Center Eficiente. APC Schenider Electric, 2011. pág. 16.
43. BICSI. Data Center Design and Implementation Best Practices. ANSI/BICSI 002-2011. Tampa, FL 33637-1000 USA : BICSI, 2011, págs. 1-36.
44. American National Standard. ANSI/BICSI 002-2011 Data Center Design and Implementation Best Practices. Florida, USA : BICSI, 2011.
45. UpTime Institute. THE TIER CLASSIFICATION SYSTEM. UpTime Institute, 2011.
46. Bouley, Dennis. Creating Order from Chaos in Data Centers and Server Rooms. Schneider Electric, 2011.
47. IT Watch Dogs. How to Protect Your Data Center from Environmental Threats. IT Watch Dogs, 2011.
48. Bouley, Dennis. How Monitoring Systems Reduce Human Error in Distributed Server Rooms and Remote Wiring Closets. Scheneider Electric, 2011.
49. Cowan, Christian and Gaskins, Chris. Monitorin g Physical Threats in the Data Center. Schneider Electric, 2011.
50. Rasmussen, Neil. Proyectos de centros de datos: La planeación del sistema. APC, 2010.
51. DC Consultores. Normas, estándares y auditoría en un datacenter. 2010.
52. Bayle, Thierry. Estrategia de mantenimiento preventivo para centros de datos. APC Legendary Reliability, 2010.
53. UpTime Institute . Data Center site infrastructure Tier Standard: Operational Sustainability. New York : UpTime Institute, LLC, 2010.
54. Banks, Stephen. BICSI Data Center Standard. Bicsi, 2010.
55. Technologies, Lee. The Top 9 Mistakes in Data Center Planning. Lee Technologies, 2010.
56. Data Centers: tendencias y seguridad. Fernández, Jonathan González. 2009, Seguridad Pública, págs. 86-88.
57. Laboratorio de comunicaciones 66.79. Cableado estructurado. FIUBA, 2009.
58. Niles, Suzanne. Seguridad física en instalaciones de misión crítica. American Power Conversion - Schneider Electric, 2006.
59. ADC. Cómo diseñar un centro de datos óptimo. ADC, 2006.
60. Niles, Suzanne. Seguridad física en instalaciones de misión crítica. APC, 2006.
61. Codensa. Manual de seguridad eléctrica. Bogotá : Codensa, 2006.

62. Ministry of Gender Quality. ISO 27001 Controls and Objectives. Ministry of Gender Quality, 2006.
63. ANSI/TIA/EIA-569-A. Commercial Building Standard for Telecommunication Pathways and Spaces. Hochiminh : QUANG DUNG TECHNOLOGY, 2006.
64. Telecommunications Industry Association. Telecommunications Infrastructure Standard for Data Centers. Arlington, VA : TELECOMMUNICATIONS INDUSTRY ASSOCIATION, 2005.
65. San Martín García, José Miguel. La Seguridad de la Información. Norma UNE de Seguridad de la Información. La Seguridad de la Información. Nueva ventaja competitiva en la empresa (I/IV). Enero - Febrero de 2004.
66. ISO/IEC. International Standard ISO/IEC 11801 Generic cabling for customer premises. Switzerland , 2002.
67. SANS Institute. Data Center Physical Security Checklist. Sean Heare, 2001.
68. Departamento de control de calidad y auditoría informática. Guía para pruebas en áreas de centros de cómputo. Departamento de control de calidad y auditoría informática, 2000.

Anexo 8. Autorización acceso al centro de cómputo

INFORMATION SYSTEMS

Bogotá, 08 de Enero 2014

Autorización para ingreso temporal a Centro de Cómputo **dirección oficinas**.

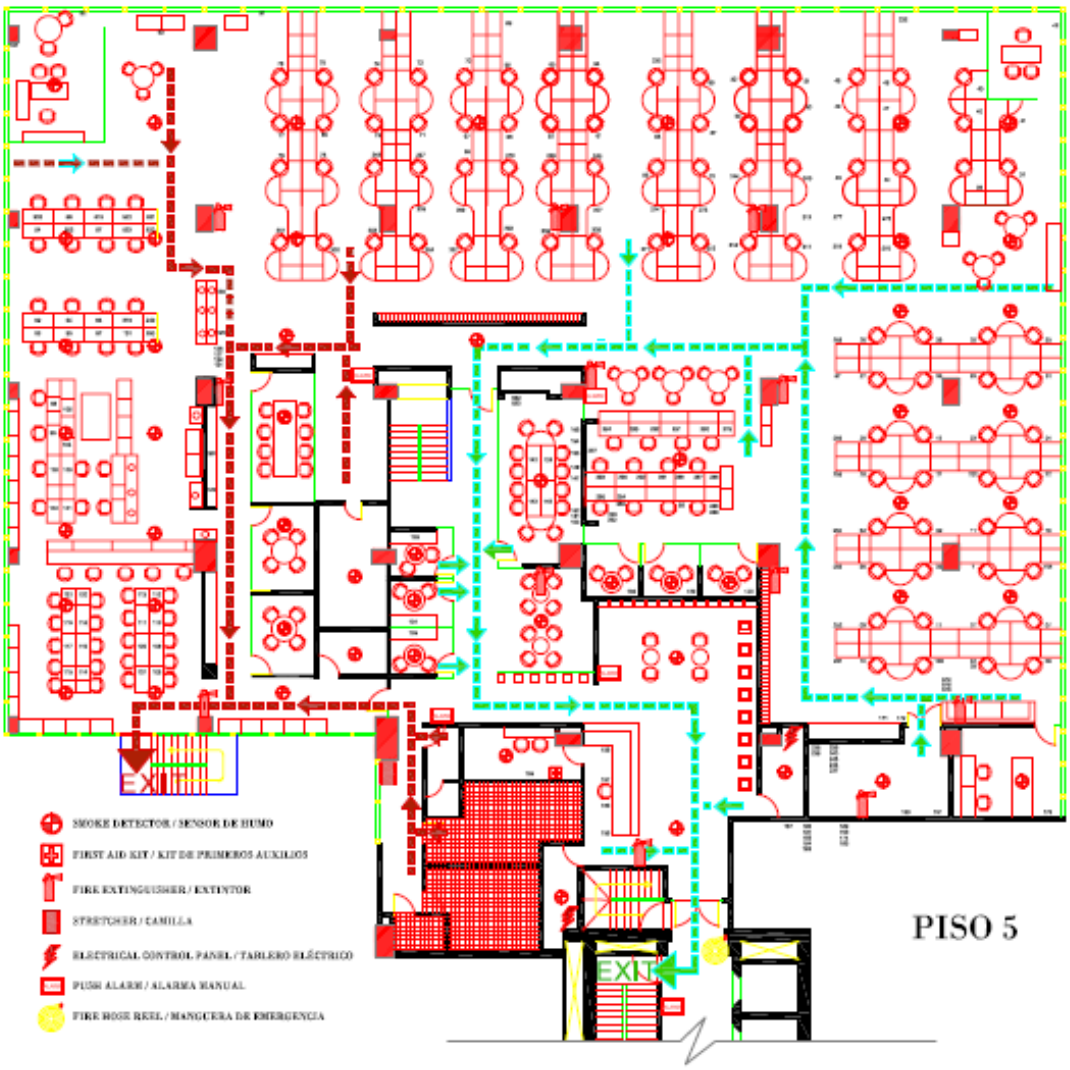
Nombre Apellido es autorizado para tener el acceso temporal a las instalaciones del Centro de cómputo de la **dirección oficinas** para **razón de la visita**.

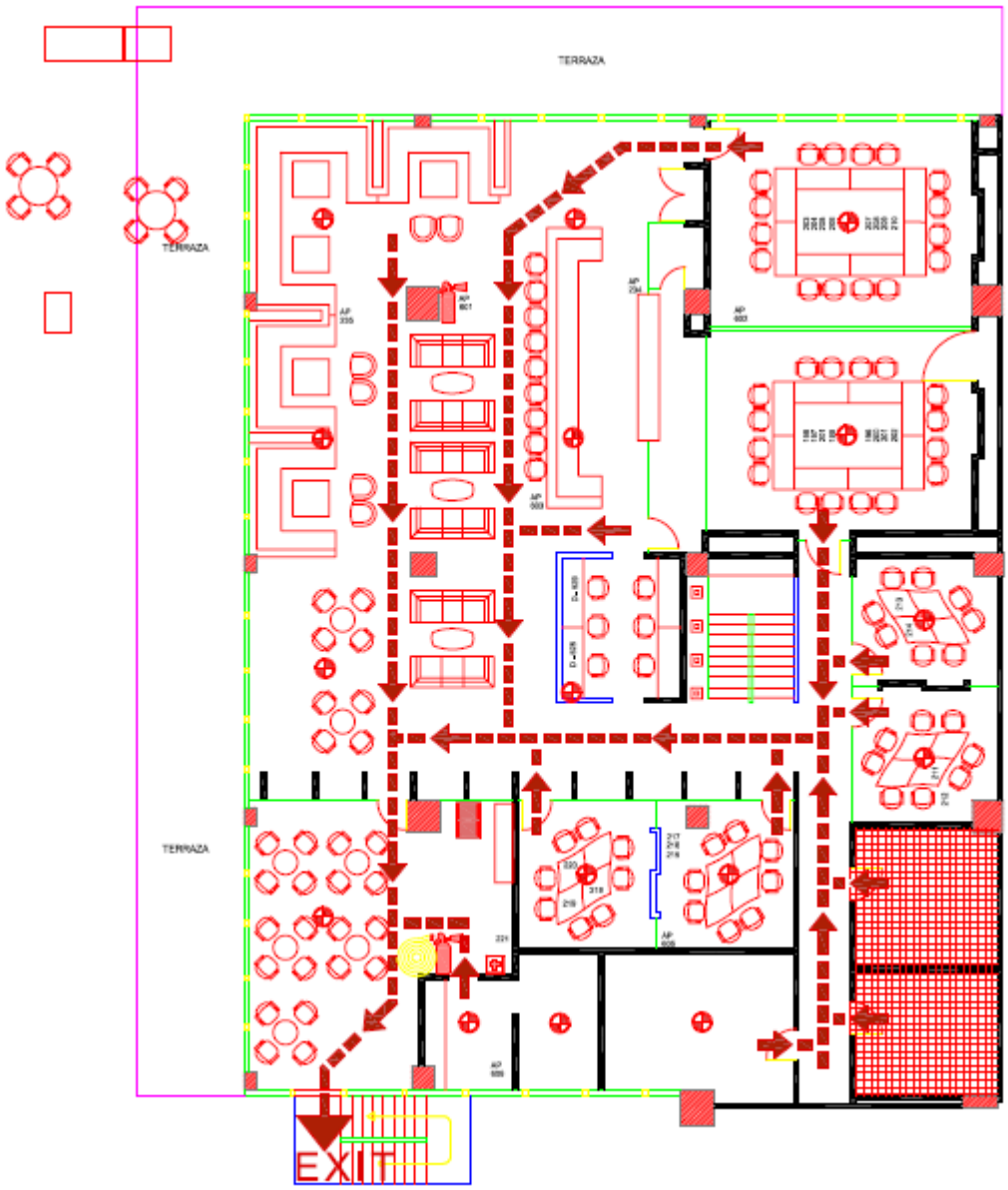
Valida por el día 08 de Enero 2014

_____
Nombre de analista
Analista de sistemas. Aprueba

_____
Nombre Autorizado –Compañía
C.C. **Número Cédula**

Anexo 9. Planos de la empresa





PISO 6