Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencias de la Administración

Decadencia del centro de datos por las nuevas tecnologías

T e s i s

Que para optar por el grado de:

Maestro en Informática Administrativa

Presenta:
Iván Martínez Rico

Tutor:
M.A. René Montesano Brand
Facultad de Contaduría y Administración

Ciudad de México, enero de 2020

INDICE

Dedicatorias.

A mis padres: quienes me enseñaron el valor de la constancia, responsabilidad y trabajar arduamente a pesar de todo lo que pueda suceder. Si estoy aquí... ¡Es gracias a ustedes!

A mis hijos: nunca dejen de soñar, recuerden que todo es posible… Si en verdad lo desean y si están dispuestos a trabajar por ello. Pero principalmente… ¡Los Amo!

A Rocio Santana: no existen palabras para poder agradecerte todo lo que has hecho por mí, sin tu apoyo, comprensión y paciencia no lo hubiera logrado.

A Beatriz Solano: solo puedo decirte: "*He buscado a través de lo físico, lo metafísico, lo delirante, … y vuelta a empezar. Y he hecho el descubrimiento más importante de mi carrera, el más importante de mi vida. Sólo en las misteriosas ecuaciones del amor puede encontrarse alguna lógica*" (John Forbes Nash citado por Romero, 2019). ¡Gracias por ser parte importante de mi vida!

Al Ing. Mtro. y Dr. José Bedolla Cordero: es tanto lo que tengo que agradecerte que me faltarían palabras para poder expresarlo adecuadamente. Gracias por enseñarme que la dedicación, la constancia y los deseos de aprender nunca se pierden. En especial por la "*historia de la vaca*", me ha sido de especial utilidad en mi vida profesional y que gracias a ella esta tesis de maestría cobro vida.

Al Ing. Y Mtro. René Montesano Brand, Mi asesor de tesis: gracias por todo el apoyo recibido.

Agradecimientos.

A mis profesores, compañeros y amigos:

Hace varios años, tuve un sueño y un deseo largamente anhelado… ¡Poder terminar mi Maestría!, y no en cualquier universidad, sino nada más y nada menos que en la máxima casa de estudios: La Universidad Nacional Autónoma de México. Mi casa y Alma Mater de la cual aprendí muchas cosas, especialmente a tenerle un profundo cariño y respeto. El día de hoy que concluyo mis estudios de maestría, recuerdo especialmente las palabras de mi padre:

> ***"Nunca digas... ¡No puedo!, la fortaleza viene de lo más profundo del corazón y del alma.... ¡Siempre Intenta, una y otra y otra vez, aprende que la tenacidad, la constancia y el coraje se obtienen levantándose una y otra vez!***
> ***¡Nunca dejes de luchar por aquello que quieres!... Nunca permitas que alguien te diga que no puedes hacer esto o aquello, recuerda que la única persona que más importa en el mundo ¡ERES TÚ!***
> ***Y es únicamente a ti a quien debes de convencer que TODO ES POSIBLE... ¡SI ESTAS DISPUESTO A HACERLO!".***

Motivo por el cual, estoy profundamente agradecido con todos y cada uno de mis profesores, asesores y amigos. Por todo este tiempo que compartimos juntos en Posgrados de la Facultad de Contaduría y Administración, aprendí mucho y reafirmé conocimientos.

Es tanto lo que me gustaría decir, pero me faltan las palabras para poder expresarme adecuadamente, por el cual solo puedo decir…

¡MUCHAS GRACIAS POR TODO!

"Por mi raza hablará el espíritu"

A la Universidad Nacional Autónoma de México (UNAM):

Especialmente al área de Posgrados de la Facultad de Contaduría y Administración a la que le tengo tanto cariño y aprecio, gracias por todo el apoyo recibido durante este período de enseñanza en la Maestría.

"Por mi raza hablará el espíritu"

Al Consejo Nacional de Ciencia y Tecnología (CONACYT):

Gracias por todo el apoyo recibido ya que, sin su valiosa ayuda, no hubiera sido posible realizar mis estudios de Maestría.

¡MUCHAS GRACIAS POR TODO!

Índice de ilustraciones.

Índice de tablas.

Introducción.

> *"La primera regla de cualquier tecnología utilizada en los negocios, es que la automatización aplicada a una operación eficiente magnificará la eficiencia. La segunda, es que la automatización aplicada a una operación ineficiente magnificará la ineficiencia"*. Bill Gates citado por Skaff, (2015)

El propósito de la presente investigación es explorar la hipótesis de la decadencia del centro de datos con más de cinco años de antigüedad y el impacto de las tecnologías emergentes, específicamente el Internet de las Cosas (*IoT,* por sus siglas en inglés *Internet of Things*); al ser implementado bajo tales circunstancias. Bajo el precepto de que las organizaciones están migrando sus centros de datos a la Nube (*Cloud Computing*) para reducir costos administrativos y de operación, sin embargo, es necesario considerar las estadísticas en donde se está observando una disminución de la inversión a nivel mundial de los gastos de las Tecnologías de la Información (*TI*) para los próximos años.

Por el cual es necesario explorar los efectos que se tendría en los centros de datos de las organizaciones la implementación masiva del *IoT*. Adicionalmente la complejidad de los centros de datos de las organizaciones que centran su fortaleza en nuevas formas de administrar sus datos para generar valor, han generado que los departamentos de administración de las *TI* sean más difíciles de administrar con el paso del tiempo.

El presupuesto que destinan las organizaciones a los departamentos de *TI*, no podrán continuar por mucho tiempo el creciente ritmo de la tecnología de los centros de datos debido a su complejidad de administración. Los departamentos de *TI*, requieren de una reducción de las cosas que debe administrar, algunos de estos procesos se pueden realizar mediante la automatización de los mismos, otros en la

Nube y algunos mediante nuevos sistemas con un mayor rendimiento; lo cual permitiría consolidar los antiguos.

Adicionalmente, para las organizaciones es muy importante poder controlar sus costos operativos, sin embargo, en los negocios de la era digital moderna, la velocidad es un factor importante y decisivo. Por lo que la manera en la que una organización juzga las *TI* son: la confiabilidad y la velocidad de implementación de los nuevos servicios.

Antecedentes.

Los centros de datos mejor conocidos como *Datacenter* comienzan a tener un auge en las organizaciones de una manera preponderante a partir de la década de los noventas, cuando las necesidades de una conectividad rápida y continua hacia la red de Internet comienza a crecer a un ritmo acelerado; por lo que los recursos internos de las organizaciones comenzaron a considerar seriamente las nuevas necesidades de mantener un flujo de datos de una manera ininterrumpida como algo primordial.

Sin embargo, el mundo ha cambiado de forma trascendental desde la década de los noventas y la necesidad de responder de manera tecnológica a los nuevos requerimientos; han hecho que los centros de datos no sean lo suficientemente flexibles para reaccionar adecuadamente a las nuevas necesidades de una manera óptima. Por lo que las necesidades de respuesta de los centros de datos se vuelven más intensas y de igual forma, la ventaja competitiva de la tecnología en las organizaciones comienza a desaparecer.

En la gran mayoría de las organizaciones ya sean públicas o privadas, los centros de datos son considerados la parte medular de las mismas y están catalogados como factores de “misión crítica”. Sin embargo, un gran número de estos centros de datos en la actualidad han presentado una gran cantidad de problemas de

rendimiento, por lo que requieren ser modernizados para así mantener su ventaja estratégica al interior de las organizaciones.

A pesar de que todos los centros de datos de las organizaciones suelen ser muy diferentes, comparten ciertas características de modernización que pueden variar basadas en las circunstancias que las mismas organizaciones requieran como son, por ejemplo: costo, flujo de efectivo y factores estratégicos tales como: marco de tiempo de implementación, ambiente regulatorio y cultura empresarial.

Para Martínez H., (2017), se presentan cuatro categorías generales de enfoques a la modernización que son:

- ***Bajo presupuesto*** *– Este enfoque consiste en arreglos rápidos como la consolidación de activos subutilizados, la mejora del flujo de aire y la intensificación de las prácticas de mantenimiento preventivo. El objetivo en estos casos es comprar tiempo cuando hay poca financiación para mejoras disponibles.*
- ***Mejora de los sistemas centrales en el sitio existente*** *– El envejecimiento de los sistemas centrales disminuyen la confiabilidad, aumentan el costo de mantenimiento y disminuyen la eficiencia. Los sistemas de potencia y refrigeración modulares y escalables ahora permiten actualizaciones sencillas a través del suministro de componentes pre moldeados y estancados. Esto acelera el acceso a la nueva capacidad y permite "pagar a medida que crece" la planificación y la inversión.*
- ***Construcción de un nuevo centro de datos*** *– Este enfoque tiene más sentido si la expectativa de vida del nuevo centro de datos supera los cinco años, y permite a las partes interesadas un control completo y directo de su operación.*

- ***La tercerización de centros de colocación o la Nube*** *– Las empresas con una alta aversión a los gastos de capital inicial pueden preferir un modelo de colocación, ya que convierte el centro de datos en más de un gasto operativo, a pesar de que el TCO[1] es más alto a largo plazo.* (Martínez H. , 2017)

En la última década, se han desarrollado diversos documentos y proyectos relacionados a los centros de datos, los cuales pretenden subsanar las necesidades actuales de desempeño, confiabilidad, velocidad y disponibilidad de la información que los Centros de Datos almacenan. Asimismo, existen diversas investigaciones que exponen los métodos y formas de la instalación del centro de datos utilizando un método holístico en su desarrollo las cuales se presentan a continuación:

En su trabajo de grado para ingeniería titulado ***"Diseño de infraestructura de telecomunicaciones para un Centro de datos"*** Castillo Devoto, (2008), nos indica que pretendió realizar un proyecto con las normas internacionales de la *Electronic Industries Alliance* (EIA) y la *Telecommunications Industry Association* (TIA) 568-B[2] de cableado estructurado y la *American National Standards Institute* (ANSI) /TIA/EIA-942[3]

> *Para diseñar un Centro de datos se deben tener en cuenta varios factores más allá del tamaño y la cantidad de equipos de datos que éste debiera albergar. Establecer el lugar físico, acceso a la energía,*

[1] Costo total de propiedad (una estimación de todos los costos directos e indirectos involucrados en la adquisición y operación de un producto o sistema durante su vida útil). Reducir el costo total de propiedad es un incentivo clave para que las empresas muevan las cargas de trabajo existentes dentro de la Nube. (Oxford, 2019)

[2] Véase anexo I – Principales estándares del cableado estructurado sección: Estándar ANSI/TIA/568-C.0.
Cableado genérico de telecomunicaciones para las instalaciones del cliente (*Generic Telecommunications Cabling for Customer Premises*)

[3] Véase anexo I – Principales estándares del cableado estructurado sección: ANSI/TIA 942-A Estándar de Infraestructura de Telecomunicaciones para Centros de *Datos (Telecommunications Infraestructure Standard for* Data **Centers).**

nivel de redundancia, cantidad de refrigeración, rigurosa seguridad y el tipo de cableado son algunos de los factores a considerar (Castillo Devoto, 2008, pág. 1).

Dentro de sus conclusiones, el autor hace mención de que no cumplió en su totalidad con la norma de la EIA/TIA 942 por las características definidas del proyecto y la distribución del edificio en el cual se encontraría instalado el centro de datos, como lo determina en sus conclusiones:

- *Luego de haber revisado diferentes normas necesarias para el diseño de infraestructura de red, se puede concluir que no siempre se cumplirán en su totalidad ya que las características de las instalaciones de un edificio y las exigencias del cliente serán las que definan el diseño real. Lo que se debe procurar es buscar solución que más se acerque a las recomendaciones de las diferentes normas.*
- *La solución que se plantea es independiente de la tecnología y equipos que se usen, prueba de esto es que todo fue diseñado sin referencia alguna de las técnicas que utilizarán los dispositivos mostrados. El diseño sólo se basó en las propiedades de los diferentes medios a utilizar, lo cual asegura que el sistema sea 96 vigente hasta que se llegue a utilizar métodos de transmisión o recepción que superen la capacidad de los medios.*
- *Dado que el diseño se realizó en base solo a los planos tiene un margen de error de aproximadamente 20% en lo que refiere a rutas de cableado, bandejas o cables.* (Castillo Devoto, 2008, págs. 95 - 96).

Es importante hacer notar que existe un gran problema con la subjetividad y la interpretación de las normas del cableado estructurado específicamente la norma

EIA/TIA 942 que es la utilizada para la implementación del Centro de Datos; derivado directamente de las características del edificio en donde el mismo seria implementado.
Lo que representa un potencial factor de riesgo al mediano plazo derivado directamente de una deficiente interpretación e implementación de las normas del cableado estructurado. Y que terminara por afectar la forma en la que se planeó el desempeño estratégico de la tecnología por parte de la organización.

En su trabajo de grado para ingeniería titulado ***"Centro de datos para mejorar la Infraestructura de Comunicación de Datos en el Departamento de Sistemas Informáticos y Redes de Comunicación (DISIR) de la Universidad Técnica de Ambato"*** Córdova Flores, (2012)**,** determina la necesidad de la creación de un centro de datos para centralizar los recursos informáticos con la implementación de un Centro de Datos basado en los estándares internacionales.

> *El diseño de un Data Center en el Departamento de Sistemas Informáticos y Redes de Comunicación (DISIR) de la Universidad Técnica de Ambato pretende disminuir pérdidas de información y el mantenimiento ineficiente de equipos informáticos y de comunicaciones entre los integrantes de la comunidad universitaria, lo cual amerita contar con una estructura tecnológica ubicada en un lugar adecuado que organice, resguarde y administre los procesos internos de la Universidad, puesto que para los miembros de la institución la seguridad, protección de datos, el respaldo y la recuperación, son las iniciativas más importantes y principales actualmente. Tomando en cuenta que en los Data Center se necesita elementos de seguridad que son costosos, es por ello que se requiere la centralización de los equipos y así minimizar el número de elementos de seguridad requeridos. La optimización de energía es un parámetro importante que actualmente no se toma en cuenta y es un*

gasto permanente y puede llegar a ocasionar grandes erogaciones de dinero (Córdova Flores, 2012, págs. 2-3).

Dentro de sus conclusiones el autor nos indica que la selección del lugar en donde fue instalado el centro de datos no es el indicado y por lo mismo la infraestructura necesaria para el mantenimiento del centro de datos será insuficiente al mediano plazo:

- *De acuerdo con los objetivos planteados al inicio de la investigación, se puede concluir, que existen aspectos a mejorar en la infraestructura de comunicaciones de datos en la Universidad Técnica de Ambato, debido a que el backbone[4] no se encuentra en un espacio físico adecuado y basado en estándares internacionales.*
- *Según la encuesta realizada al personal del DISIR y Administradores de red de las diferentes Facultades, se puede indicar que es notoria el gran porcentaje que manifiesta que el área en donde está ubicado los servidores no se encuentran en un lugar con las debidas seguridades contra desastres.*
- *No se cuenta con sistemas de enfriamiento y aire acondicionado adecuados para la refrigeración de los equipos en la sala de servidores. Tampoco se dispone de mecanismos para la seguridad física del área.*
- *En la mayoría de las facultades la sala de servidores no posee infraestructura complementaria como piso falso y peor aún no se toma en cuenta estándares para proteger a los equipos de cómputo de incendios o daños.*
- *La Universidad Técnica de Ambato no cuenta con un Centro de datos en donde la infraestructura de red sea redundante y*

[4] (Núcleo estructural de la red) es el cable que conecta todos los componentes de la red de manera que se pueda producir la comunicación. (Terán, 2014, pág. 453)

> *segura y que permita en un futuro brindar servicio a otras empresas o entidades* (Córdova Flores, 2012, págs. 191 - 192).

Como podemos observar en las conclusiones el centro de datos no fue instalado de manera adecuada; al igual que toda la infraestructura principal de la red de datos, por lo cual basados en la información proporcionada, podemos deducir que el centro de datos tendrá un desempeño deficiente en la transmisión de datos al corto plazo. De igual forma el crecimiento que podría tener en el futuro cercano se ve comprometido al no cumplir con las normas del cableado estructurado.

En su trabajo de grado de Ingeniería titulado ***"Diseño de un centro de proceso de datos"*** De Castro-Acuña Lasheras, (2013)**,** indica que para analizar las mejores prácticas en la instalación e implementación de un centro de datos bajo las normas europeas, determina presentar el centro de datos como un conjunto de infraestructuras necesarias cuyo diseño e integración sean óptimas para el resguardo de la información crítica, utilizando las mejores prácticas de instalación e implementación del centro de datos conforme a las normas europeas basadas en un caso ficticio de instalación de un centro de datos en una organización.

En su parte introductoria nos indica:

> *El CPD[5] es, en muchos aspectos, el cerebro de una compañía. Un CPD bien diseñado y gestionado con efectividad incrementará la productividad de la compañía proporcionando una red de mayor disponibilidad y fiabilidad, y mayor velocidad de procesamiento de datos. Adicionalmente, un CPD bien diseñado estará preparado para futuras ampliaciones e innovaciones.* (De Castro-Acuña Lasheras, 2013, pág. 23)

[5] Centro de proceso de datos. Nota del autor.

Uno de los preceptos más importantes de cualquier red de datos, es que siempre crecerá de forma exponencial con el paso del tiempo. Por lo cual deberán de implementarse medidas de expansión en los centros de datos, así como dentro de toda la infraestructura de red que se encuentre instalada en la organización. Es un hecho que como medida de seguridad y de buenas prácticas en la implementación, siempre se debe considerar un mínimo del veinte por ciento de crecimiento a futuro en toda la infraestructura instalada; considerando las futuras aplicaciones y nuevas tecnologías.

> *Dado que no existen estándares que especifiquen cómo debe construirse un CPD, tan sólo buenas prácticas que deben aplicarse en la medida que mejor se ajusten a los requerimientos particulares de cada CPD, la primera fase fue de recopilación y lectura de estándares relacionados con las infraestructuras del CPD. Tras esto, se fue recorriendo cada una de las infraestructuras a partir de las soluciones más comunes y recomendadas para cada una de ellas, basándome en hojas de datos (datasheets) y casos de estudio (white papers) de las soluciones de distintos fabricantes.* (De Castro-Acuña Lasheras, 2013, pág. 24)

Dentro de sus conclusiones nos permite ver una de las problemáticas principales del uso de nueva tecnología dentro del centro de datos al cambiar servidores para utilizar mejor el espacio disponible en los gabinetes:

- *Uno de los principales problemas del Centro de Proceso de Datos es la disipación del calor que generan los equipos que contiene. Debido a la reducción del tamaño de los servidores, se originan puntos calientes en el Centro de Proceso de Datos que deben ser eliminados para evitar una caída del servidor.*
- *Una de las principales causas de paradas de servicio de un Centro de Proceso de Datos, con las consiguientes pérdidas*

> *económicas y de datos que esto pueda provocar, es la interrupción o alteración del suministro eléctrico* (De Castro-Acuña Lasheras, 2013, pág. 194).

En su trabajo de grado de ingeniería titulado ***"Análisis para el diseño de infraestructura de un centro de datos/Datacenter"*** Barreiro Varela, (2013) determina las necesidades y requerimientos técnicos generales para la obra civil, equipo tecnológico y estándares técnicos internacionales para el funcionamiento de un centro de datos. Al utilizar los estándares más estrictos de alta disponibilidad, redundancia eléctrica, mecánica, comunicaciones, detección y seguridad para el diseño e implementación de los requerimientos del proyecto. La finalidad del proyecto consistió en obtener una clasificación *TIER III*[6], la cual indica que el centro de datos deberá estar con disponibilidad de un 99.98 por ciento de operación continua con 1.6 horas de falla al año.

El autor nos indica que, a pesar de haber realizado el diseño y la instalación desde la planeación en forma inicial de un centro de datos, su prioridad fue crear un centro de datos que cumpliera con las especificaciones del sistema de clasificación *Tier* al momento de realizar el diseño del centro de datos, como nos lo hace ver en sus conclusiones:

- *El tener un proceso representa una base objetiva para el diseño de un Centro de Datos, bajo las mejores formas y prácticas para su construcción. Lo anterior se ha derivado de nuestra experiencia adquirida a través del tiempo y el número de sitios diseñados. Además, se ha tomado una metodología que diferencia cuatro calificaciones de topología de infraestructura de sitio, tanto en componentes como en redundancia, denominada Tier Stándard Topology of Institute Uptime. La*

[6] Véase anexo I – Principales estándares del cableado estructurado sección: Clasificación *Tier* para centros de datos

secuencia de los temas trata de indicar los criterios y diseños que deben tomarse como forma para la infraestructura a nivel de sitio, requeridos para sostener las operaciones de los centros de datos, integrando una serie de subsistemas de infraestructura por separado, para poder tener una decisión más crítica de los diseñadores para la elección y consideración de las múltiples tecnologías en las diferentes especialidades mencionadas en este diseño, que son básicamente cuatro: eléctrica, mecánica, arquitectónica y los sistemas de seguridad y detección.

- *En el mismo orden y dirección, se identifica con claridad la ruta de diseño del Centro de Datos y la configuración de los sistemas dentro de su instalación, incorporando las decisiones y/o estrategias hechas durante el diseño, apoyándonos en la planeación representada en un cronograma y proponiendo un diseño arquitectónico para una mejor funcionalidad de los sistemas mecánico, eléctrico y, en específico, los sistemas especiales. No olvidemos que los códigos de construcción predominantes en la región deberán regir los elementos no cubiertos por este documento y deberán ser considerados como requisitos mínimos.*
- *A manera de colofón, se puede decir que esta propuesta de implementación no pretende imponer restricciones o requerimientos innecesarios o desalentar la innovación en el diseño Tier III, como se describe por el Uptime Institute[7]. Asimismo, no solo toma en cuenta la innovación tecnológica, sino también las estrategias de funcionalidad y ahorro de energía. Cabe señalar, nuevamente, que el aspecto de la eficiencia y eficacia de las operaciones de este diseño consiste*

[7] *Uptime Institute* es reconocido mundialmente por la creación y administración de los estrictos Estándares y Certificaciones *Tier*, que permiten a los centros de datos cumplir su misión y, al mismo tiempo, mitigar los riesgos. (Uptime Institute, 2019)

> *en tener una redundancia concurrente y entregar una disponibilidad de al menos 99.98% de operación continua con 1.6 horas de falla al año. Los sistemas redundantes mantendrán operaciones de forma continua y facilitarán el mantenimiento concurrente, sin ventanas de mantenimiento para reparar, reemplazar o mantener los sistemas mecánicos, eléctricos y sistema especiales que contiene la seguridad del inmueble* (Barreiro Varela, 2013, pág. 122).

Como podemos observar en las conclusiones anteriormente expuestas en las instalaciones del centro de datos, no siempre se han seguido las recomendaciones y principalmente los estándares de instalación de la infraestructura necesaria para los centros de datos de las organizaciones.

Adicionalmente a lo expuesto, las nuevas tecnologías tanto de infraestructura como emergentes, han sostenido un crecimiento más acelerado que las actualizaciones de las normas de cableado estructurado. Motivo por el cual los diseños de los centros de datos de la última década han visto incrementados los problemas de disponibilidad de los servicios por la convergencia de tecnologías en los centros de datos entre otros factores determinantes.

Justificación de la investigación

En la última década, se han realizado importantes avances en tecnología principalmente en equipos de transmisión de datos, como son: aumento de las velocidades de ancho de banda por medio de fibra óptica, reducción de los costos de fabricación de fibra óptica, reducción de los servidores con mayor potencia de procesamiento de datos, entre una amplia gama de dispositivos que actualmente se incorporan a los centros de datos.

Adicionalmente, la aparición de las llamadas tecnologías emergentes que han marcado la necesidad de replantear la implementación y administración de la

infraestructura tecnológica dentro de las organizaciones, que afectan directamente a los centros de datos.

Sin embargo, dado la importancia que se ha dado en los últimos años al crecimiento exponencial en las comunicaciones y transferencia de datos entre las corporaciones, institutos de enseñanza y en la industria en general con el uso de videoconferencias, migración de datos a la Nube, la facilidad de acceso a Internet de los dispositivos móviles y las implementaciones actuales del *IoT*, el crecimiento y la convergencia[8] de tecnologías, han llegado a colapsar las comunicaciones en diversas ocasiones de los centros de datos de las empresas.

Para Martínez H., (2017), el primer paso para poder rescatar un centro de datos es reconocer los signos de envejecimiento:

- ***Falta de espacio / capacidad de potencia*** *– Cuando el espacio físico o la capacidad de potencia del centro de datos comienza a agotarse, ocurren dos tipos de problemas. En primer lugar, la capacidad de crecimiento al ritmo deseado por la compañía se ve limitada. Si se presenta una oportunidad de mercado a corto plazo, la capacidad que tenga el centro de datos para adaptarse rápidamente es un factor de éxito crucial para sacar provecho de dicha oportunidad. El segundo problema es que añadir nuevos servidores puede sobrecargar los circuitos derivados y aumentar la temperatura del centro de datos. Ambas situaciones pueden llevar a un tiempo de inactividad inesperado.*
- ***Enfriamiento ineficiente*** *– Con el tiempo, las densidades del estante tienden a aumentar. Al final, se llega a un punto*

[8] Velocidad y capacidad de un grupo de dispositivos de red que ejecutan un protocolo de enrutamiento específico para concordar sobre la topología de una interconexión de redes luego de un cambio en esa topología. (Terán, 2014, pág. 457)

de inflexión y se generan zonas conflictivas dentro del centro de datos. El personal del centro de datos necesitará determinar si la distribución de enfriamiento existente puede manejar estas cargas más concentradas. Para un centro de datos tradicional, no contenido, en un piso elevado, más del 50% del aire frío suministrado por las unidades de enfriamiento volverá directamente a estas unidades como resultado de los caminos de derivación que existen. Estas malas prácticas de gestión del flujo de aire reducen la efectividad de los sistemas de enfriamiento existentes.

- ***Aumento de los costos de mantenimiento*** *– Si los costos de mantenimiento continúan aumentando a una tasa estable, esto puede significar que los sistemas anticuados están amenazando la fiabilidad de las operaciones del centro de datos. A medida que envejece la infraestructura, también aumenta la posibilidad de una falla. Por lo tanto, cada vez es más importante desarrollar un programa efectivo de operaciones y de mantenimiento.*
- *Las señales de advertencia que indican que los componentes dentro del centro de datos están cerca del final de su vida útil; incluyen proveedores que dejan de dar soporte a los sistemas instalados, escasez de partes de repuesto, KPI's de eficiencia y capacidad que no cumplen con las necesidades actuales o futuras, y partes obsoletas que están fallando o que probablemente van a fallar*. (Martínez H. , 2017)

En la actualidad, se tienen que replantear los modelos de seguridad dentro de las organizaciones y realizar modificaciones para poder efectuar un análisis de riesgos de diversas brechas de seguridad dentro de las empresas que son derivadas

directamente del uso exponencial de los dispositivos de *IoT y* que en los últimos años se han visto incrementados al interior de las organizaciones.

Adicionalmente al uso cada vez mayor de las redes sociales como una forma de comercio electrónico por parte de las organizaciones, han incrementado el nivel de las transferencias de datos en las redes de comunicaciones.

Para Greg Zwakman (2019), vicepresidente de mercado e inteligencia competitiva de 451 Research "*más de la mitad de los racks utilizados a nivel mundial estarán en instalaciones fuera de las instalaciones, incluidos los sitios de Nube y colocación, para fines de 2024*" (Citado por 451 Research, 2019).

> *En todos los tipos de propietarios y ubicaciones geográficas, los proveedores de servicios y la Nube están impulsando la expansión, y los hiperescaladores representan la punta de lanza. Esperamos ver una disminución en los bastidores utilizados en toda la empresa, con un aumento de CAGR*[9] *de medio dígito en la colocación fuera de la Nube, y los proveedores de Nube y servicios expandiendo su huella utilizada en más del 13%.* (451 Research, 2019)

La planeación de los departamentos de *TI* en las organizaciones, quienes concibieron una idea de flujo de información al diseñar sus centros de datos, han visto rebasados los anchos de banda en muy poco tiempo y al mismo tiempo se ha observado un incremento exponencial del flujo de información, ocasionando que en diversas ocasiones colapsen centros de datos con la más reciente tecnología instalada. De igual forma, la convergencia de los centros de datos es ahora una realidad y se encuentran afectando principalmente los sistemas de distribución de una forma no prevista anteriormente.

[9] Tasa de crecimiento anual (por sus siglas en inglés *CAGR (Compound Annual Growth Rate)*) véase (Econodía, 2011)

Con base en los pronósticos de las investigaciones de mercado a nivel mundial realizadas por la empresa Gartner, nos indican que tendremos una reducción de la inversión del gasto en el área de *TI* para los siguientes años. Indicando que el gasto mundial en Tecnologías de la información presentara un crecimiento de tres punto dos por ciento como podemos observar en la ***Tabla 1 - Pronóstico mundial de gastos de TI***.

Tabla 1 - Pronóstico mundial de gastos de TI

Pronóstico mundial de gastos de TI (miles de millones de dólares estadounidenses)						
	Gasto 2018	**Crecimiento 2018 (%)**	**Gasto 2019**	**Crecimiento 2019 (%)**	**Gasto 2020**	**Crecimiento 2020 (%)**
Sistemas de centros de datos	202	11.3	210	4.2	202	-3.9
Software empresarial	397	9.3	431	8.5	466	8.2
Dispositivos	669	0.5	679	1.6	689	1.4
Servicios de TI	983	5.6	1,030	4.7	1,079	4.8
Servicios de comunicaciones	1,399	1.9	1,417	1.3	1,439	1.5
TI en general	**3,650**	**3.9**	**3,767**	**3.2**	**3,875**	**2.8**

Fuente: (Gartner, 2019)

Con base en la información proporcionada en la ***Tabla 1 - Pronóstico mundial de gastos de TI***, podemos observar lo siguiente:

- El crecimiento esperado para el 2019 en los centros de datos será de apenas un 4.2 por ciento, a comparación del 11.3 por ciento que se obtuvo en el 2018.

- El pronóstico esperado para el año 2020 presentará una reducción del gasto en *centro de datos* del 3.9 por ciento.
- El gasto en software empresarial presentara un ligero decremento de 8.5 por ciento en comparación del 9.3 por ciento del período 2018 y se pronostica un ligero decremento de 8.2 por ciento para el 2020.

Por otra parte, se encuentran los resultados del informe del monitor del mercado de infraestructuras y servicios del centro de datos, que se creó con base en la reconocida cobertura líder de la industria del *451 Research* del mercado mundial de centros de datos. En el informe, se proporciona una visión de la base mundial instalada del número total de sitios de centros de datos a nivel mundial (451 Research, 2019).

> *Nuestra investigación aprovecha otros 451 resultados de investigación, como Datacenter Knowledge Base [una base de datos detallada de más de 6,300 centros de datos de múltiples inquilinos], encuestas de usuarios finales de Voice of the Enterprise y otros productos de Market Monitor. Al hacerlo, podemos ampliar nuestro análisis en torno a áreas como el impacto de IoT en los proveedores de centros de datos, la participación de los proveedores de servicios y la Nube en el mercado de centros de datos y otros análisis derivados*. (451 Research, 2019)

Los hallazgos clave de este informe incluyen:

- *El crecimiento total de la base instalada del centro de datos mundial continuará disminuyendo ligeramente, a una CAGR de -0.1% entre 2019-2024; sin embargo, la capacidad total en términos de espacio, potencia y bastidores continuará aumentando a medida que las organizaciones cambien a centros de datos más grandes.*

- *Las salas de servidores y los armarios representan casi el 95% del total de centros de datos, pero solo el 23% del total de bastidores utilizados en 2019.*
- *La mayoría del espacio del centro de datos de la empresa (60%) corresponde a centros de datos de menos de 10,000 pies cuadrados.*
- *El centro de datos de múltiples inquilinos promedio (MTDC) es casi nueve veces más grande que un centro de datos empresarial (excluyendo salas / armarios y micro CC / centros de telecomunicaciones) en 2019.*
- *Los seis principales hiperescaladores representan el 42% del total de bastidores utilizados en la Nube y los proveedores de servicios en 2019. Se espera que se expanda a una CAGR del 18%, alcanzando el 50.4% del total para 2024.*
- *Se espera que la demanda de racks para soportar cargas de trabajo de IoT y almacenamiento de datos de IoT crezca a una CAGR del 46% de 2019 a 2024, lo que representa el 15% del total de los racks de centros de datos globales para finales de 2024.* (451 Research, 2019)

En general, podemos hablar de un proceso de decadencia[10] al observar que el área de *TI* en las organizaciones; comienza a presentar un ligero decremento en sus porcentajes de crecimiento anual esperado. Adicionalmente, las habilidades del personal interno de *TI* de las organizaciones, comienzan a presentar un retraso en su desarrollo, esto a medida que las mismas adoptan el uso de nuevas tecnologías para poder impulsar el negocio digital como son el uso de los dispositivos *IoT.*

[10] Decadencia es la declinación o el principio de la ruina. Se trata de un proceso de deterioro y menoscabo a través del cual las condiciones o el estado de algo o alguien comienzan a empeorar. La noción de decadencia puede aplicarse a las personas o a los objetos. El concepto, a su vez, puede hacer mención a una característica física (material) o a una cuestión abstracta (simbólica, espiritual). Respecto a las cosas, la decadencia suele referirse al descuido o a los daños materiales por el paso del tiempo. (Definicion.de, 2019)

Así como los requerimientos necesarios para poder realizar la implementación de la Inteligencia Artificial (*IA*), análisis de grandes volúmenes de datos (*Big Data*), entre otras plataformas necesarias para la prestación de servicios y la administración de datos generados para la toma de decisiones. Situaciones que hoy en día están cambiando más rápido de lo esperado.

Preguntas de investigación.

Primera pregunta.

¿Cómo impacta la implementación del *IoT* en un centro de datos con más de cinco años de antigüedad?

Segunda pregunta.

¿Qué consecuencias tiene el *IoT* en la seguridad de los centros de datos en las organizaciones?

Tercera pregunta.

¿Qué efectos tendrá para el centro de datos de las organizaciones la implementación del *IoT* en la Nube (*Cloud Computing*)?

Objetivo general.

- Analizar como las tecnologías emergentes, principalmente el *IoT* impactan en el desempeño y la seguridad de los centros de datos con más de cinco años de antigüedad; que fueron implementados siguiendo las normas del cableado estructurado.

Objetivo particular.

La presente investigación tiene como objetivo particular los siguientes preceptos:

- Analizar el impacto en la seguridad que tienen las tecnologías emergentes en los centros de datos de las organizaciones específicamente el *IoT*.

- Analizar los efectos económicos de la implementación masiva del *IoT* en las ciudades inteligentes (*Smart Cities*) y su impacto en los centros de datos de las organizaciones.

Hipótesis.

Hipótesis de la primera pregunta.

Las organizaciones están preparadas para enfrentar los retos de la administración de las *TI* al implementar las nuevas tecnologías emergentes específicamente los dispositivos del *IoT* en sus centros de datos derivado directamente de los pronósticos del incremento exponencial de dispositivos a nivel mundial.

Hipótesis de la segunda pregunta.

Las organizaciones tienen un adecuado proceso de auditoria informática y seguridad para poder implementar con éxito los dispositivos del *IoT* en sus centros de datos actuales.

Hipótesis de la tercera pregunta.

Las organizaciones tienen considerado migrar sus procesos de un centro de datos tradicionalmente centralizado hacia la Nube lo cual representa un ahorro considerable en su administración y marca la tendencia de la desaparición del centro de datos de manera tradicional (centralizado).

Método.

La presente investigación se realizará por medio del método cuantitativo de investigación y tendrá un alcance de estudio exploratorio de corte longitudinal, lo que nos permitirá realizar un análisis de las circunstancias actuales de la infraestructura y la implementación de las tecnologías emergentes dentro de las organizaciones. En específico, el *IoT* al brindarnos el objetivo de investigar sobre un tema poco estudiado y que nos permitirá determinar tendencias, identificar áreas de oportunidad, ambientes y situaciones de estudio posterior.

Resumen capitular.

- En el **Capítulo I – Marco Teórico**., se hablará acerca los conceptos teóricos fundamentales para la implementación del centro de datos en las organizaciones y de las características básicas de las principales tecnologías emergentes.

- En el **Capítulo II – Las Tecnologías emergentes y las organizaciones**, se mostrarán más detalladamente las características de las principales tecnologías emergentes y su integración con las organizaciones, así como los retos que deben enfrentar la administración de los departamentos de *TI* para los Centro de Datos.

- En el **Capítulo III – Pronósticos del tráfico de datos**, se analizarán los pronósticos basados en las estadísticas mundiales de los niveles de transmisión de datos. Al igual que los motivos por los que las organizaciones están migrando sus centros de datos tradicionales a la Nube y utilizando la Computación al Borde para generar ahorros en infraestructura y el impacto que esta decisión representa.

- En el **Capítulo IV – Principales desafíos de las organizaciones** se demostrarán los problemas del centro de datos que enfrentan las empresas, derivados de las nuevas tecnologías y se analizaran los principales efectos de mantener un centro de datos de forma centralizada, así como el impacto que tienen con el *IoT*.

- En el **Capítulo V - Análisis de resultados**, se analizaran los resultados obtenidos de la investigación para poder comprobar las hipótesis, preguntas de investigación y los objetivos de la misma.

1 Capítulo I – Marco Teórico.

1.1 Centro de datos o *Datacenter*

Un Centro de datos o mejor conocido como *Datacenter*[11], debe cumplir con características específicas y principalmente instalarse en un área de acceso restringido, ya que ahí es donde se almacenará toda la información crítica y vital de la organización.

En este contexto el centro de datos debe ser regido por una norma o regla que será el precedente para la manera correcta en la que deberemos implementar los siguientes conceptos primordiales:

- Cuestiones de seguridad perimetral como son: control de accesos, Circuito Cerrado de Televisión (CCTV) y sistemas biométricos.
- Control de energía redundante.
- Control ambiental como son: aire acondicionado, humedad, temperatura.
- Distribución de los equipos tales como: gabinetes, servidores, equipos de energía redundante.
- Sistema de protección contra incendios como son: detectores de humo, extintores de gas o polvo químico, extractores de humo.
- Canalización adecuada del cableado estructurado como: escalerillas, ductería abierta, piso falso, organizadores de cableado.

En la ***Ilustración 1 - Centro de datos típico***., podremos observar la forma típica de un centro de datos con una instalación estándar basada en las normas internacionales del cableado estructurado. En donde se encuentran aplicados los

[11] Una instalación empleada para albergar un sistema de información de componentes asociados, como telecomunicaciones y los sistemas de almacenamientos donde generalmente incluyen fuentes de alimentación redundante o de respaldo de un proyecto típico de Centro de datos que ofrece espacio para hardware en un ambiente controlado, como por ejemplo acondicionando el espacio con el aire acondicionado, extinción de encendidos de diferentes dispositivos de seguridad para permitir que los equipos tengan el mejor nivel de rendimiento con la máxima disponibilidad del sistema (Definición de Datacenter, 2015).

estándares del cableado estructurado y principalmente la norma de la EIA/TIA 942[12] para diseño del centro de datos que debe implementarse en las organizaciones. Lo cual permite brindar un nivel de confiabilidad de que todo el cableado de red corporativa se encuentra centralizado en un centro de datos bajo los estándares y normas correctas de instalación. Lo que permitirá si es necesario, obtener una certificación del fabricante del cableado[13] y sus diversos accesorios garantizando la funcionalidad y desempeño de la infraestructura para las aplicaciones futuras durante los próximos veinte años.

Ilustración 1 - Centro de datos típico.
Fuente: *(Integrity, 2018)*

[12] Véase anexo I – Principales estándares del cableado estructurado sección: ANSI/TIA 942-A Estándar de Infraestructura de Telecomunicaciones para Centros de *Datos (Telecommunications Infraestructure Standard for* Data **Centers).**

[13] La certificación del cableado estructurado es un proceso en el que se compara el rendimiento de transmisión de un sistema de cableado instalado con un estándar determinado, empleando un método definido por el estándar para medir dicho rendimiento. Nota del autor.

Un centro de datos se encuentra integrado por diversas infraestructuras que se consideran las mínimas indispensables para la seguridad perimetral del centro de datos, como son:

- Sistema de tierra física.
- Energía regulada redundante por medio de UPS ’s de alta capacidad.
- Sistemas de enfriamiento.
- Gabinetes de protección para los servidores.
- Servidores de datos de alto desempeño para ser instalados en racks.
- Sistemas de distribución de cableado estructurado.
- Sistema contra incendios.
- Sistema de video vigilancia.
- Seguridad perimetral con registro biométrico.

Por lo tanto y debido a las características principales del centro de datos dentro de las organizaciones, es de suma importancia que se encuentre instalado en un área estratégicamente ubicada dentro de las instalaciones de la empresa o institución. A lo que comúnmente se le denomina un centro de datos tradicional.

1.2 Estándares, certificaciones y documentos relacionados.

Dentro del diseño e implementación de un centro de datos, se deben de considerar los estándares internacionales y certificaciones del país en el que se pretenda realizar la implementación del centro de datos. Entre los más importantes a considerar se encuentran los presentados en la ***Tabla 2 - Estándares y Certificaciones Internacionales.***

Tabla 2 - Estándares y Certificaciones Internacionales

TIA-942-B	*Telecommunications Infraestructure Standard for Data Centers.*
BICSI 002	*Data Center Design and Implementation Best Practices.*

EN 50600	*Information technology – data centre facilities and infraestructures.*
AS/NZS 2834	*Computer Accommodation Standars Australia BCL.*
EIA/ECA-310-E	*Cabinets, Racks, Paneles and Associeted Equipment.*
UL 2416	*Standard for Audio/Video, Information and Communication Technology Equipment Cabinet, Enclosure and Rack Systems.*
ANSI/TIA-568-C.0	*Generic Telecommunications Cabling for Costumer Premises.*
ANSI/TIA-568-C.1	*Commercial Building Telecommunications Cabling Standard.*
ANSI/TIA-568-C.2	*Balanced Twisted-Pair Telecommunications Cabling and Components Standard.*
ANSI/TIA-568-C.3	*Optical Fiber Cabling Components Standard.*
ANSI/TIA-569-D	*Telecommunications Pathways and Spaces.*
ANSI/TIA-606-B	*Administration Standard for Telecommunications Infraestructure.*
ANSI/TIA-607-B	*Telecommunications Bonding and Grounding (Earthing) for Customer Premises.*
ANSI/TIA-607-C	*Telecommunications Bonding and Grounding (Earthing) for Customer Premises.*
ANSI/TIA-758-B	*Customer-Owned Outside Plant Telecommunications Infraestructure Standard.*
ISO/IEC 24764	*Information Technology – Generic Cabling Systems for Data Centres.*
FC-BB-5	*Standard Fibre Channel over Ethernet (FCoE)*
LEED Certification	*USGBC (United States Green Building Council).The Green Grid. Energy Star (EPA).*
Uptime Institute	*Tier Standard:* ***Topology.*** *Tier Standard:*

	***Operational Sustainnability*.** **ATD** *(Accredited Tier Designer)* **ATS** *(Accredited Tier Specialist) – Uptime Institute.*
NESC® IEEE C 2	*National Electric Safety Code®.*
IEEE Std. 446	*Recommended Practice for emergency and Standby Power Systems for Industrial and Commercial Applications.*
UL Std. 1100	*Recommended Practice for Powering and Grounding Electronic Equipment.*
UL 2043	*Fire Test for Heat and Visible Smoke Release for Discrete Products and their Accesories Installed in Air-Handling Spaces.*
ISO 50001	*Energy Managment.*
NFPA 101	*Life Safety Code®.*
ANSI/NFPA 90A	*Installation of Air-Conditioning and Ventilating Systems.*
NFPA 70	*NEC® National Electric Code®.*
NFPA 75	*Standard for the Protection of Information Technology Equipment.*
NFPA 76	*Standard for the Fire Protection of Telecommunications Facilities.*
NFPA 25	*Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems.*
NFPA 13	*Standard for the Installation of Sprinkler Systems.*

Fuente: (Standards Reference Guide, 2017)[14]

Una parte fundamental dentro de las organizaciones es el cableado estructurado, el cual puede limitar el crecimiento de la organización cuando el mismo se encuentra mal diseñado, planeado y administrado. La razón de que existan distintas normas internacionales y nacionales para la implementación de un cableado estructurado y

[14] Véase Anexo I – Principales estándares del cableado estructurado

principalmente para el diseño de un centro de datos, es el de garantizar que las aplicaciones actuales y futuras puedan ser debidamente ejecutadas sin que existan problemas en la transmisión de datos, derivadas de una mala implementación o administración de la infraestructura de red dentro de las empresas. Como podemos observar, existen diversas normas y certificaciones que deben ser tomadas en consideración para el diseño, instalación e implementación de un centro de datos.

En México, las normas y estándares surgen del Organismo Nacional de Normalización denominado "Normalización y Certificación Electrónica, S.C. (NYCE)[15] quien es responsable de desarrollar los estándares del cableado estructurado y comunicaciones para los usuarios de infraestructura de *TI* en México.

Este organismo ha liberado hasta la fecha nueve normas relacionadas con el cableado estructurado, y que se encuentran basadas en los estándares internacionales de la ISO/IEC-14763-2[16]; su declaratoria de vigencia se encuentra aprobada y publicada por el Diario Oficial de la Federación y son las que se mencionan en la ***Tabla 3 - Normas mexicanas de cableado estructurado***.

Tabla 3 - Normas mexicanas de cableado estructurado.

NMX-I-108-NYCE-2006	Puesta a tierra en sistemas de telecomunicaciones
NMX-I-132-NYCE-2006	Especificaciones de las Pruebas de cableado balanceado - Parte 1: Cableado Instalado
NMX-I-154-NYCE-2008	Cableado genérico residencial
NMX-I-248-NYCE-2008	Cableado de Telecomunicaciones para Edificios Comerciales - Especificaciones y Métodos de prueba

[15] Para poder tener acceso a las Normas, se requiere registro y posterior pago (Normalización y Certificación NYCE, S.C., 2019).

[16] Véase (International Organization for Standardization (ISO), 2012)

NMX-I-279-NYCE-2009	Canalizaciones y Espacios para cableado de telecomunicaciones en Edificios Comerciales
NMX-I-14763-1-NYCE-2010	Implementación y Operación de cableado en Edificios Comerciales - Parte 1: Administración
NMX-I-24764-NYCE-2013	Tecnología de la Información - Sistema de cableado genérico para Centros de Datos
NMX-JCI-489-ANCE-ONNCCE-NYCE-2014	Centros de Datos de Alto Desempeño sustentable y energético - Requisitos y Métodos de comprobación
NMX-I-14763-2-NYCE-2017	Tecnologías de la Información-Implementación y Operación de Cableado Estructurado - Parte 2: Planeación e instalación

Fuente: *(Normalización y Certificación NYCE, S.C., 2019)*

Las normas tienen la finalidad de proporcionarle a las empresas una garantía de que las infraestructuras instaladas del cableado estructurado, así como de los centros de datos dentro de las organizaciones, cuenten con las características necesarias para soportar las aplicaciones y el crecimiento a futuro de nuevas implementaciones de tecnología, motivo por el cual es importante cumplir con ciertas normas y estándares dentro de las organizaciones para que puedan estar seguras de que la inversión realizada en infraestructura sea redituable a futuro.

La sociedad actualmente ha generado que las personas tengan un consumo y una producción de información (datos) a un nivel nunca antes visto: Internet, motores de búsqueda, aplicaciones para móviles y los teléfonos inteligentes (*Smartphone*) podemos encontrarlos por todas partes, y consideramos que su existencia es una cosa natural. Pero la realidad es que todos los dispositivos dependen del almacenamiento, la distribución en red, el procesamiento de datos digitales y casi todas las operaciones se ejecutan en un centro de datos o con su mediación. Sin duda, los centros de datos se han convertido en un factor vital para las organizaciones que ejecutan aplicaciones críticas.

La infraestructura de *TI* se clasifica normalmente en tres categorías: servidores, conmutadores de red (*Switches*) y espacio de almacenamiento. Cada grupo tiene su función exclusiva, aunque en muchos casos los servidores incluyen almacenamiento; los centros de datos ejecutan gran variedad de software, virtualización, bases de datos, hospedaje Web, sistemas operativos y Nubes. Por lo que las empresas han considerado realizar migraciones de ciertos procesos a la Nube con lo cual buscan reducir los costos operativos en la administración del centro de datos.

Como podemos observar, los centros de datos son la base medular de cualquier organización y se encuentran presentes en diversos sectores que podrían considerarse prioritarios como pueden ser las que se presentan en la ***Tabla 4 - Principales sectores de inversión.***

Tabla 4 - Principales sectores de inversión

***Housing* y *Hosting*[17]**.	Muchas empresas pequeñas y/o medianas no quieren o no tienen la capacidad necesaria para poder invertir en la infraestructura requerida para un centro de datos, por lo que recurren a empresas de *Hosting* y/o *Housing*, las cuales buscan proporcionar mediante una renta los servicios de almacenamiento de páginas web y también los servicios propios de administración de *TI*.
Entidades financieras[18].	Todas las entidades financieras requieren de un centro de datos y de su gran disponibilidad para poder realizar las transacciones bursátiles de manera eficiente, confiable, segura y rápida. Los

[17] Véase (AXARNET, 2018)
[18] Véase (Martínez C. A., 2018)

	bancos y diversas instituciones financieras como, por ejemplo: La Bolsa Mexicana de Valores (BMV), la bolsa de valores de Nueva York (NYSE), la bolsa de valores de Tokio.
Telecomunicaciones.	Dentro del sector de las telecomunicaciones el centro de datos desempeña un papel fundamental, ya que actualmente casi todos los servicios de telefonía son digitales y muchas organizaciones utilizan VoIP (por sus siglas en inglés *Voice over IP*), utilizando la conectividad de Internet. Entre los que se encuentran: Telmex, AT&T, Alestra, solo por mencionar algunos de ellos. Los principales proveedores de telecomunicaciones, poseen, construyen y explotan sus propios centros de datos con fines comerciales.
Servicios de TI.	Empresas como *Facebook*, *Google*, *Amazon*, *eBay*, entre muchas otras, se iniciaron con el "boom" de Internet hace ya quince años y su principal recurso es la comercialización de servicios que van desde la publicidad hasta la venta por Internet.
Administración pública.	Dentro de la administración pública, un ejemplo muy claro de la necesidad de un centro de datos robusto y eficiente es la Secretaria de Hacienda y Crédito Público (SHCP). Para los organismos públicos, la necesidad de contar con un centro de datos implica un costo muy alto. Motivo por el cual debe verse como una inversión y tener una planeación estricta.

Asistencia Sanitaria[19].	Considerando en este rubro a los centros hospitalarios, por citar algunos: Instituto Mexicano del Seguro Social (IMSS), Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), Medica Sur, gracias a la tendencia de digitalización de los historiales clínicos de los pacientes.
Sociedades, comercio minorista, fabricación, compañías de servicio público.	Se incluye una gama de empresas públicas y privadas de diversos sectores. Las industrias privadas como los grandes corporativos, cuentan con sus propios centros de datos a diferencia de las PYME ´s que por lo general optaran por los servicios de hosting. Por ejemplo: las compañías de gas, empresas automotrices, empresas de comercialización de productos alimenticios, etcétera.

Fuente: Elaboración propia.

Como podemos observar el centro de datos es la base fundamental para la operación de las organizaciones de diversos sectores. Sin embargo, los centros de datos han venido evolucionando con el paso de los años derivado de los cambios constantes de tecnología.

Han sido principalmente el tráfico de red y las necesidades de un mundo globalizado las razones que han marcado la pauta en el desarrollo e integración de nuevas tecnologías al interior de los centros de datos y que les permiten a las organizaciones tener mejores beneficios en la operación y administración de la tecnología generando valor al interior de las mismas.

[19] Véase (ehCOS, 2016)

1.3 Principales Tecnologías emergentes.

Existen varias definiciones de lo que son las tecnologías emergentes, pero la más reconocida es la que publica Day, G. S.; Schoemaker, P. J. H. (2001) en su libro **"*Transferencia de tecnología. Gerencia de tecnologías emergentes"***:

> "*Las tecnologías emergentes son aquellas que se encuentran en la fase inicial del ciclo de vida de la tecnología; nacen cuando surgen propuestas innovadoras de desarrollo de procesos, habilidades o aplicaciones diferentes que cambian las concepciones ya establecidas dentro del mercado y son capaces de modificar industrias ya constituidas y técnicas afianzadas*". (Jiménez-Hernández, Castellanos-Domínguez, & Villa-Enciso, 2011)

Para Santos, (2019) en la publicación de su artículo titulado: ***"Cinco tecnologías que influirán en 2019"***, las tecnologías emergentes presentaran un mayor impacto en el presente año a nivel mundial y por su relevancia tendrán un efecto preponderante en el desempeño de los centros de datos de las organizaciones lo que representara un reto para la administración de las áreas de *TI*, así como para las organizaciones en el futuro cercano.

> *Descifrar el futuro nunca es una tarea fácil, en la medida en que nuevas tecnologías y recursos serán cada vez más importantes a largo plazo. Lo que nos interesa particularmente es observar aquellas que, a corto plazo, empiezan a generar valor de manera que son más útiles para la industria y, claro, para los consumidores. Como lo son: la Inteligencia Artificial (IA), El Cloud y Edge Computing, La Ciberseguridad, las tecnologías inteligentes para beneficiar al medio ambiente y la integración entre sensores para respuestas inteligentes (IoT). Esta nueva realidad requerirá aún más que los equipos de TI estén actualizados sobre las potenciales vulnerabilidades de los equipos conectados a la red.* (Santos, 2019)

1.3.1 Inteligencia Artificial

Para poder hablar de la Inteligencia Artificial (*IA*), es indispensable hacer referencia a los aportes de Alan Turing, quien fuera un célebre matemático y criptógrafo excepcional de nacionalidad británica, es considerado el padre de la Inteligencia Artificial y la ciencia de la computación teórica.

De acuerdo a Historia y Vida, (2018), en 1936 publican su artículo titulado: **"*Sobre números computables, con una aplicación al Entscheidungsproblem*"** (traducible como "problema de decisión"), en el que se define lo que es computable y lo que no es computable, sentando las bases teóricas de que todo lo que es factible de resolverse mediante un algoritmo es susceptible de ser automatizado, de igual forma sienta las bases de la informática teórica.

En septiembre de 1938, el gobierno británico llamó a Alan Turing para dirigir un grupo multidisciplinario para un proyecto en *Bletchley Park* que en ese momento era el centro de criptografía del país y tenía como misión descifrar los mensajes que se generaban de la máquina Enigma que transmitía órdenes codificadas a las fuerzas alemanas y a los submarinos nazis que operaban en el Atlántico.

Es gracias al ingenio de Turing, que se realiza el desarrollo de las primeras máquinas Bombe, que son dispositivos electromecánicos construidos específicamente para descifrar los códigos de la maquina Enigma. De las cuales se construyeron 211 unidades en Bletchley Park y unas 120 en los Estados Unidos, sin embargo, el gobierno británico ordenaría su destrucción al término de la guerra junto con todos los documentos que estuvieran vinculados a su creación (Historia y Vida, 2018).

Turing se planteó el reto de construir una máquina que tuviera las mismas capacidades que el cerebro humano, para lo cual intervino en el diseño de la ACE (*Automatic Computer Engine*, motor de computadora automático) el cual era una

computadora digital electrónica que fue concebida para poder resolver más de un propósito a la vez y que fuera capaz de almacenar un programa en su memoria, lo cual fue el esbozo de las actuales computadoras.

En 1947 Turing dirigió el *Computing Machine Laboratory* de Manchester, en donde desarrolló un nuevo equipo llamado MADAM (mejor conocida como *Manchester Mark I*), la cual era una computadora que poseía la capacidad de almacenar un programa en su memoria principal y que tenía mayores capacidades que su antecesora.

Para ese momento, Turing se encontraba muy interesado en lo que se denomina *IA* que es el modo de imitar artificialmente las funciones del cerebro humano. En 1950, en su estudio denominado: ***Computering Machinering and Intelligence*** (Maquinas de computación e inteligencia), estableció las bases de la *IA* y desarrolló una especie de prueba para determinar si una maquina era inteligente o no, este estudio se le conoce como el test de Turing (Historia y Vida, 2018).

De acuerdo a Iberdrola, (2019) en su publicación: ***"¿Qué es la Inteligencia Artificial?"*** una de las definiciones más claras a la fecha de lo que es la *IA* es: *"La Inteligencia Artificial (IA) es la combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano"*. (Iberdrola, 2019).

De igual forma como comentan los expertos en ciencias de la computación Stuart Russell y Peter Norvig, citados por Iberdrola, (2019), se pueden diferenciar diversos tipos de *IA* y entre los más importantes tenemos los que se muestran en la ***Tabla 5 - Tipos de Inteligencia Artificial.***

Tabla 5 - Tipos de Inteligencia Artificial

Sistemas que piensan como humanos	Que nos permiten la automatización de actividades que son requeridas para la toma de decisiones,

	resolución de problemas y sobretodo el aprendizaje. Un claro ejemplo son las redes neuronales artificiales.
Sistemas que actúan como humanos	Son las computadoras y los equipos de cómputo que realizan tareas de forma similar a como lo hacen las personas como es el caso de los robots.
Sistemas que piensan racionalmente	Son los sistemas que intentan emular el pensamiento lógico racional de los humanos, por lo que se investiga la forma de lograr que las máquinas puedan percibir, razonar y actuar en consecuencia. Los sistemas expertos son un claro ejemplo de este segmento.
Sistemas que actúan racionalmente	Son aquellos que tratan de imitar de manera racional el comportamiento humano, como los agentes inteligentes.

Fuente: (Iberdrola, 2019)

La *IA* se encuentra presente en una amplia gama de dispositivos en la actualidad, como los dispositivos móviles los cuales tienen la capacidad de realizar reconocimiento facial, en los asistentes virtuales de voz como los que se encuentran instalados en *Siri* de Apple, *Alexa* de Amazon o *Cortana* de Microsoft, y entre muchas aplicaciones que existen para diversas áreas como pueden ser el diagnóstico médico, el aprendizaje de idiomas, solo por citar algunas. Todas ellas tienen la finalidad de hacer más fácil la vida de las personas en su vida cotidiana.

Es gracias a los avances obtenidos con el uso de la *IA* que se ha incrementado la utilización de una de las tecnologías emergentes de mayor demanda dentro de las organizaciones el *Big Data*[20], esto es debido a la habilidad que tiene para el procesamiento de grandes volúmenes de información y así proporcionar ventajas de comunicación, comerciales y empresariales.

[20] Véase (PowerData, 2019)

Como podemos observar en la ***Ilustración 2 - Aplicaciones prácticas de la IA***, han llevado al *Big Data* en conjunto con la *IA* a posicionarse como unas de las tecnologías esenciales para las próximas décadas y que son utilizadas en diversos sectores como son: asistentes personales virtuales, finanzas, educación, comercial, climáticas, agrícolas, sanidad, logística y transporte, entre otras.

Ilustración 2 - Aplicaciones prácticas de la *IA*
Fuente: (Iberdrola, 2019)

1.3.2 Computación en la Nube (*Cloud Computing*).

Para poder brindar una definición de lo que es la Nube, debemos tomar en cuenta que es un concepto que durante años ha sido causa de polémica en diversos sectores al momento de dar una conceptualización de la Nube, dado que el concepto de en realidad es una metáfora de Internet, la cual surge a raíz de que se solía representar de manera gráfica la infraestructura de servidores que formaban Internet, como una Nube que flotaba encima de todo y que era capaz de aceptar diversos tipo de conexiones, la que a su vez distribuía la información a los servidores que se conectaban a ella (PowerData, 2019).

En una arquitectura de *Cloud Computing*, todos los datos se recopilan y procesan en una ubicación centralizada, generalmente en un centro de datos. Todos los dispositivos que necesitan acceder a estos datos o utilizar aplicaciones asociadas deben primero conectarse a la Nube. Los cuales abarcan aplicaciones y servicios, como son por ejemplo los servicios que ofrecen Google (Gmail, Google Drive, etcétera) a formas de almacenamiento de datos como lo hace Dropbox, aplicaciones de facturación, CRM, entre otras.

Por lo que el concepto de Nube (*Cloud)*, significa almacenar y acceder a datos y programas los cuales utilizan como medio de transmisión Internet por medio de un tercero, en lugar de realizarlo de forma directa a través de los medios de almacenamiento de los servidores que se encuentren instalados dentro de la organización.

Es necesario marcar una diferencia entre los conceptos de *Cloud* y *Cloud Computing*, el primero hace referencia básicamente a Internet en forma general y nos referimos a ella cuando necesitamos obtener datos, aplicaciones o infraestructura que se encuentra fuera de nuestras instalaciones y que no necesariamente son desarrollos propios de la organización.

Por otro lado, el *Cloud Computing* nos habla de los productos y servicios que funcionan en la Nube y a los cuales podemos acceder por medio de Internet, por lo tanto, se refiere al acceso de los equipos de cómputo, elementos de *TI* y aplicaciones de software los que, mediante la utilización de una conexión a Internet (utilizada como un medio de comunicación) pueden acceder a centros de datos utilizando redes de área amplia (*WAN*, por sus siglas en inglés *Wide Area Network*). Por lo que, en adelante, para fines prácticos nos referiremos a la Nube como los procesos referentes al *Cloud Computing*.

En la actualidad, podemos hablar de diversos tipos de Nubes en los cuales podemos distinguir principalmente ciertas características de propiedad, tamaño y acceso al momento de realizar una implementación a la Nube, por lo que tendremos cuatro modelos de Nube que son los más comúnmente utilizados en las organizaciones y que podremos observar en la ***Tabla 6 - Tipos de Nube***

Tabla 6 - Tipos de Nube

Nube pública	Es una red abierta para uso público en la cual se ofrece el servicio de computación y almacenamiento a todos los clientes externos que precisan de esta tecnología en Internet. Se usan para dar soporte a quienes buscan reducir los costes y aumentar las opciones de tecnologías, a veces incluso de forma gratuita. No obstante, en lo que respecta a la seguridad, los proveedores de servicios en la Nube pública poseen y operan la infraestructura en su centro de datos y el acceso es a través de Internet, ofreciendo servicios de conexión directa que requieren que los clientes compren o arrenden una conexión privada a un punto de intercambio ofrecido por el proveedor de la Nube.
Nube privada	Permite centralizar el acceso a los recursos de *TI* de la organización, utilizando una tecnología de Nube propia. La gestión de este entorno puede llevarla a cabo la misma compañía o subcontratarlo a terceros. A pesar de que la Nube privada

	puede residir físicamente en las instalaciones de la organización, los recursos de *TI* que alberga todavía se consideran basados en el *Cloud*, por ser accesibles de forma remota por los usuarios.
Nube híbrida	Este modelo varía en función de las necesidades del negocio, resulta de la combinación de una Nube privada y una pública o de alguna de ellas y una comunitaria. De la misma forma, también coexisten diferentes proveedores de servicios de Nube. Los requisitos de cumplimiento de la industria y las prioridades que cada organización establezca en materia de seguridad de la información marcarán la configuración y los usos que decidan dar a la Nube.
Nube de comunidad	Esta interpretación se asemeja bastante a la Nube pública con la diferencia de que, el acceso queda limitado a una comunidad específica, o algunos de sus miembros, que deben definir las reglas y encargarse de su desarrollo.

Fuente: (PowerData, 2019)

Son pocas las organizaciones que dentro de la esfera pública o privada no hacen uso en alguna medida de la Computación en la Nube para el almacenamiento de su información. Por el contrario, muchas de las empresas han realizado grandes inversiones en su infraestructura actual para ser utilizadas en modelos basados en la Nube.

La naturaleza centralizada de la Computación en la Nube dificulta el procesamiento de datos recopilados desde el borde de la red de manera rápida y efectiva. Sin embargo, lo que le falta a la Nube en velocidad lo compensa en potencia y capacidad. Dado que la Computación en la Nube se basa en una infraestructura del centro de datos escalable, puede ampliar su capacidad de almacenamiento y procesamiento según sea necesario. Esta escalabilidad es un gran beneficio para las pequeñas empresas que buscan expandirse rápidamente.

Las organizaciones han tomado la decisión de utilizar servicios basados en la Nube para poder minimizar sus costos de operación en sus centros de datos de manera local, enfocando parte de su operación a los modelos de *SaaS* (por sus siglas en inglés *Software as a Service*), *IaaS* (por sus siglas en inglés *Infraestructure as a Service)* y *PaaS* (por sus siglas en inglés *Plataform as a Service)* como los modelos principalmente utilizados en la Nube tal como podemos observar en la ***Tabla 7 - Modelos de servicios en la Nube*** (Equipo Editorial Reporte Digital, 2019).

Tabla 7 - Modelos de servicios en la Nube

SaaS	El software como servicio es el lugar donde una parte del software está alojada por un tercero y se puede acceder a través de la web, normalmente solo iniciando sesión, y generalmente se cobra por suscripción o por usuario. Esto difiere del antiguo modelo de compra e instalación de software en una máquina o servidor de forma manual.
IaaS	La infraestructura como servicio es un tercero que proporciona una infraestructura de *TI* altamente automatizada y escalable (almacenamiento, alojamiento, computación, redes) y solo realiza cargos por lo que se usa. Por lo tanto, en lugar de poseer activos como licencias de software o servidores, las empresas pueden alquilar recursos de forma flexible de acuerdo con sus necesidades.
PaaS	La plataforma como servicio es proporcionar todos los conceptos básicos de *IaaS*, así como las herramientas y capacidades necesarias para desarrollar e implementar aplicaciones de forma segura.

Fuente: (Carey, 2018)

De acuerdo con PowerData, (2019) un indicio de los resultados que se obtienen gracias a la implementación de la Computación en la Nube son:

- La reducción de tiempo en la aparición de nuevos productos y servicios.
- La mejora en la sincronización entre las unidades de negocio.

- Un servicio al cliente de manera optimizada.
- Reducción de costos de mantenimiento de *TI*.
- Oferta de servicios de computación, almacenamiento, redes *Big Data*, aprendizaje automático e *IoT*.
- Herramientas de gestión, seguridad y desarrollo en la Nube.

La Computación en la Nube seguirá siendo un recurso valioso para las infraestructuras de centros de datos más tradicionales. Si bien los dispositivos *IoT* representan una nueva y emocionante frontera en la industria tecnológica, no todas las empresas verán muchos beneficios al trasladar sus activos al borde de la red.

1.3.2.1 Desventajas de la Nube

Con la velocidad, la eficiencia y las innovaciones actuales en tecnología que se proporcionan con la Computación en la Nube, claramente se tienen riesgos inherentes a la misma operación de trabajar con la Nube en las organizaciones.

La seguridad siempre será una constante preocupación para todas las organizaciones que tengan instaladas soluciones en la Nube, especialmente si se trata de información sensible como son los datos financieros de las organizaciones. Si bien las regulaciones legislativas obligan a las empresas que brindan los servicios de Computación en la Nube a reforzar sus medidas de seguridad y a su cumplimiento estricto, sigue siendo un problema latente y continuo. Sin embargo, a pesar de que el cifrado protege la información vital de las organizaciones, el hecho de perder la clave de cifrado, implica un grave riesgo para los datos de las organizaciones.

Los servidores que son mantenidos por las empresas de servicios de Computación en la Nube, también pueden ser susceptibles a los desastres naturales, errores internos y a los cortes de energía. Por lo cual el alcance geográfico de la Computación en la Nube se corta en ambos sentidos: por ejemplo, un apagón en

California, podría afectar seriamente a los usuarios de Nueva York y paralizar todas sus operaciones por un largo periodo de tiempo.

Como con cualquier tecnología, hay una curva de aprendizaje tanto para los empleados como para los gerentes. Pero con muchas personas que acceden y manipulan la información a través de un solo portal, los errores involuntarios pueden transferirse a todo un sistema.

1.3.3 Computación al Borde (*Edge Computing*).

Internet es uno de los componentes clave al realizar una implementación de cualquier arquitectura informática, en su forma más simple, las aplicaciones Cliente-Servidor, nos hacen recordar la arquitectura basada en mainframe de los años 50´s los cuales son un claro ejemplo de lo que es el cómputo centralizado.

El Internet es también la plataforma para arquitecturas complejas Cliente-Servidor de ***"n"*** niveles, en donde el Internet actúa simplemente como una pasarela que dirige las solicitudes del cliente a los objetos de negocio apropiados y a su vez transmite a estos las respuestas de vuelta hacia los navegadores web. Esta arquitectura es similar a cualquier otra arquitectura de ***"n"*** niveles, en el sentido de que la lógica de negocio de la aplicación está separada en un conjunto de objetos de negocio que pueden reutilizarse de una aplicación a otra (Bjeletich & Mable, et al., 1999, págs. 8-9).

La Computación al Borde mejor conocida como *Edge Computing*, es diametralmente opuesta al concepto del cómputo en la Nube. A diferencia de la Nube en donde los recursos de almacenamiento se encuentran en centros de datos ubicados en cualquier parte del mundo y que en realidad son propiedad del proveedor de la misma. En la Computación al Borde, el almacenamiento y los recursos que son necesarios para las aplicaciones, se encuentran ubicados cerca del usuario que requiere la información o de la fuente que genera los datos (Panduit, Inc., 2018).

La Computación al Borde, es básicamente una arquitectura que implementa un sistema de red el cual procura reunir, analizar y procesar datos de distintos dispositivos de una forma más eficiente que la arquitectura usada en la Nube. Tiene como objetivo principal la reducción de los datos que se envían a la Nube y disminuir los tiempos de latencia en la red y de Internet, para a su vez mejorar el tiempo de respuesta del sistema a las aplicaciones remotas y de misión crítica (Panduit, Inc., 2018).

La Computación al Borde es un concepto relativamente nuevo debido a que comenzó a hablarse del mismo hasta hace unos pocos años de manera constante. En la realidad la Computación al Borde está llevando un centro de datos con capacidades reducidas de espacio, pero con alto desempeño del procesamiento de información al lugar más cercano de la organización en donde se generan los datos. En él se encontrarían conectados los dispositivos de *IoT* que por sus características de desempeño y de latencia requieren de una respuesta rápida.

El *IoT* toma una gran ventaja de la Computación al Borde por su desempeño y funcionalidad, ya que a pesar de tener un periodo de latencia muy reducido; a diferencia de la Computación en la Nube, para la Computación al Borde este periodo de latencia es prácticamente cero. Por lo que se realiza un uso más eficiente en el procesamiento de los datos generados al reducir los tiempos de respuesta en los datos enviados a los servidores centrales en tiempo real y que son necesarios para la analítica de los mismos (Rittal, 2018).

A medida que los dispositivos del *IoT* se vuelven más comunes e incorporan más potencia de procesamiento, se genera una gran cantidad de datos en el "borde" externo de las redes informáticas. Tradicionalmente, los datos producidos por los dispositivos *IoT* se transmiten a un servidor de red central, generalmente alojado en un centro de datos. Una vez que se procesan esos datos, se envían más instrucciones a los dispositivos en el borde de la red.

Hay dos problemas con esta configuración:

- Primero, los datos tardan en viajar desde el dispositivo de borde de regreso al centro de datos para su procesamiento. Este retraso puede ser solo una cuestión de milisegundos, pero puede ser crítico.
- En segundo lugar, todos esos datos que viajan de un lado a otro entre el borde y el centro de datos de la red ejercen una enorme presión sobre el ancho de banda.

Esta combinación de distancia y tráfico de gran volumen puede ralentizar la red de manera sensible y por ende ocasionar problemas de transmisión de datos y retrasos significativos.

La Computación al Borde ofrece una solución al problema de latencia al reubicar el procesamiento de datos cruciales al borde de la red. En lugar de entregar constantemente datos a un servidor central, los dispositivos con capacidad perimetral pueden recopilar y procesar datos en tiempo real, lo que les permite responder de manera más rápida y efectiva.

Cuando se usa junto con los centros de datos de borde, la computación de borde es un enfoque versátil para la infraestructura de red que aprovecha la abundante potencia de procesamiento que ofrece la combinación de dispositivos *IoT* modernos y centros de datos de borde.

Para poder realizar una implementación efectiva de una solución de la Computación al Borde, se requiere de la identificación de las aplicaciones que necesitan prioridad en recibir respuestas en tiempo real, como es el caso del *IoT*, el resto de las aplicaciones pueden operar y funcionar adecuadamente desde soluciones basadas en centros de datos propietarios de la organización o en soluciones basadas en la Nube como podemos observar en la ***Ilustración 3 - Tiempo real desde la Nube.***

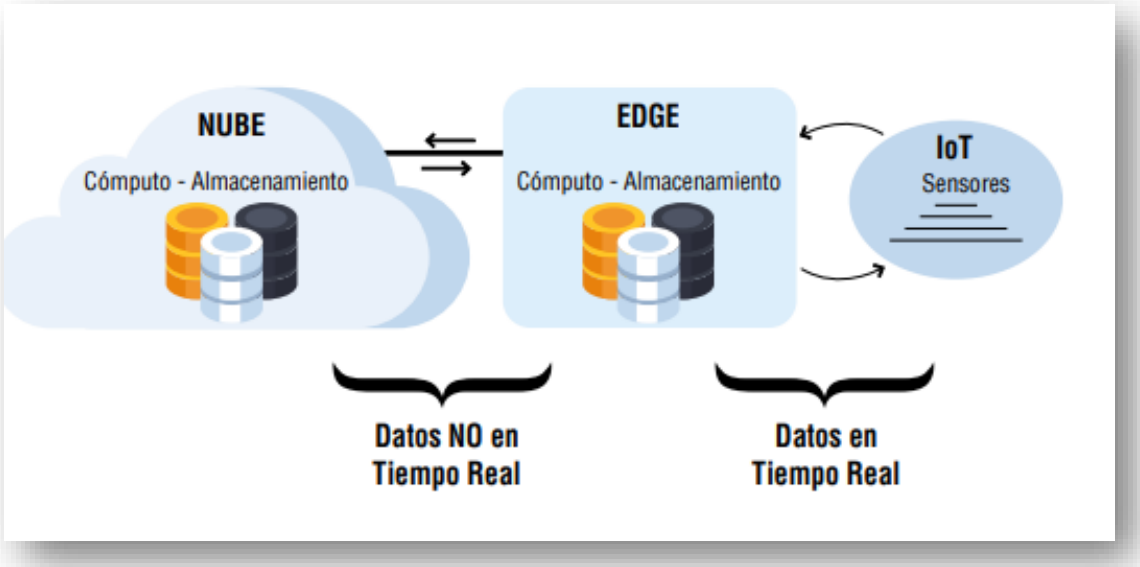

Ilustración 3 - Tiempo real desde la Nube
Fuente: (Panduit, Inc., 2018)

Dado que el aumento de los dispositivos que se conectan a la Nube han generado una saturación de las redes inalámbricas y de toda la infraestructura que se encuentra actualmente instalada en las organizaciones, la aparición de la Computación al Borde proporciona a las organizaciones un medio que les permite a los diversos dispositivos móviles, cámaras de video vigilancia, sensores, etcétera, reaccionar de una forma más rápida.

Lo que evita la necesidad de realizar una transmisión masiva de datos hacia la Nube debido ya que los mismos podrán ser procesados en forma local, y a su vez centralizar, consolidar y transmitir la información estadística o en su caso disparar alertas que requieren atención inmediata de una forma más eficiente y así tener una reducción del flujo de transmisión de datos, derivado de que solo se enviarían los datos consolidados para posteriormente ser analizados por parte del área indicada y así tomar las decisiones pertinentes.

1.3.4 Ciberseguridad.

En la actualidad muchas de las actividades que se realizan de forma cotidiana dentro de las organizaciones están basadas en la transmisión de datos por medio de sus redes corporativas que a su vez se encuentran conectadas a Internet. El crecimiento que se ha tenido de Internet en la última década, ha propiciado la aparición de múltiples servicios telemáticos, como son: el comercio electrónico, servicios de multimedia de banda ancha, administración electrónica, videoconferencias, sistemas de video vigilancia, solo por mencionar algunas de ellas.

Para Gómez Vieites, (2014) los servicios críticos que se utilizan dentro de una sociedad moderna en diversos sectores como son, por ejemplo: los servicios financieros, el control de la producción y el suministro eléctrico (centrales eléctricas, redes de distribución y transformación), medios de transporte (control de tráfico aéreo, control de vías terrestres y marítimas), la sanidad (historial clínico informatizado, telemedicina), las redes de abastecimiento (agua, gas y saneamiento) o la propia administración pública están soportados en su totalidad por sistemas y redes informáticas.

Define la seguridad informática como:

> "C*ualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema*" (Gómez Vieites, 2014, pág. 38).

La ciberseguridad es una práctica de la seguridad informática que se encarga de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se le conoce

como seguridad de tecnología de la información o seguridad de la información electrónica. Al tratarse de un término muy amplio, este se puede aplicar a numerosos elementos que van desde la seguridad informática hasta la recuperación ante desastres (Kaspersky, 2019).

El rápido crecimiento de manera exponencial de las nuevas tecnologías que utilizan como vía de comunicación la red de Internet, han propiciado que el incremento de las tendencias tecnológicas sea todo un reto para la seguridad informática, con iniciativas empresariales para reducir gastos como el "traiga usted su propio equipo" (*BYOD*[21], por sus siglas en inglés *Bring Your Own Device*) y el *IoT*, que han propiciado una rápida adopción de aplicaciones y cargas de trabajo basadas en la Nube y que extienden las necesidades de seguridad informática más allá de los límites del centro de datos tradicional (Palo Alto Networks, Inc., Cyberpedia, 2019).

La función principal de la ciberseguridad es la protección de los sistemas informáticos y la información de las principales amenazas informáticas, las cuales pueden tener su origen de diversas formas como son: ataques de aplicaciones, *malware*, *ransomware*, *phishing*, kits de explotación, entre otros. Sin embargo, mantener una estrategia en las operaciones de seguridad en la actualidad puede ser todo un desafío, especialmente en las redes gubernamentales y empresariales en donde las amenazas cibernéticas son cada vez más frecuentes y sofisticadas (Palo Alto Networks, Inc., Cyberpedia, 2019).

Dentro de la seguridad informática, tenemos la clasificación de los tipos más comunes de ciberseguridad los cuales se describen con más detalle en la ***Tabla 8 - Tipos de ciberseguridad.*** En donde podremos observar las formas de protección más comunes que existen en la actualidad para la seguridad de la información.

[21] Véase (Lavin, 2013)

Tabla 8 - Tipos de ciberseguridad

Network Security	Protegen el tráfico de la red al controlar las conexiones entrantes y salientes para evitar que las amenazas ingresen o se propaguen en la red.
Prevención de pérdida de datos (DLP)	Protegen los datos al enfocarse en la ubicación, clasificación y monitoreo de la información en reposo, en uso y en movimiento.
Cloud Security	Proporciona protección para los datos utilizados en servicios y aplicaciones basados en la Nube.
Sistemas de detección de intrusos (IDS) / Sistemas de prevención de intrusos (IPS)	Trabajan para identificar la actividad cibernética potencialmente hostil.
Administración de Identidad y Acceso (IAM)	Utiliza los servicios de autenticación para limitar y rastrear el acceso de los empleados para proteger los sistemas internos de las entidades maliciosas.
Cifrado	Proceso de codificación de datos para que sea ininteligible, se utiliza durante la transferencia de datos para evitar el robo en tránsito.
Soluciones antivirus / antimalware	Analizan los sistemas informáticos en busca de amenazas conocidas.

Fuente: (Forcepoint, 2019)

1.3.5 Internet de las cosas (*Internet of Things*, *IoT*)

En la última década comenzó a surgir el termino de *Internet of Things* (*IoT*) cuando Kevin Asthon, quien era profesor del *Massachusetts Institute of Technology* (MIT)

de forma publica la utilizo por primera vez en 2009[22]. Es en ese momento cuando Ashton publica en el *RFID journal* el concepto, a pesar de que era un término de uso corriente desde finales de la década de los 90´s, en los últimos años ha tenido un crecimiento ampliamente aceptado dentro de las organizaciones por su facilidad de integración con los centros de datos y la administración centralizada de diversos dispositivos que conforman el *IoT*.

El *IoT* tiene la finalidad de proporcionar a los dispositivos físicos la capacidad de transmitir datos utilizando la red de Internet, mediante el uso de sensores que son interconectados a los dispositivos que a su vez son conectados a la red de comunicaciones de datos, utilizando un medio de transmisión de información principalmente radiofrecuencia, WiFi o mediante la conexión a la red de datos, lo que permite realizar la administración y control de una forma remota de una amplia gama de dispositivos.

Tomando en consideración la definición anterior, podemos precisar que el *IoT* es la conexión de dispositivos de uso cotidiano a los cuales se les incorpora un medio de transmisión de datos informáticos para poder tener un medio de comunicación, que les permita el envío y recepción de datos mediante una conexión a Internet. Permitiéndoles la funcionalidad de controlar, monitorear y administrar información a miles de millones de dispositivos físicos que se encuentran en todo el mundo.

Como podemos observar en el esquema mostrado en la ***Ilustración 4 - Internet of Things (IoT).***, la posibilidad de conexión de casi cualquier dispositivo es posible gracias a la incorporación de los medios de transmisión y de conexión que se realizan en la fabricación de dichos dispositivos y que le da origen a la *IoT* . Por lo que cualquier dispositivo analógico es factible de ser modificado mediante sensores

[22] Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiera saberse de cualquier cosa –usando datos recolectados sin intervención humana- seriamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante los costes y malos usos. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El Internet de las Cosas tiene el potencial de cambiar el mundo como ya lo hizo Internet, o incluso más (Cendón, 2017).

que hacen la conversión a datos digitales que permitan su monitoreo, administración y generación de datos estadísticos que son útiles para las organizaciones al incorporarlos en sus redes corporativas.

El *IoT*, nos permite la interconexión de una amplia gama de dispositivos que pueden ser controlados mediante una conexión de Internet, o por medio del cableado estructurado ya sea de forma alámbrica o por medio del WiFi de la organización que requiera el uso de las mismas.

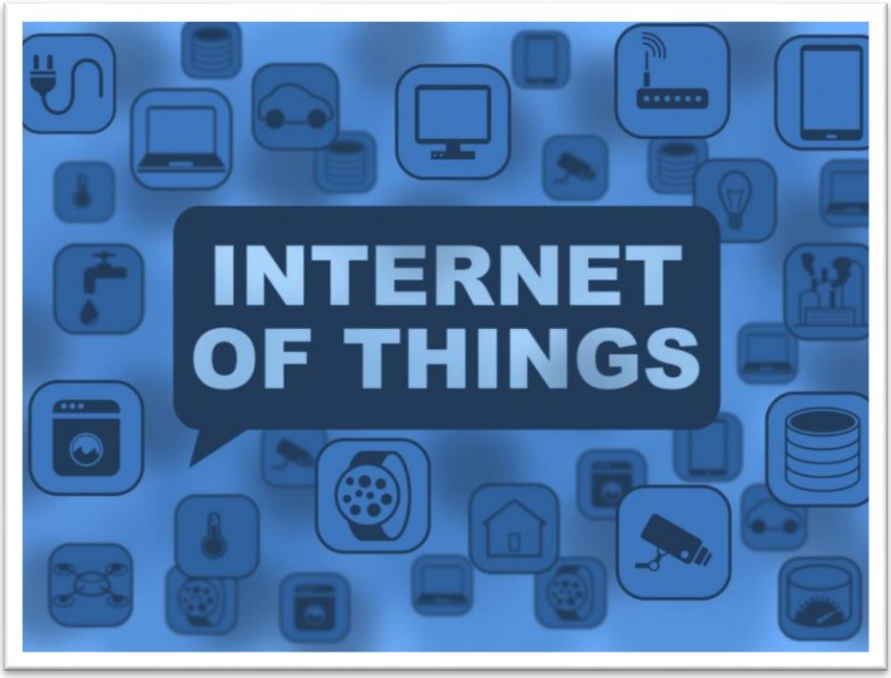

Ilustración 4 - Internet of Things (IoT).
Fuente: *(Tilves, 2019)*

Sin embargo, es a principios de la década de los 90´s, cuando comienza a surgir un concepto innovador en la industria, los edificios inteligentes[23]. Pero, ¿Cómo podemos definir que un edificio es inteligente? Un edificio es considerado inteligente, cuando ha sido dotado de tecnología la cual le permite al personal de sistemas, controlar de forma remota por medio de sensores varios dispositivos que se encuentran automatizados; mediante los diversos sistemas de administración de cómputo existente de una forma eficiente.

[23] Véase (Domótica Integrada, 2018)

Una de sus propiedades fundamentales es la de personalizar las características de funcionamiento de diversas formas, como pueden ser presencia, horarios, horas de mayor carga de trabajo, etcétera; lo cual nos permite un control eficiente de los recursos para optimizar tiempo y dinero. De igual forma permite administrar los sistemas de seguridad y sustentabilidad de la infraestructura instalada en el edificio de una forma confortable. (Lamudi, 2017).

Dentro de las características que podemos encontrar en un edificio inteligente y que nos permiten realizar de manera eficiente la administración de una gran cantidad de diversos rubros se encuentran:

- Sistema de control de clima.
- Sistemas de control y eficiencia de iluminación eléctrica.
- Sistemas de control y eficiencia de elevadores y puertas.
- Circuito Cerrado de Televisión (CCTV).
- Sistemas de control de acceso.
- Administración inteligente de recursos.
- Sistema centralizado para procesar datos.
- Automatización de áreas de trabajo.
- Sistemas de detección de humo y alarma de intrusión (Lamudi, 2017)

Sin embargo, dentro de la industria podremos encontrar otro tipo de rubros en los cuales el *IoT* encuentra una gran diversidad de usos como pueden ser: manejo de maquinaria, control de automatización de procesos, control de robots de forma automatizada, sistemas de posicionamiento de robots para distribución de equipos y materiales.

Es en la década de los 90´s cuando se da el "*boom*" del Internet comercial, cuando el *IoT*, encuentra los parámetros necesarios para poder crecer a pasos agigantados. Las empresas y principalmente las industrias se han visto beneficiadas en diversos

rubros entre los cuales el Internet es fundamental para poder llevar a cabo la automatización y control de áreas que anteriormente se realizaban de forma manual o independiente.

Pero esto implicaba centralizar en un área específica los equipos de control y procesamiento de la información y es cuando la industria comienza a incorporar en los centros de datos ya existentes las diversas tecnologías que anteriormente se encontraban instaladas de formas independientes.

Craig Resnick, Vicepresidente de *ARC Advisory Group* (2018) nos comenta en relación al *IoT* de la evolución que existe dentro de las organizaciones acerca de la implementación del *IoT* y de las necesidades que requieren acerca del procesamiento de la información que se genera de los dispositivos industriales, maquinaria, controladores y sensores.

> *IoT está evolucionando la forma en la que las organizaciones crean, recaban y analizan datos, pues IoT extiende los límites de dispositivos industriales, máquinas, controladores y sensores. Edge Computing y la analítica se ubican cerca de máquinas y fuentes de datos, haciendo posible que la información se genere más rápido y en volúmenes nunca antes vistos* (Panduit, Inc., 2018)**.**

Las tecnologías emergentes, han cambiado la forma en que los centros de datos de las organizaciones han tenido que realizar ajustes en su infraestructura y formas de operación, por lo cual su implementación requiere de un mayor análisis de las consecuencias que implican su utilización en un centro de datos en las organizaciones cuando los mismos tienen más de cinco años de antigüedad.

2 Capítulo II – Las Tecnologías emergentes y las organizaciones

2.1 El centro de datos y las organizaciones

Los centros de datos son la parte neurálgica de las organizaciones, por lo cual suelen ser instalaciones industriales muy especializadas que se encuentran llenas de equipos y sistemas complicados e interrelacionados con necesidades críticas de la empresa. Los centros de datos se pueden definir como tres infraestructuras paralelas: *TI*, electricidad y refrigeración. Las tres infraestructuras tienen que ser perfectamente compatibles y estar armonizadas para lograr el funcionamiento perfecto de una instalación critica.

La electricidad y la refrigeración son las dos infraestructuras necesarias para que funcionen los equipos de *TI*. La electricidad procede principalmente de la red y la alimentación eléctrica de los equipos de *TI* se hace por medio de topologías complejas de transformadores, sistemas de alimentación ininterrumpida (*UPS*), barras de bus y conmutadores de transferencia automáticos. La electricidad bruta suministrada por la compañía se transforma, convierte, acondiciona y distribuye a los servidores en los gabinetes de *TI*.

Las necesidades de un mundo globalizado y el tráfico de red, han marcado la pauta para la modernización de los centros de datos y la forma en la cual se realizan los procesos de diseño de los mismos. En la última década, seguíamos trabajando con las normas del cableado estructurado[24], mismas que no tomaban en consideración las nuevas tecnologías y con velocidades de transmisión de un Gigabit/segundo (Gb/s) de transmisión de datos en el ancho de banda.

Sin embargo, con la aparición de más dispositivos de *IoT* y el problema de la centralización del centro de datos, las organizaciones han tenido que realizar cambios substanciales en la forma de mejorar el desempeño de sus centros de datos.

[24] Véase Estándares, certificaciones y documentos relacionados.

En la actualidad podemos tener velocidades de hasta 400 Gigabit/segundo (Gb/s) de transmisión en el ancho de banda, lo que ha forzado a que las normas del centro de datos específicamente la norma EIA/TIA 942-B[25], sufriera modificaciones importantes para poder incorporar a su estándar las nuevas tecnologías y presentan un marco de referencia con el que se brinda apoyo a la industria para hacer modificaciones en los centros de datos y adaptarse rápidamente a las nuevas tecnologías que se han presentado en los últimos años y que marcaran la pauta a seguir dentro del ámbito de las telecomunicaciones.

Las organizaciones desde hace décadas han buscado la forma de hacer más eficientes y productivos sus procesos operativos y administrativos. Por lo que han buscado la manera de realizar implementaciones en sus cadenas de producción, administración y encontrar la forma de minimizar los costos operativos para tales fines.

La aparición de los sistemas de cómputo en la década de los 50´s con los mainframes[26] comienzan a dar un esbozo de las necesidades de las organizaciones de centralizar su información generada, para así poder realizar procesos matemáticos, administrativos y de análisis estadístico de una manera automatizada, eficiente y precisa.

Dando paso a la aparición de aplicaciones Cliente-Servidor permitiendo a las computadoras tener un papel primordial en las aplicaciones comerciales para las organizaciones. En la actualidad para tener centros de datos de manera centralizada, se requiere unificar el almacenamiento de información en un solo sitio

[25] Véase anexo I – Principales estándares del cableado estructurado sección: ANSI/TIA 942-A Estándar de Infraestructura de Telecomunicaciones para Centros de *Datos (Telecommunications Infraestructure Standard for* Data **Centers).**

[26] Véase (Espeso, 2014)

ubicado en un área estratégica de la organización, mediante controles de seguridad de una manera adecuada lo que se le conoce como centro de datos o *datacenter*.

Para Frost & Sullivan, (2018) en su artículo titulado: **"*La LAN Moderna: reconsiderando el diseño de redes para la era moderna*"**:

> *Los procesos en el diseño de las redes tradicionales se encuentran atrapados en un mundo cerrado el cual se encuentra centralizado en las PC ´s, lo cual coloca a los sistemas inteligentes en un riesgo latente de las amenazas cibernéticas importantes y de una administración medio ambiental deficiente, además de tener un impacto negativo dentro de los resultados de las empresas. Las redes de área local (LAN, por sus siglas en inglés Local Area Network) son consideradas el centro neurálgico de la mayoría de las empresas en la actualidad, lo que ofrece aplicaciones y comunicaciones que son consideradas de misión crítica para los usuarios finales de la organización.* (Frost & Sullivan, 2018)

Las organizaciones deben confiar plenamente en su infraestructura instalada de redes de datos corporativa, para operar todas las facetas de sus operaciones, con dispositivos inteligentes conectados que reemplazan todo, desde los teléfonos en los escritorios de los empleados hasta las cámaras y los sensores que aseguran sus instalaciones.

En la actualidad los sistemas inteligentes requieren de una red que sea más inteligente que las redes de datos tradicionales, basadas en un conjunto de mejores prácticas fundamentales que reflejen estas nuevas plataformas y los dispositivos inteligentes que cada vez son más asequibles para las empresas ya que sus requerimientos de implementación representan un desafío para los administradores de redes en las organizaciones.

Las arquitecturas de redes que se encuentran basadas en la funcionalidad de las PC ´s, requieren de una cantidad de ancho de banda cada vez mayor para poder garantizar el rendimiento adecuado de las aplicaciones empresariales básicas y así mejorar el desempeño y funcionalidad de los equipos de escritorio para los usuarios finales. Además, los requerimientos actuales de las comunicaciones en tiempo real, como lo son Voz sobre *IP* (*VoIP*, por sus siglas en inglés *Voice over IP*), sistemas de videoconferencia y video vigilancia, que han migrado de su propia infraestructura hacia los centros de datos aprovechando el Protocolo de Internet (*IP*).

Las prácticas de diseño de manera tradicional de las redes de área local (*LAN*, por sus siglas en ingles *Local Area Network*), las cuáles se encuentran basadas en una infraestructura de red homogénea y suposiciones de requerimientos de ancho de banda, están creando una serie de desafíos para las organizaciones en la medida que las mismas están incorporando a sus centros de datos corporativos un amplio conjunto de dispositivos o puntos finales dentro de sus centros de datos. Los cuales representan un factor de riesgo si no se implementan correctamente; pero adicionalmente a esto, se tiene el factor de que los fabricantes no han realizado a la fecha actualizaciones importantes en cuestiones de seguridad dentro de sus dispositivos lo que representará en un futuro uno de los principales retos que deberá cubrir la industria del *IoT*.

La conectividad de la red de datos de las organizaciones, requiere del uso de un gran ancho de banda, mismo que se ve limitado por las normas del cableado estructurado[27] específicamente por la norma EIA/TIA 568[28], la cual limita la distancia del cable instalado a solo 100 metros lineales entre los dispositivos de la red. Por lo que se requiere de la instalación de cuartos de cableado intermedio (*IDF*, por sus siglas en inglés *Indeterminate Distribution Frame*), mismos que proporcionan un

[27] Véase capítulo I Sección: Estándares, certificaciones y documentos relacionados.

[28] Véase anexo I – Principales estándares del cableado estructurado sección: Estándar ANSI/TIA/568-C.0.
Cableado genérico de telecomunicaciones para las instalaciones del cliente *(Generic Telecommunications Cabling for Customer Premises*)

punto de unión entre los switches de red y el cableado hacia los distintos dispositivos de red cercanos.

En una arquitectura de red instalada de forma tradicional centrada en PC ´s, todo el cableado estructurado puede planificarse o instalarse dentro de los cubículos de las oficinas de la organización. Sin embargo, esto se convierte en una barrera importante cuando la organización cuenta con puntos adicionales de conexión, como son: teléfonos *VoIP*, cámaras de seguridad o sensores de edificio inteligente/*IoT*. Ya que estos dispositivos se encuentran normalmente fuera del alcance del personal para evitar manipulaciones a los mismos y se encuentran ubicados en toda la instalación de la organización. Por lo que a menudo superan las distancias límites del cableado estructurado basado en *Ethernet*, por lo que las organizaciones requieren de la instalación de cuartos de interconexión intermedios para poder funcionar sin problemas (Frost & Sullivan, 2018)**.**

2.2 La Inteligencia Artificial y las innovaciones

Es gracias a los modelos matemáticos de Alan Turing, que la Inteligencia Artificial y la computación comienzan a sentar las bases de lo que actualmente inspiro a las computadoras modernas. Por eso es considerado como el padre de la computación y fundador de la *IA*, con el desarrollo de la Maquina de Turing que fue pieza clave para descifrar los códigos de la maquina Enigma en la segunda guerra mundial (Historia y Vida, 2018).

Para Pérez Orozco, (2018) en su publicación de la oficina de información científica y tecnológica para el congreso de la unión titulada: **“Inteligencia Artificial”**:

> *La Inteligencia Artificial (IA) tiene profundas consecuencias sociales, económicas, educativas y legales las cuales aumentaran en los próximos años; debido a su aplicación en diversos sectores, por ejemplo: posibilita el desarrollo de automóviles autónomos, revoluciona el diagnóstico y tratamiento de enfermedades, con el*

> *análisis de grandes cantidades de información médica y facilita el proceso educativo, al dar asesoría personalizada de forma automática a estudiantes de todos los niveles educativos* (Pérez Orozco , 2018)

El concepto de *IA* se utiliza básicamente cuando una máquina es capaz de imitar las funciones cognitivas de la mente humana, como son: creatividad, sensibilidad, aprendizaje, entendimiento, percepción del medio ambiente y uso del lenguaje. Por eso son muy importantes los avances tecnológicos y modelos matemáticos que fueron desarrollados y aplicados por Alan Turing.

Dentro del campo de la *IA*, que ha tenido un gran auge en los últimos años, podemos encontrar el aprendizaje computacional o mejor conocido como *Machine Learning*[29]*,* en el cual un sistema aprende a ejecutar tareas ya sea mediante ejemplos o por prueba y error. También tenemos los modelos llamados redes neuronales, los cuales están inspirados en el funcionamiento de las neuronas cerebrales de una manera simplificada. Las cuales han sido muy exitosas en la aplicación de tareas de alta complejidad como son: la identificación de objetos en imágenes y el reconocimiento del habla humana (Pérez Orozco , 2018).

En los últimos años, el campo de la *IA* y sus aplicaciones han crecido a gran velocidad, debido a tres detonadores principalmente, que son:

- El desarrollo de algoritmos y circuitos electrónicos especializados (los cuales cuentan con mayores capacidades de procesamiento de datos).
- El crecimiento de los datos disponibles.
- El aumento en recursos humanos y financieros que se han destinado para su desarrollo.

[29] Véase (Iberdrola, 2019)

Con lo cual se han podido realizar desarrollos y aplicaciones diversos, que se pueden aplicar en una amplia gama de rubros como podemos observar en la ***Tabla 9 - Aplicaciones de la Inteligencia Artificial***.

Tabla 9 - Aplicaciones de la Inteligencia Artificial

Reconocimiento visual	Sistemas capaces de reconocer y rastrear objetos y personas en imágenes y video.
Reconocimiento del lenguaje natural	Sistemas capaces de reconocer, reproducir de modo artificial y descifrar el significado del lenguaje hablado. Incluyendo también la traducción automática entre diferentes idiomas, así como respuestas automáticas de preguntas y el análisis y síntesis de documentos.
Estrategia y planeación	Sistemas capaces de generar estrategias optimizadas para resolver problemas de gran complejidad y a largo plazo. Algunos ejemplos son los sistemas autómatas, capaces de apoyar tareas de logística y manufactura, jugar videojuegos o navegar a través de espacios físicos.
Diagnóstico y apoyo en la toma de decisiones	Sistemas capaces de analizar problemas complejos y ayudar a tomar decisiones, por ejemplo, en medicina, en la detección de enfermedades o la elección del tratamiento más adecuado. Incluye también el análisis de datos para agilizar el desarrollo de medicamentos.
Colaboración humano-computadora	Consiste en incorporar sistemas inteligentes como parte de equipos de trabajo humanos. Por ejemplo, para responder más ágilmente a desastres naturales, se han desarrollado sistemas que pueden analizar vistas aéreas de las zonas afectadas donde se requiere mayor apoyo.

Fuente: (Pérez Orozco , 2018)

La *IA* ha evolucionado de tal manera en los últimos años, que por primera vez un Robot computacional (comúnmente llamado *Bot*) llamado *Eugene Goostman* en el

año 2014, fue capaz de lograr engañar a 30 de 150 jueces a los que se sometió al realizar el Test de Turing, haciéndoles creer que estaban hablando con un niño ucraniano de 13 años de edad. Siendo un parteaguas que marca un antes y un después para la *IA* (HojadeRouter.com, 2014)

La *IA* ha impactado profundamente en la sociedad y en las organizaciones en diversas áreas de aplicación cada vez con nuevos e innovadores desarrollos como podemos ver en la tabla ***Tabla 10 - Implicaciones sociales de la Inteligencia Artificial.***

Tabla 10 - Implicaciones sociales de la Inteligencia Artificial

Sector productivo	Las oficinas gerenciales incorporan métodos automáticos para la toma de decisiones.
Manufactura	Se utilizan robots con capacidades de desplazamiento y localización de objetos.
Agricultura	Se desarrollan tecnologías para diagnosticar oportunamente enfermedades de las cosechas; así como sistemas de vigilancia de suelo, utilizando sensores, imágenes satelitales y registros históricos para predecir la productividad de los plantíos; sin embargo debido a su alto costo, solo son accesibles para grandes empresas en la actualidad.
Salud	Sistemas inteligentes, sensores de bajo costo y ambientes virtuales están transformando la prevención, el diagnóstico y el tratamiento de enfermedades de alto riesgo como el cáncer, obesidad, hipertensión y diabetes. Por ejemplo, en la prevención, algunas aplicaciones móviles permiten utilizar los sensores del teléfono celular para vigilar la cantidad de azúcar ingerida y el ritmo cardiaco del usuario. Gracias a su bajo costo, estas tecnologías pueden llevarse a zonas rurales, incrementando la cobertura y evitando el gasto de traslado de pacientes. Por otro lado, el uso de ambientes virtuales pude cambiar el tratamiento

	y la rehabilitación de padecimientos motrices o cognitivos que requieren ejercicios físicos o mentales.
Educación	Actualmente ya hay sistemas inteligentes capaces de dar asesoría personalizada a cada alumno en reportes y ensayos, lo cual permite a los profesores identificar áreas de oportunidad con mayor eficacia. Asimismo, ha crecido el número de plataformas que ofrecen tutorías por Internet para todos los grados educativos
Seguridad	Se pueden analizar eficientemente días enteros de grabación de cámaras de seguridad de circuito cerrado, así como rastrear la ubicación de los individuos. También se podrían emplear sistemas inteligentes en drones para detectar actividades criminales, aunque este uso es controvertido, ya que suscita preocupaciones sobre el control que el gobierno podría ejercer sobre la población y su privacidad.

Fuente: (Pérez Orozco , 2018)

En los ámbitos éticos y legales se debaten las asignaciones de responsabilidades y obligaciones en situaciones en donde intervienen sistemas inteligentes. En consecuencia, los desarrolladores de sistemas inteligentes, tienen la responsabilidad de cumplir con estándares internacionales que aseguren la transparencia y confiabilidad de los sistemas inteligentes que hacen uso de la *IA*. Debido a que los sistemas inteligentes, pueden aprender prejuicios desde los datos mismos como son las asociaciones de genero para ciertos rubros profesionales. Para poder prevenir que los sistemas hereden tantos prejuicios y a su vez representen al grueso de la población, se hacen esfuerzos para que exista igualdad de género entre los desarrolladores (Pérez Orozco , 2018).

2.3 La Seguridad Informática y el Internet de las cosas (*IoT*)

Es derivado de la incorporación de los diversos dispositivos que se están incorporando a la red de datos de las organizaciones, la llegada de nuevos servicios

que se encuentran basados en la Nube, las aplicaciones centradas en dispositivos móviles y principalmente el *IoT*, que el diseño de la red tradicional se ha visto afectado en su desempeño de una forma tal que las organizaciones han observado dentro de sus métricas, una afectación en el rendimiento al interior de sus centros de datos de una manera substancial.

La consolidación de las redes en la actualidad, presentan diversos riesgos de seguridad ya que las soluciones de seguridad como son: cámaras de seguridad, sensores de movimiento, lectores de tarjetas y dispositivos de control de acceso al igual que las soluciones de comunicaciones tales como: teléfonos de escritorio, teléfonos de salas de conferencias y puntos finales de videoconferencia, operaban con sus propias redes independientes de la red principal de datos. Lo cual, si bien marco una limitada integración, proporciono una medida de seguridad y confiabilidad para cada red de datos (Frost & Sullivan, 2018).

De acuerdo con eSemanal (2019),

> *El escenario digital se encuentra integrado por más de 150 billones de dispositivos que operan y que se encuentran conectados a través de diferentes ventanas abiertas como sensores, medidores, y procesadores de información, los cuales son un puente directo para cualquier tipo de ciberataque y que requieren contar con el mejor blindaje posible. A pesar de que estas violaciones han existido desde el inicio de la era digital, los ataques cada vez van en aumento, resaltando que a nivel global ocurren 15 millones por día. En cuanto a México se refiere, nuestro país se encuentra en el top tres de los países con mayor número de violaciones por parte de dichos ciberdelincuentes* (eSemanal, 2019).

Las amenazas son constantes y conforme pasan los años las organizaciones se enfrentan cada día a nuevos retos para poder mantener a salvo sus sistemas e

infraestructura corporativa y así tener continuidad en sus operaciones de manera normal. Durante la última década, hemos visto como prosperan los ataques a organizaciones de diversos sectores como lo son principalmente: el sector financiero, energético, industrial, petróleo y gas. Por lo cual es fundamental que las organizaciones lleven a cabo valoraciones periódicas de toda su infraestructura en la que puedan garantizar la seguridad del sistema y con ello, ser capaces de poder prevenir e incluso contrarrestar cualquier tipo de ataque cibernético. Sin embargo, esta es una práctica que en México aún no cobra la importancia necesaria

De acuerdo con datos de Schneider Electric:

> *El 80% de las empresas mexicanas no han realizado una valoración en años, lo que representa un alto riesgo y momento de vulnerabilidad para el sector energético, uno de los más importantes y propensos a sufrir un atentado debido al gran impacto que pueden llegar a causar en la operación, costo y reputación de la empresa* (Citado por, eSemanal, 2019).

Un ataque cibernético, puede causar un gran daño a las organizaciones si estas no prestan atención a las diversas brechas de seguridad que representa mantener una red sin las debidas valoraciones de manera constante. Motivo por el cual el mercado mexicano requiere que se realice una valoración constante del estado de su red y la infraestructura que conlleva, para así poder verificar que no existen brechas de seguridad que puedan dejar abiertas ventanas y que estas deriven en afectaciones para las organizaciones.

Felipe Rivera, vicepresidente de la división de Automatización de Procesos de la marca Schneider Electric en México y Centroamérica, citado por eSemanal (2019, hace mención a esta problemática:

> *Sabemos que la tecnología avanza de manera acelerada, razón que provoca que los equipos se vuelvan más susceptibles a los ciberataques, un ejemplo claro es el sector energético y en los segmentos a los que pertenecen nuestros clientes como el minero y el de petróleo y gas. Es necesario ayudar en la concientización de las vulnerabilidades que pudieran estar presentes en sus activos, si no se cuenta con la seguridad correspondiente en sus redes OT*[30] (eSemanal, 2019)

Para cualquier organización privada o pública la seguridad de su información es primordial, por lo que la protección de datos es parte vital de las empresas y de las personas. Con la aparición del *IoT*, se ha presentado un riesgo a la seguridad informática que en un futuro cercano deberá ser tomado en consideración por los fabricantes y principalmente por las empresas que hacen uso de las mismas; para que sus respectivos departamentos de *TI* puedan tomar las medidas necesarias para detectar, evaluar y minimizar los riesgos inherentes a los dispositivos.

De acuerdo con Tilves, Mónica (2019), los ataques a los dispositivos de *IoT* se han incrementado exponencialmente:

> *Durante los seis primeros meses del año se llegó a detectar 105 millones de ataques a dispositivos IoT que procedían de 276,000 direcciones IP únicas. Si se comparan estas cifras con las de la primera mitad de 2018, la evolución es evidente. Hace un año se identificaban 12 millones de ataques de este tipo, de 69,000 direcciones IP* (Tilves, 2019).

Como podemos observar, los ataques cibernéticos buscan una vulnerabilidad dentro de la infraestructura de red instalada, así como de las deficiencias en la seguridad de los dispositivos interconectados a los centros de datos que cada vez

[30] Tecnología operativa, por sus siglas en inglés *Operational Technology.* Nota del autor.

más organizaciones compran e instalan en sus centros de datos, pero que no todos consideran que valga la pena protegerlos. Los ataques cibernéticos a los dispositivos de *IoT* se han dado principalmente por tres amenazas que hasta el momento han causado grandes problemas:

- *Mirai* es la amenaza principal, ya que se encuentra detrás del 39 % de los ataques.
- *Nyadrop*, presente en un cercano 38.57 %, y
- *Gafgyt*, con un porcentaje del 2.12 %.

Dan Demeter, investigador de seguridad de *Kaspersky*, citado por Tilves (2019), nos indica:

> *A juzgar por el mayor número de ataques y la persistencia de los delincuentes, podemos decir que el IoT es un entorno fructífero para los atacantes, que utilizan incluso los métodos más primitivos, como adivinar la contraseña y las combinaciones de inicio de sesión* (Tilves, 2019).

El Instituto Nacional de Ciberseguridad con sede en Madrid, España en su publicación titulada: **"*IoT: riesgos del Internet de los trastos* (2017)"**[31], hace énfasis en que los dispositivos conectados a la infraestructura de red de las empresas, no consideran de forma adecuada la realización de las auditorías de seguridad informática, lo cual representa un riesgo de seguridad al interior de las organizaciones.

[31] Los sistemas de seguridad físicos como cámaras de vigilancia Web IP, sistemas de control de presencia o alarmas que permiten el control remoto, sistemas de videoconferencia, medidores de energía o termostatos controlados en remoto desde un servidor, etc. son dispositivos que disponen de conexión directa a Internet o las redes internas de la empresa y que no suelen estar controlados por la política de seguridad de redes de las empresas. Son dispositivos englobados en lo que se denomina IoT o «Internet de las cosas», que consiste en conectar a Internet objetos cotidianos con el fin de que puedan ser manejados o gestionar la información que generan en remoto (Instituto Nacional de Ciberseguridad, 2017).

> *Es importante y vital que dentro de las organizaciones en los procesos de gobernabilidad corporativa de las TI, se tome en consideración que todos los recursos implementados de IoT , y que en general cualquier dispositivo conectado a una red empresarial o mediante una conexión vía Internet, es susceptible de ser intervenido de forma remota por personal no autorizado y así ver comprometida la seguridad al ser accedidos o intervenidos por personal que cuenta con la capacidad tecnológica y los conocimientos necesarios para poder ingresar de manera indebida a las redes de las organizaciones. Ya que tales dispositivos no cuentan hasta el momento con los mismos estándares de calidad de seguridad informática a diferencia de los dispositivos diseñados específicamente para redes de datos* (Instituto Nacional de Ciberseguridad, 2017).

Para Santos, (2019) en su artículo titulado: **"Cinco tecnologías que influirán en 2019"** nos comenta lo siguiente:

> *Durante muchos años la seguridad física era analógica. Los equipos de TI se preocupaban poco por las cámaras; sin embargo, con la popularización de la video vigilancia digital, la situación cambio y exige nuevas adaptaciones de los profesionales del mercado, como se observará más intensamente este año* (Santos, 2019).

Las redes basadas en el protocolo *IP*, ofrecen nuevas capacidades para las plataformas de seguridad y comunicaciones las cuales incluyen entre otras cosas un nivel más profundo de integración con las aplicaciones comerciales y una economía de escala que viene con la infraestructura compartida; sin embargo esto conlleva un costo ya que, al tener una infraestructura compartida, los dispositivos y servicios que utilizan *IoT* al momento de ser desplegados de una manera inadecuada y al realizar una implementación rápida pueden conllevar un impacto

negativo en la seguridad de los servicios de misión crítica de las organizaciones al igual que los sistemas y las comunicaciones que se encuentran basadas en PC ´s.

Por otro lado, las aplicaciones y servicios que consumen un gran ancho de banda, podrían restar inadvertidamente valiosos recursos vitales para su correcto funcionamiento a otros dispositivos. La desegregación pone de manifiesto que todos los dispositivos dentro de la red de datos, serían susceptibles de riesgos de ataques de denegación de servicio[32] o *DoS* (por sus siglas en inglés *Denial of Service*) y la denegación de servicio distribuido o *DDoS* (por sus siglas en inglés *Distributed Denial of Service*). La diferencia entre ambos es el número de ordenadores o direcciones *IP´s* que realizan el ataque, malware o inclusive un punto final de conexión que consuma más ancho de banda dentro de la red de lo que debería de consumir (Frost & Sullivan, 2018)

Las tecnologías relacionadas con el *IoT* son relativamente nuevas y su seguridad aún es muy frágil, aunado a la constante expansión en diversos rubros, existe el riesgo latente de accesos no autorizados a los dispositivos de *IoT*.

Como nos lo indica Peña, (2019) en su artículo: ***"Qué es el Internet de las Cosas y cómo afecta tu vida diaria"*** en el cual comenta acerca de los riesgos del *IoT*:

> *En el 2016, se presentó el primer malware que demostró la vulnerabilidad de la Internet de las Cosas. Conocido con el nombre de Mirai, este malware accedió a algunos dispositivos conectados utilizando las contraseñas y nombres de usuario que vienen predeterminados con los productos* (Peña, 2019).

La penetración que ha tenido en todos los sentidos en la vida de las organizaciones y las personas el *IoT* se encuentran presentes en gran parte de la vida cotidiana de la sociedad actual. Es donde comienza a producirse un efecto que resulta

[32] Véase (Oficina de Seguridad del Internauta (OSI), 2018)

interesante ya que podemos hablar actualmente de hogares inteligentes, educación inteligente, cuidado de la salud inteligente, Internet en los vehículos (*IoV*, por sus siglas en inglés *Internet of Vehicles*), edificios inteligentes (*Smart Buildings*) y ciudades inteligentes (*Smart Cities*).

Dentro de las necesidades básicas para que el *IoT* pueda funcionar adecuadamente, debemos de considerar su base tecnológica, que es la misma que se encuentra dentro de las organizaciones y que incluyen en sus centros de datos dispositivos, plataformas tecnológicas y aplicaciones. Las mismas que a su vez requieren de medidas de protección y de seguridad en cada etapa de su interacción con el resto de los principales dispositivos de comunicación de red. Así como las capacidades de inteligencia y análisis de la seguridad total de la información de datos generada para poder aprovechar adecuadamente la sinergia que es generada entre los dispositivos y la Nube.

Derivado de lo anteriormente expuesto, la evolución que ha tenido en la actualidad la seguridad informática dentro de las organizaciones y de la sociedad en general. Así como su privacidad, pueden llegar a verse seriamente comprometidas por las posibles amenazas de ciberseguridad, dado el hecho que actualmente existen diversos dispositivos que hacen uso de una conexión a Internet para la transmisión de datos como son: relojes inteligentes, aplicaciones de localización, sistemas de cuidado médico, etcétera.

Los cuales al contar con la capacidad de transmitir información y procesarla de una forma automática, también son fuente de problemas de seguridad. Derivadas directamente de las vulnerabilidades técnicas que existen con la autenticación de usuarios y cifrado de información de los datos que transmiten y que a su vez pueden ser factibles de una intervención por personal no autorizado para su acceso.

La tecnología del *IoT* se considera un concepto relativamente nuevo dentro de las organizaciones, y principalmente la integración de los mismos hacia los centros de

datos es uno de los mayores desafíos los cuales deben de enfrentar las organizaciones al momento de implementar una solución basada en *IoT*.

Sin embargo, deben de considerarse seriamente en las políticas de seguridad informática como una parte dentro de la infraestructura tecnológica que presenta una serie de riesgos y vulnerabilidades que deberían de tomarse en consideración tal y como podremos observar en la tabla ***Tabla 11 - Riesgos y vulnerabilidades del IoT.***

Tabla 11 - Riesgos y vulnerabilidades del *IoT*

Recursos limitados	Los procesos de control de seguridad avanzados no pueden aplicarse de forma adecuada en los dispositivos de *IoT* , debido que en la mayoría de ellos se encuentran con capacidades limitadas de procesamiento, memoria y potencia.
Ecosistema complejo	Es común que el *IoT* se vea como un conjunto de dispositivos independientes del sistema de infraestructura corporativo; sin embargo, esto agrava los problemas de seguridad ya que debería verse como un conjunto de dispositivos que interactúan con la organización como dispositivos, comunicaciones, interfaces y personal.
Bajo costo	Las características de seguridad de los dispositivos de *IoT* por parte de los fabricantes tienen una limitante para asegurar un bajo costo y por lo tanto, la seguridad del producto podría no ser capaz de proteger contra ciertos tipos de ataques.
	Al ser un ámbito novedoso en tan poco tiempo, hay una falta de personal con las

Falta de experiencia	capacidades y experiencia suficiente en materia de ciberseguridad en *IoT* que cuente con un histórico de problemas o amenazas en este sentido y que les permitan a las organizaciones aplicar lecciones aprendidas. Simplemente se cuenta con unas reglas muy generales en este sentido que se deben de aplicar de manera adecuada.
Fallos de seguridad en el diseño propios del dispositivo y de su explotación	La gran mayoría de los fabricantes, se enfocan en lanzar sus productos de forma rápida en un mercado muy competido, por lo cual descuidan las fases de seguridad en su diseño y pruebas con aspectos tales como son: cifrado de la información transmitida, controles de acceso, etcétera.
Falta de control y asimetría de la información	Los mecanismos convencionales utilizados para obtener el consentimiento de los usuarios son considerados consentimientos "de baja calidad". Además, esta información puede llegar a manos de terceros sin que el usuario sea consciente de la difusión de la misma. También, aunque no es una práctica especifica de *IoT* , la falta de control que existe en tecnologías como los servicios en la Nube y el Big Data[33], incluso en la problemática que surge de la combinación de ambos, hace que la falta de control y la asimetría de la información estén muy presentes en el ámbito del *IoT* .

[33] Véase (PowerData, 2019)

Limitaciones en la posibilidad de permanecer en el anonimato cuando se utilizan servicios	El avance de la tecnología *IoT* provocará la pérdida del anonimato en el uso de múltiples servicios en los que al día de hoy se presupone como algo garantizado. Para proteger dicho anonimato será necesario mejorar las técnicas de control de acceso y de cifrado, desarrollar técnicas de apoyo al concepto de Privacidad por Diseño, evitar la inferencia de información y preservar la privacidad de la ubicación del usuario.
Seguridad frente a eficiencia	La presión de tiempo de comercialización de los productos *IoT* es mayor que en otros ámbitos, a veces se imponen limitaciones a los esfuerzos para desarrollar dispositivos seguros. Por esta razón, y a veces también debido a problemas de presupuesto, las empresas que desarrollan productos *IoT* ponen más énfasis en la funcionalidad y usabilidad que en la seguridad.
Responsabilidades poco claras	La falta de una asignación clara de responsabilidades (fabricante/prestador del servicio/usuario) podría dar lugar a ambigüedades y conflictos en caso de ocurrir un suceso que afecte a la seguridad, especialmente teniendo en cuenta la gran y compleja cadena de suministro que entraña el *IoT*. Además, la cuestión de cómo gestionar la seguridad si un solo componente fuera compartido por varias partes sigue sin resolverse.

Fuente: (Puente García, 2017)

2.4 Edificios Inteligentes (*Smart Buildings*)

El *IoT* se ha incorporado dentro de la sociedad y de las organizaciones de una forma no prevista con anterioridad, dando pauta a la aparición de varios conceptos nuevos dentro de las mismas, como es el caso de los edificios inteligentes y que a pesar de que se lleva implementando desde la década de los 90's, en la actualidad podemos ver cada vez más desarrollos de edificios llamados inteligentes en las ciudades y cada vez más organizaciones tienden a desarrollar sus propios edificios inteligentes en su beneficio.

Cuando la tecnología se traslada a los principios de arquitectura para poder dotar de las facilidades de la automatización en las funciones de la administración propias del edificio en cuestión, se le denomina un edificio inteligente.

Se considera a un edificio inteligente, cuando es capaz de satisfacer de manera automatizada y controlada de forma no presencial diferentes rubros como son: demandas de seguridad, eficiencia energética, confort, actividades mecánicas, mantenimiento y operaciones diversas que se encuentren dentro de las normativas actuales.

Aquí podemos englobar a diversos tipos de construcciones que son susceptibles de llamarse edificios inteligentes, como son, por ejemplo: naves industriales, locales comerciales, viviendas, espacios deportivos, escuelas, administraciones públicas o privadas solo por citar algunas.

En el desarrollo de un edificio inteligente, se requiere de la intervención de personal experto y multidisciplinario y que es necesario para la implementación de un edificio inteligente, como son arquitectos, ingenieros de telecomunicaciones e industriales, técnicos que sean capaces de realizar una integración de los diversos dispositivos dentro de las instalaciones para que estos puedan funcionar de manera automática

de una forma eficiente y segura. Lo que conlleva la instalación y utilización de un centro de datos de manera tradicional.

La finalidad de un edificio inteligente es conseguir una serie de objetivos en diversos niveles para poder ser considerado inteligente, los cuales se muestran en la ***Tabla 12 - Objetivos de un edificio inteligente.***

Tabla 12 - Objetivos de un edificio inteligente

Nivel arquitectónico	Debe cumplir las necesidades funcionales de sus usuarios en cuanto a confort, seguridad, operatividad y durabilidad actual y futura, además de aportar un diseño estético, práctico y flexible que permita remodelaciones rápidas y económicas gracias a su desarrollo modular tanto en instalaciones como en estructura, y genere una estimulación positiva que aumente el rendimiento productivo en las actividades realizadas dentro de éste.
Nivel tecnológico	Debe de contar con un gran número de servicios integrados mediante la automatización de sus instalaciones y controlados a través de sistemas de telecomunicación avanzados.
Nivel ambiental	Deben cumplir una serie de compromisos respetuosos con el medio ambiente que pasan por el tipo de materiales utilizados en su construcción, optimización de los elementos de iluminación y ventilación natural, eficiencia energética, y previsión de una máxima reducción de residuos y vertidos contaminantes en su funcionamiento.
	Debe conseguir reducir todos sus costes de funcionamiento y mantenimiento, consiguiendo

Nivel económico	alargar su vida útil, además de generar un mayor interés de adquisición y/u ocupación, con la consiguiente repercusión en los precios de venta y alquiler que aumentan en paralelo con la mejor valoración de los inmuebles. Los edificios inteligentes aportan un plus en la imagen de las compañías que se instalan en ellos, y a cualquier otro nivel, aportan información sobre el estatus de sus propietarios y usuarios.

Fuente: (Domótica Integrada, 2018)

En función del grado de tecnología aplicada a los edificios y a la cantidad de sensores que permiten la automatización podemos catalogar el nivel de inteligencia del mismo, y es gracias a los sensores de *IoT* que esto es posible por lo que se clasifican en tres niveles, como nos muestra la ***Tabla 13 - Nivel de Inteligencia de un edificio.***

*T*abla 13 - Nivel de Inteligencia de un edificio

Nivel 1	Corresponde a edificios con ciertos servicios de telecomunicaciones avanzadas, pero no integrados interactuando con instalaciones y equipos.
Nivel 2	Cuentan con sistemas de automatización y control, pero no están totalmente interconectados con las redes de telecomunicación.
Nivel 3	Se trata de edificios inteligentes que cuentan con una total integración entre la actividad, automatización y telecomunicaciones.

Fuente: (Domótica Integrada, 2018)

El *IoT* al ser integrado dentro una organización de forma adecuada, nos permite realizar la automatización de diversas áreas centralizándolos en un centro de datos;

sin embargo, una de las características principales en cualquier organización es minimizar los costos de integración y que a su vez sean redituables y rentables en su implementación.

Es debido a eso que la tecnología del *IoT*, debe ser visto como un sistema que se integra de acuerdo a las necesidades de cada entidad y como tal debe ser tratado en sus diversas partes que se incorporan a un sistema modular propio o ya existente de la organización mediante el uso de Internet como medio de transmisión de datos.

Dentro de una organización, podremos encontrar tres sistemas principales de control en donde el *IoT* encuentra sus principales funcionalidades al interior de la organización como podemos observar en la ***Tabla 14 - Sistemas principales de aplicación del IoT.***

Tabla 14 - Sistemas principales de aplicación del *IoT*

Control del edificio y su entorno	Es el encargado de verificar el estado de las instalaciones básicas de suministro como son electricidad, agua, gas, o prestaciones indispensables como son ascensores y escaleras eléctricas.
Control de la seguridad del edificio	Que actúa para proteger personas, equipos e información, mediante sistemas de detección de incendios, fugas de agua, gases o humo, circuitos de vigilancia interior, perimetral, control de accesos y detectores de movimientos sísmicos.
Sistemas de ahorro de energía	Instalados en el edificio, que actúan trasfiriendo temperatura entre zonas, usando energía solar, estudiando consumos, programando horarios de iluminación y climatización, y optimizando el funcionamiento de todos los equipos interconectados.

Fuente: (Domótica Integrada, 2018)

México dentro de la modernización de la infraestructura de las organizaciones, cuenta con siete edificios que se encuentran considerados como edificios inteligentes al cubrir las características antes descritas. Los cuales son:

- Torre Reforma.
- Hospital Gabriel Mancera.
- Plaza Carso.
- Torre KOI.
- Torre Mayor.
- Complejo Toreo de Grupo Danhos.
- Antiguo Palacio del Ayuntamiento.

Son las edificaciones con mayor cantidad de automatización en la ciudad de México y que en algunos casos han recibido la certificación LEED Platino[34] (Máximo reconocimiento a nivel mundial del *U.S Green Building Council* para sustentabilidad) (Arroyo Gómez, 2018).

2.5 Ciudades Inteligentes (*Smart Cities*)

La aparición de cada vez más edificios denominados inteligentes (*Smart Buildings*), comienza a dar paso al siguiente nivel, que son la aparición de las llamadas ciudades inteligentes (*Smart Cities*), las cuales hacen uso de la infraestructura urbana para poder brindar cierto nivel de inteligencia con los servicios propios de la misma y a su vez brindar valor a las organizaciones tanto privadas como gubernamentales.

En su artículo titulado: **"C*laves para entender las Smart Cities*"** Frigola, (2017) nos brinda las características principales que deben existir en una *Smart City*, los procesos de planificación, gestión y principalmente la incorporación de las amplias

[34] Véase (LEED (Leadership in Energy and Environmental Design), 2019)

posibilidades que brindan los avances tecnológicos son una parte fundamental en su funcionamiento.

Lo que le permite a la *Smart City* mejorar de una manera eficiente los servicios que presta al convertir los mismos en formas más fáciles y sencillas de administrar su tecnología instalada, ya que les brinda la flexibilidad que les ofrece el entorno tecnológico como son, por ejemplo: los servicios de limpieza urbana, el transporte público, la sincronización de los sistemas de semáforos, entre muchas posibles aplicaciones.

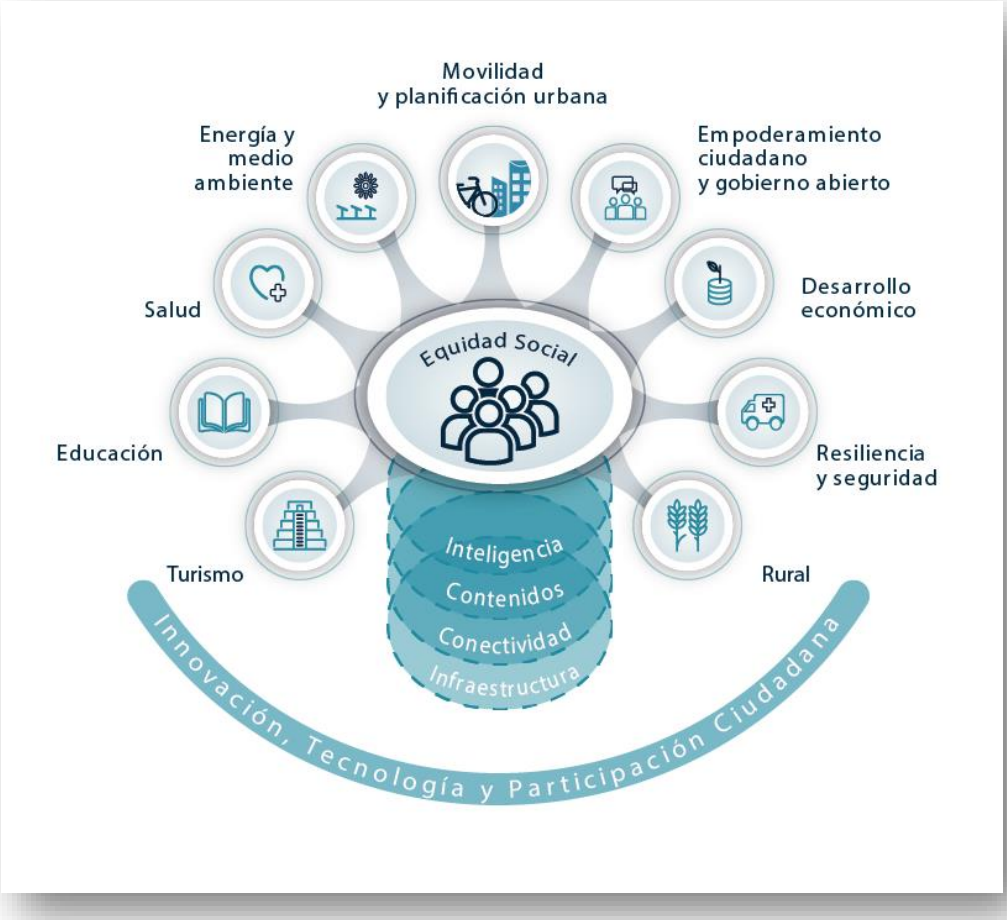

Ilustración 5 - Esquema Smart City
Fuente: (Smart cities México, 2019)

Para Frigola (2019) existen tres principales ejes del cambio que deben existir en una *Smart City* los cuales son:

- El crecimiento del tamaño de la ciudad.
- El respeto al medioambiente.
- Mejoría de los servicios a los ciudadanos.

Como se muestra en la ***Ilustración 6 - Estrategia urbana y sostenibilidad***, existen tres ejes de gestión que deben ser ejecutadas de forma paralela para que una *Smart City* pueda funcionar de manera adecuada y de forma óptima.

Ilustración 6 - Estrategia urbana y sostenibilidad
Fuente: *(Frigola, 2017)*

Las cuales se describen con más detalle en la ***Tabla 15 - Ejes de gestión Smart Cities*** que se muestra a continuación:

Tabla 15 - Ejes de gestión *Smart Cities*

Servicio Inteligente (Smart service).	En este eje de gestión, se describen las necesidades, los contenidos requeridos de cada servicios prestado, la forma en la que se prestara dicho servicio y que tan accesible es para los usuarios de cada servicio urbano que se prestara dentro de la *Smart City*, lo cual permite una planeación estratégica de los alcances de los servicios prestados a los usuarios.
Información Inteligente (Smart information).	Integra principalmente a los sistemas de información con base en las diversas plataformas de datos que deberán interactuar con una amplia base de datos digitales de información que será generada por los dispositivos instalados y que deberán abordar de manera eficaz el gran desafío del uso de *Big Data*.
Infraestructura Inteligente (Smart infraestucture).	Es la integración de la infraestructura como parte medular de la inversión e implementación de los rubros de telecomunicaciones, así como los sensores y dispositivos necesarios requeridos para poder llevar a cabo el monitoreo y administración de forma eficaz y eficiente de las redes de comunicación y de energía necesarias para la amplia gama de dispositivos requeridos en la *Smart City*.

Fuente: *(Frigola, 2017)*

Es gracias al avance en conjunto de estos tres grandes ejes, lo que permite a una *Smart City* la innovación necesaria para la prestación de los servicios tradicionales, minimizando los impactos ambientales y estructurales lo que a su vez permite la reducción de los factores de riesgo externos que puedan surgir en su implementación con la colaboración de las empresas públicas y privadas, así como la colaboración de los ciudadanos son un factor determinante en el éxito de una *Smart City*.

Una de las nuevas *Smart Cities* que utiliza los preceptos antes descritos es la ciudad de *Songdo*[35], en Corea del sur en donde se han construido infraestructuras basadas en sensores instalados por toda la ciudad, la cual le permite una administración de casi todos los servicios requeridos por la ciudadanía, como son: administración de luminarias, semáforos, fuentes en parque públicos, entre muchas aplicaciones que se han desarrollado gracias al *IoT* en beneficio de la sociedad.

> *El valor que se genera para las organizaciones y la oportunidad de tener mayor capacidad de decisión, las cuales anteriormente tenían que realizarse más por medio de la intuición que de datos concretos y precisos. Hace que la capacidad de gestión y análisis de este volumen de datos que se genera requiera el aprovechamiento de toda la infraestructura y de todas las herramientas disponibles* (Maroto, 2015).

Es debido a este volumen de información que se genera en tiempo real que el *Big Data* en conjunto con el *Machine Learning*, resultan ser una gran oportunidad de concentrar, almacenar y resulta ser un medio de analizar la información generada

[35] La ciudad de Songdo es considerada como “la ciudad más inteligente” del mundo la cual cuenta con un sistema de recolección de basura eficiente, una gran cantidad de parques y una comunidad internacional vibrante, todo ello envuelto en una obra maestra transitable con sensores del diseño urbano del siglo XXI. De igual forma que todo desde las luces hasta la temperatura de su departamento se pueden ajustar mediante un panel de control central o desde su teléfono. Durante el invierno, puede calentar el apartamento antes de ir a casa. (Poon, 2018).

con la velocidad y eficacia que la situación requiera para ayudar a adelantar decisiones y por lo tanto aumentar así la velocidad de respuesta, contribuyendo a lo que se denomina la creación de una *Smart City*.

Lo que resulta sin duda una de las grandes aportaciones de valor en donde el análisis y la gestión del *Big Data* les proporciona a las empresas el beneficio del potencial del análisis de datos masivos en tiempo real.

Sin embargo, también existen riesgos potenciales como nos los indica *IT Trends*, (2019):

> *Las ciudades están creciendo en todo el mundo, y la ONU indica que para 2050 el 68% de la población vivirá en zonas urbanas. Al mismo tiempo, las ciudades se están volviendo más y más "inteligentes" a través de los proyectos de Smart City, especialmente en los países más desarrollados. La conjunción de estos factores va a complicar mucho las cosas en cuanto a la seguridad y la privacidad de los datos* (IT Trends, 2019).

Cada vez los gobiernos municipales, están invirtiendo más en infraestructura tecnológica y en aplicaciones para poder mejorar la gestión pública como son la prestación de servicios y la movilidad urbana en general. Esto es debido al aumento de los dispositivos del *IoT*, los cuales están dedicados a proporcionar información sobre numerosos aspectos del funcionamiento de las ciudades; sin embargo, la optimización de las operaciones, también conlleva que el volumen de los datos que se generan, almacenan y analizan, deben de estar protegidos en los centros de datos que se instalan para tal fin.

Aquí es donde entra la Computación al Borde al proporcionar una gran cantidad de centros de datos de forma reducida para las diversas aplicaciones y dispositivos del *IoT* que son instalados en las llamadas *Smart Cities*. Pero la realidad es que los

mecanismos de protección de esta información generada, es insuficiente para poder garantizar la seguridad y privacidad de los datos.

Como nos lo refiere *IT Trends*, (2019) acerca de los problemas de seguridad actuales en las ciudades inteligentes:

> *Destaca la infección de ransomware que afectó en abril de este año a los servidores de la ciudad de Stuart (Florida). Debido a este ataque se vieron afectados los servicios de correo electrónico, las nóminas y otras funciones vitales de la ciudad, y el coste del rescate de todos estos sistemas fue de $600,000 dólares* (IT Trends, 2019).

La seguridad siempre será importante para las organizaciones, más en las implementaciones que se realizan con las *Smart Cities*, sin embargo, los desarrolladores de las mismas, parecen no comprender el alcance del problema que se vislumbra en el mediano plazo y la gran mayoría no está aplicando los esfuerzos necesarios para poder mejorar la seguridad de los proyectos de las *Smart Cities*.

Como nos refiere *IT Trends* (2019) la seguridad física de las infraestructuras instaladas en las *Smart Cities* y que se encuentran repartidas en las ciudades, complica en exceso la tarea de la seguridad:

> *Los analistas afirman que los entornos de TI de las ciudades inteligentes están mejorando mucho. Pero señalan que queda por abordar la seguridad de OT, que aún no permite garantizar la protección del creciente flujo de datos que se generan. los expertos recomiendan adoptar un enfoque de "confianza cero", blindando al máximo las infraestructuras en toda la cadena que conforma una ciudad inteligente* (IT Trends, 2019).

Anualmente se efectúa la cumbre sobre ciudades del futuro **"*Future Cities Summit*"**, la cual fue celebrada en la ciudad de Londres en años recientes, en donde se abordaron diversos temas, así como los desafíos a los que deberán hacer frente las empresas tecnológicas que pretendan instalar redes de última generación en las llamadas *Smart Cities*.

Sin embargo, a pesar de que en los hechos existen demasiadas ventajas competitivas de las *Smart Cities* que utilizan el *IoT* como parte medular del concepto, han tenido en su mayoría detractores del mismo, tal y como nos lo señala el Observatorio Digital, (2015) en su artículo ***"Una visión crítica sobre las ciudades inteligentes: ¿Acabarán por destruir la democracia?"***[36]. El cual realiza planteamientos interesantes que finalmente llevaran a un gran debate al respecto del uso del *IoT* en las grandes ciudades y los efectos que tendrá en las futuras *Smart Cities.*

> *Las Smart Cities a pesar de que cuentan con tecnología capaz de mantener en operación los diversos sensores que facilitan diversos tipos de servicio, aún no han podido darle solución a la pregunta ¿De qué forma afectan al modo de vida de las personas que viven en las Smart Cities? Es decir, ¿cómo cambiara el ritmo de vida de los ciudadanos gracias a la implementación del IoT en las ciudades?* (Observatorio Digital, 2015).

Como nos lo refiere el ITU[37], (2019),

[36] Es evidente que las cosas que permiten este enfoque de una amplia red de sensores que equivalen a millones de oídos, ojos y narices electrónicos también facilitan que la ciudad del futuro se convierta en un amplio campo de vigilancia perfecta y permanente para aquéllos que tienen acceso a los flujos de datos (Observatorio Digital, 2015).

[37] La UIT es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación (UIT, 2019)

> *La implementación del IoT bajo el concepto de Smart Cities, no solo permite establecer funciones urbanas definidas, sino que también promueve un grado de participación ciudadana y diversas partes interesadas tanto privadas como de gobierno en los procesos de planificación y diseño, lo que permite la creación de conocimiento compartido para la gobernanza urbana además de proporcionar la plataforma para la simulación urbana que informa los diseños futuros para el desarrollo económico, social y ambiental* (ITU, 2019).

En fechas recientes, el Banco Interamericano de Desarrollo (BID) decretó como zonas inteligentes a cinco ciudades en México las cuales son:

> *Ciudad Maderas, en Querétaro; Ciudad Creativa y Tequila en Jalisco y Smart, en Puebla. Adicionalmente la ciudad de México que a pesar de no ser 100 por ciento inteligente, cuenta actualmente con las características necesarias para convertirse en un futuro próximo en una Smart City* (Barrueta, 2019).

Dentro de las *Smart Cities*, la generación de los datos y la necesidad de transmitirlos a los centros de datos, implican una mayor transferencia de información día con día, sin embargo, es esta transferencia de datos la que tiene su origen en el crecimiento de las implementaciones de los dispositivos del *IoT* y podría llegar al punto de saturación de los anchos de banda si no se encuentran debidamente planificados.

3 Capítulo III – Pronósticos del tráfico de datos

3.1 Estadísticas de implementación de *IoT* a nivel mundial

La empresa *IoT Analitycs* quien es el líder de conocimientos de mercado e inteligencia comercial para la *Industry* 4.0 e *Internet of Things* (*IoT*), recientemente publicó los resultados de su estudio de proyectos de *IoT* a nivel mundial; que fue realizada en el año de 2018 y que estuvo centrada en los casos de uso de *IoT* que no son de consumo. El estudio detalla los diez segmentos principales que cubren la aplicación del estudio de 1,600 casos realizados y completados en más de 70 países (Scully, 2018).

La ***Ilustración 7 - Proyectos de IoT a nivel mundial***, nos muestra las estadísticas a nivel mundial de los países que realizaron una implementación de proyectos basados en *IoT* durante el año 2018, la cual nos indica:

> *América tiene el 34 por ciento de proyectos de Smart Cities actualmente completados, a diferencia del 45 por ciento de Europa y Asia Pacifico con el 18 por ciento. Adicionalmente las industrias conectadas a proyectos de IoT, en las Américas, ha tenido un 45 por ciento de crecimiento en comparación de Europa que ha visto un crecimiento del 31 por ciento en este mismo rubro. Estas regiones son las principales impulsoras de los desarrollos de IoT a nivel mundial; sin embargo, solo una quinta parte de dichos proyectos se han identificado como implementaciones de gran escala dando por hecho que el resto han sido proyectos de tamaño pequeño a mediano o que se encuentran en fase piloto de desarrollo* (Scully, 2018).

Adicionalmente, nos proporciona información acerca de los principales rubros a los que las industrias y los gobiernos han enfocado la utilización de los potenciales usos del *IoT*, para poder incorporarlos a la vida cotidiana y principalmente a la industria de manufactura, al implementarlo en la cadena de producción y áreas de suministro, seguidos de las inversiones a edificios conectados.

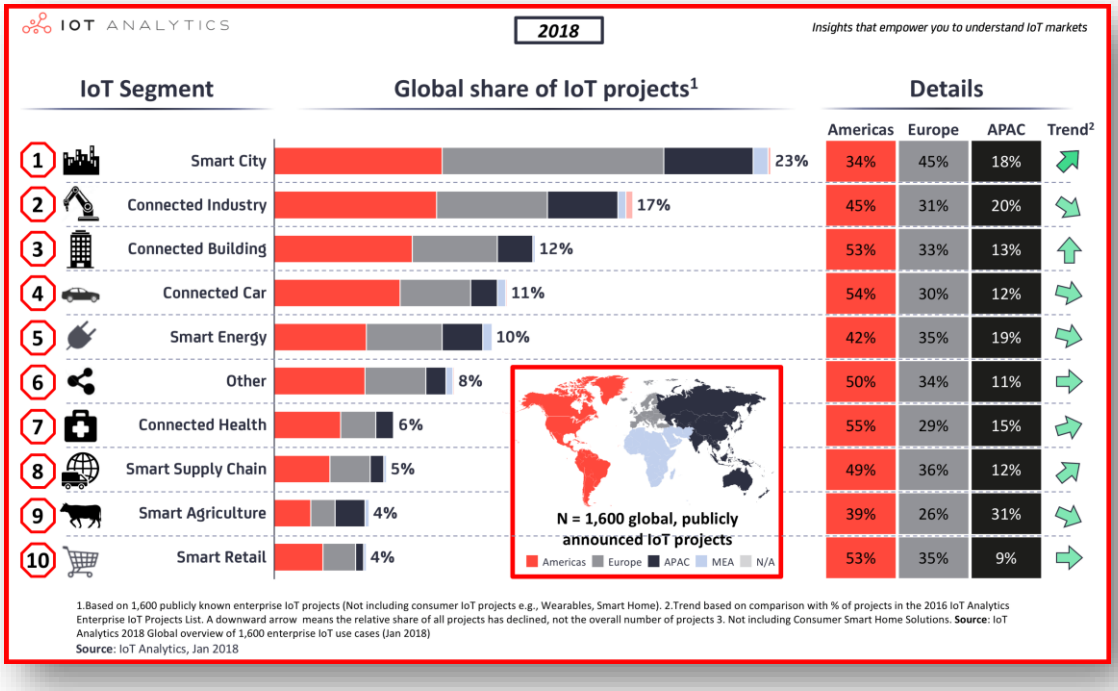

Ilustración 7 - Proyectos de *IoT* a nivel mundial
Fuente: *(Scully, 2018)*

3.2 Internet, ¿Un problema de conexión?

El medio de transmisión para el *IoT* es la red de Internet, la cual en los últimos años ha tenido un crecimiento muy amplio, derivado de las nuevas tecnologías y los cambios estratégicos en las organizaciones que cada día, hacen uso de nuevas instancias de conexión a Internet mediante sus estrategias corporativas, adicionalmente a esto, el flujo de información de datos que es generado por los equipos de cómputo.

Cada vez más cantidad de personas tienen acceso a los diversos dispositivos de *IoT* lo cual ha generado cambios substanciales dentro de la infraestructura necesaria para la transmisión de la información en diversas áreas, principalmente dentro de los centros de datos en todos los niveles.

La empresa Cisco, realiza de forma periódica una actualización de los pronósticos de tráfico de datos móviles globales del índice de redes visuales (VNI)[38], la cual es una iniciativa corporativa que se realiza de forma anual y tiene la finalidad de poder evaluar y predecir el impacto que tienen las aplicaciones de redes visuales dentro de las redes globales que utilizan como medio de transmisión la red Internet, como podemos observar en la ***Ilustración 8 - Tráfico mundial de datos móviles***.

> *Se espera que el tráfico de datos móviles en general aumente a 77 exabytes[39] por mes para 2022, lo que representa un aumento de siete veces con respecto a 2017. El tráfico de datos móviles aumentará a un CAGR[40] del 46 por ciento de 2017 a 2022* (Cisco VNI Mobile, 2019).

Ilustración 8 - Tráfico mundial de datos móviles
Fuente: (Cisco VNI Mobile, 2019)

[38] Véase (Cisco VNI Mobile, 2019)
[39] Véase (Gomar, 2018).
[40] Véase (Econodía, 2011).

A nivel mundial, el tráfico inteligente aumentará del 92 por ciento del tráfico móvil global total al 99 por ciento para 2022. Como podemos observar en la ***Ilustración 9 - Crecimiento de los dispositivos móviles inteligentes.***

> *Este porcentaje es en promedio significativamente más alto que la proporción de dispositivos inteligentes y conexiones (73% para 2022), porque en promedio un dispositivo inteligente genera un tipo de tráfico más alto que un dispositivo no inteligente. A nivel mundial, en 2017, un dispositivo inteligente generó diez veces más tráfico que un dispositivo no inteligente, y se pronostica que para el 2022 un dispositivo inteligente generará 15 veces más tráfico* (Cisco VNI Mobile, 2019)

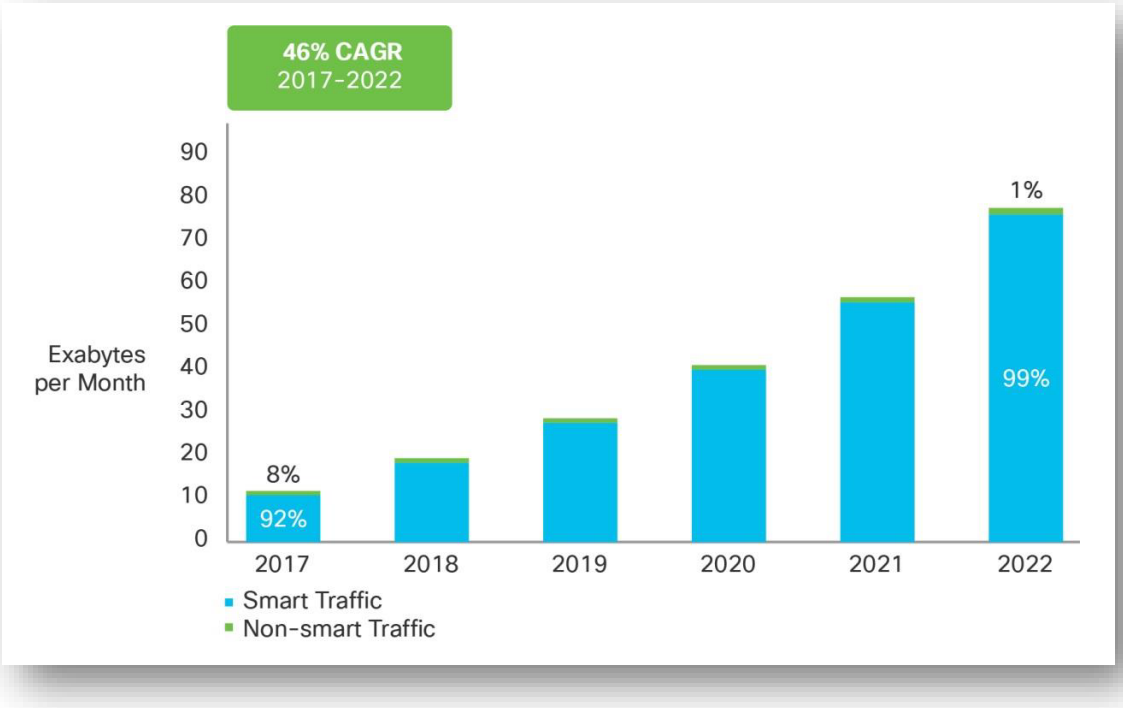

Ilustración 9 - Crecimiento de los dispositivos móviles inteligentes
Fuente: (Cisco VNI Mobile, 2019)

Considerando las estadísticas a nivel mundial de las conexiones que se encuentran actualmente funcionando y tomando en cuenta que para cada dispositivo conectado

a la red de Internet, se requiere de forma obligatoria un direccionamiento *IP* de manera específica y única por dispositivo para que a nivel mundial; pueda ser identificado dentro de la red de datos y al mismo tiempo permitir la conexión a los diversos dispositivos conectados en Internet, ha generado en los últimos años una profunda reestructuración de un nuevo modelo de direccionamiento *IP* el cual permita la interconexión a futuro de los nuevos dispositivos que se están generando día con día.

Debemos, considerar que estos direccionamientos que se realizan a los diversos dispositivos conectados a una infraestructura de red ya sea móvil o fija, se realiza mediante direcciones *IPv4* que es el protocolo que se utiliza en la actualidad y que en los últimos años casi se han agotado a nivel mundial.

> *Desde su concepción se conocía el número limitado de dispositivos que podrían conectarse, sin embargo, no se tomó en cuenta que la proliferación exponencial de los múltiples dispositivos inteligentes que existen en la actualidad requerirían una conexión a Internet, ocasionando que queden muy pocos segmentos de direcciones los cuales puedan ser utilizados en los dispositivos* (Alcalá, 2010).

Por lo cual la creación y aparición del nuevo protocolo *IPv6* más que una actualización a los estándares, fue una necesidad esperada desde hace tiempo al ofrecer ventajas derivadas de la posibilidad y facilidad de que cada dispositivo conectado a Internet mediante el protocolo *IPv6* tenga una dirección física, única e irrepetible a nivel mundial, la cual será enrutable globalmente en Internet que permitirá que los dispositivos inteligentes y el *IoT* sean una realidad (Cisco VNI Mobile, 2019).

A raíz de la aparición del nuevo protocolo *IPv6*, las industrias han reaccionado favorablemente para su paulatina adopción en los próximos años; sin embargo, el poder administrar de forma adecuada la gran cantidad de dispositivos de nueva

generación que día con día van apareciendo y que a su vez contribuyen de manera directa en el uso de la red móvil generando mayor tráfico de datos dentro de la red de Internet, será todo un desafío que pondrá a prueba las capacidades actuales en la transmisión de datos de cualquier organización que utilice como medio de transmisión de datos la red de Internet.

> *Esta estimación se basa en el soporte del sistema operativo de IPv6 (principalmente Android e iOS) y el movimiento acelerado a redes móviles de mayor velocidad (3.5G o superior) capaces de habilitar IPv6. (Este pronóstico pretende ser una proyección de la cantidad de dispositivos móviles compatibles con IPv6, no dispositivos móviles con una conexión IPv6 configurada activamente por el proveedor de servicios de Internet [ISP])* (Cisco VNI Mobile, 2019).

Debido al constante crecimiento que de manera exponencial se ha dado en los últimos años, los pronósticos del número de dispositivos del *IoT*, se muestra la necesidad de mejorar los servicios de transmisión del Internet móvil; lo cual es indispensable para hacer frente al aumento del volumen de datos que puedan transmitirse, así como la velocidad de transferencia de información. Aquí es donde entra en juego la tan esperada red 5G, lo que permitirá que se amplíen enormemente las capacidades de conectividad inalámbrica y principalmente del *IoT*.

Como nos refiere Lanner, (2019) en su definición de la red 5G:

> *Se trata de la quinta generación de estándares inalámbricos móviles basados en el estándar IEEE 802.11ac de tecnología de banda ancha. Sin embargo, mientras que las tecnologías 5G están en desarrollo, todavía no se ha establecido ningún estándar formal. Al igual que sus predecesores 3G, 4G y LTE, 5G tendrá como objetivo construir sobre los cimientos dejados por sus anteriores iteraciones, no sólo permitiendo a la gente hacer sus llamadas y textos y navegar por la*

> *web, sino también aumentar considerablemente la velocidad a la que los datos son compartidos a través de la red, haciendo posible ofrecer más servicios y aplicaciones a los usuarios* (Lanner, 2019).

Adicionalmente, las redes 5G también ofrecerán la banda ancha y la latencia necesaria para poder responder a las crecientes demandas de los dispositivos conectados, mejorando así los servicios en la Nube de las organizaciones.

Como nos refiere Sánchez-Caballero, (2019) en su articulo publicado en el diario *El País* (Madrid), con referencia al uso de las redes 5G:

> *En el futuro, es probable que la tecnología de la Nube sea lo suficientemente estable como para sustituir a los tradicionales centros de datos. Esta fiabilidad de la Nube hará también que los fabricantes ya no tengan que incluir procesadores ni memoria en los dispositivos, por lo que el hardware será cada vez más compacto. La eficiencia en cuanto a coste para las empresas podría ser enorme, porque ya no necesitarán actualizar continuamente los dispositivos para estar al día* (Sánchez-Caballero, 2019).

La combinación de las capacidades de los diversos dispositivos con un ancho de banda más rápido, más alto y redes más inteligentes facilitará la amplia experimentación y la adopción de aplicaciones multimedia avanzadas que contribuyen a aumentar el tráfico móvil y WiFi. Lo que conlleva a la necesidad de una gestión adecuada del ancho de banda por parte de las organizaciones y principalmente de los proveedores de servicios de Internet.

De acuerdo con Cisco VNI Mobile, (2019) en su Índice de redes visuales del pronóstico del tráfico mundial de datos móviles, 2017–2022, nos indica que para 2022, el impacto de 5G comenzará a surgir:

- *Las conexiones 4G serán el 54.3% del total de conexiones móviles, en comparación con el 34.7% en 2017.*
- *Las conexiones 4G móviles mundiales crecerán de 3,000 millones en 2017 a 6,700 millones en 2022 a una tasa compuesta anual del 18 por ciento.*
- *Las conexiones 5G aparecerán en escena en 2019 y crecerán varios miles de puntos porcentuales ya que pasarán de menos de medio millón en 2019 a más de 400 millones en 2022* (Cisco VNI Mobile, 2019).

Como podremos observar en la ***Ilustración 10 - Crecimiento redes móviles.***

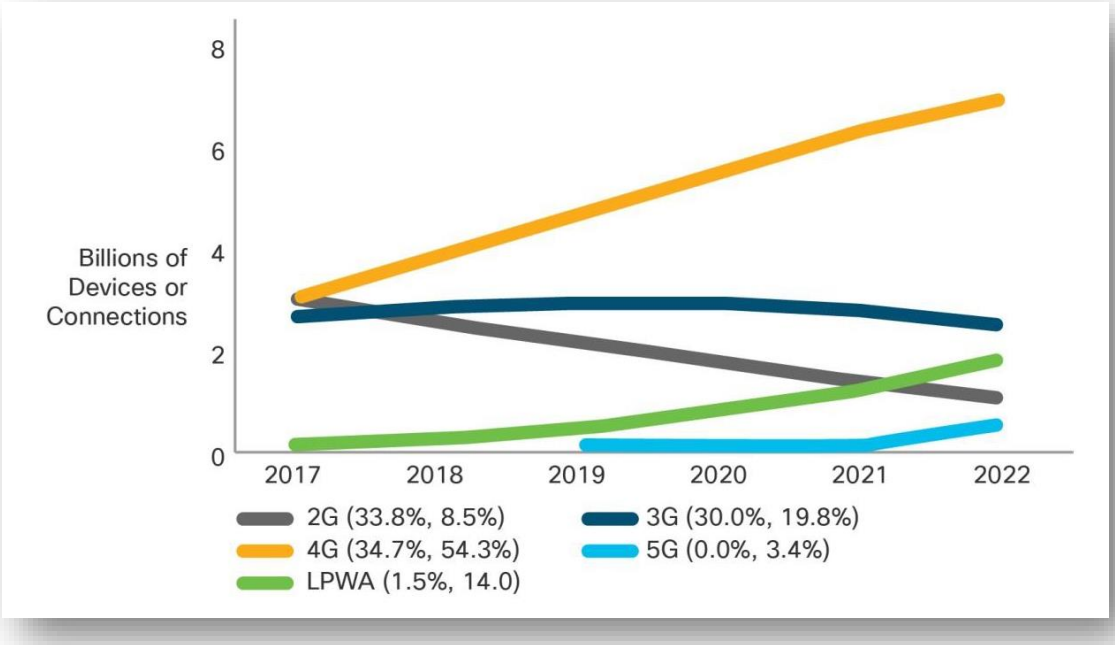

Ilustración 10 - Crecimiento redes móviles.
Fuente: (CISCO VNI Mobile, 2019)

Centrándose en los segmentos de dispositivos móviles y tabletas de dispositivos móviles de alto crecimiento, el pronóstico proyecta que el 94 por ciento de los teléfonos inteligentes y las tabletas (6.6 mil millones) será compatible con *IPv6* para

el año 2022 (un 71 por ciento, o 3,200 millones de teléfonos inteligentes y tabletas en 2017; refiérase a la ***Ilustración 11 - Cantidades de Smartphone y tabletas***).

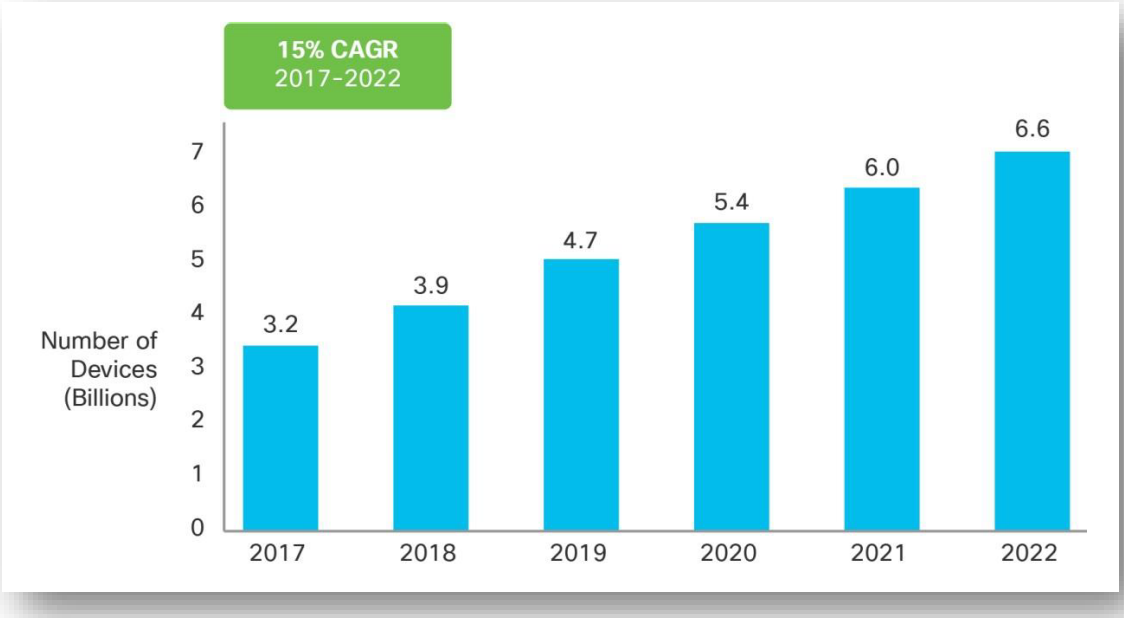

Ilustración 11 - Cantidades de Smartphone y tabletas
Fuente: (Cisco VNI Mobile, 2019)

Uno de los más claros indicadores del crecimiento del *IoT* ha sido el desarrollo y aparición exponencial de los cada vez más nuevos e innovadores dispositivos que van apareciendo con mayor frecuencia de la esperada en diversos sectores. Siendo los dispositivos de *IoT* cada vez más inteligentes y que a su vez tienen conexión Maquina a Máquina (*M2M*)[41] de forma más eficaz.

Lo cual ha permitido que los procesos, datos y elementos que se utilizan para realizar las conexiones en red sean más valiosas y relevantes hoy en día, haciendo

[41] En su reporte *Global Mobile Data Traffic Forecast Update*, 2017–2022 sección *Trend* 3: *Measuring Mobile IoT Adoption—M2M and Emerging Wearables* nos indica que “las conexiones *Machine-to-Machine (M2M)* tales como la seguridad y la automatización del hogar y la oficina, la medición inteligente y los servicios públicos, el mantenimiento, la automatización de edificios, la automoción, la salud y la electrónica de consumo y más, se están utilizando cada vez más dentro de la industria; así como dentro del segmento de los consumidores”. (Cisco VNI Mobile, 2019)

que la computación y principalmente la conectividad sean vistas de forma muy generalizada y común en la vida cotidiana, dando por hecho que dicha conectividad es algo más que necesario y esencial para las personas y principalmente para las organizaciones (Cisco VNI Mobile, 2019)**.**

Dado que la implementación de sistemas de monitoreo de las conexiones *M2M*[42] permite el monitoreo de la información en tiempo real, las conexiones de *M2M* con un uso intensivo del ancho de banda disponible se han vuelto de uso más frecuente como podemos observar en la ***Ilustración 12 - Crecimiento global M2M****,* la cual nos indica que a nivel mundial las conexiones *M2M* presentaron una diferencia en el 2017 de poco menos de mil millones a 3.9 mil millones de dispositivos conectados a nivel mundial en 2022. Cifra que por sí sola representa una proyección de crecimiento de forma asombrosa, si tomamos en consideración el tiempo relativamente corto de la aparición de los dispositivos de *IoT*, lo que representa un crecimiento de 4 veces con un CAGR del 32 por ciento.

Ilustración 12 - Crecimiento global *M2M*
Fuente: *(Cisco VNI Mobile, 2019)*

[42] Maquina a Maquina (*Machine to Machine*) Nota del autor.

Un factor importante que contribuye a la creciente adopción de *IoT* es la aparición de dispositivos portátiles, una categoría con un alto potencial de crecimiento. Los dispositivos portátiles, como su nombre indica, son dispositivos que se pueden usar en una persona y tienen la capacidad de conectarse y comunicarse a la red directamente a través de la conectividad celular incorporada o a través de otro dispositivo (principalmente un teléfono inteligente) mediante WiFi, Bluetooth u otra tecnología.

Estos dispositivos vienen en varias formas y tamaños, desde relojes inteligentes, gafas inteligentes, pantallas *Heads-Up* (HUD), rastreadores de salud y bienestar, monitores de salud, escáneres portátiles y dispositivos de navegación, ropa inteligente, etcétera. El crecimiento de estos dispositivos ha sido impulsado por mejoras en la tecnología que han soportado la compresión de datos de la computación y otros dispositivos electrónicos (haciendo que los dispositivos sean lo suficientemente livianos para ser usados).

Para el año 2022, se estima que habrá 1,100 millones de dispositivos portátiles en todo el mundo, con un crecimiento de más del doble de 526 millones en 2017 con un CAGR del 16 por ciento como podemos observar en la ***Ilustración 13 - Dispositivos portátiles conectados globalmente***.

> *Habrá una conectividad celular incorporada limitada en los dispositivos portátiles durante el período de pronóstico. Solo el diez por ciento tendrá conectividad celular incorporada para 2022, un aumento del cuatro por ciento en 2017. Actualmente, los dispositivos portátiles están incluidos dentro del pronóstico M2M* (Cisco VNI Mobile, 2019).

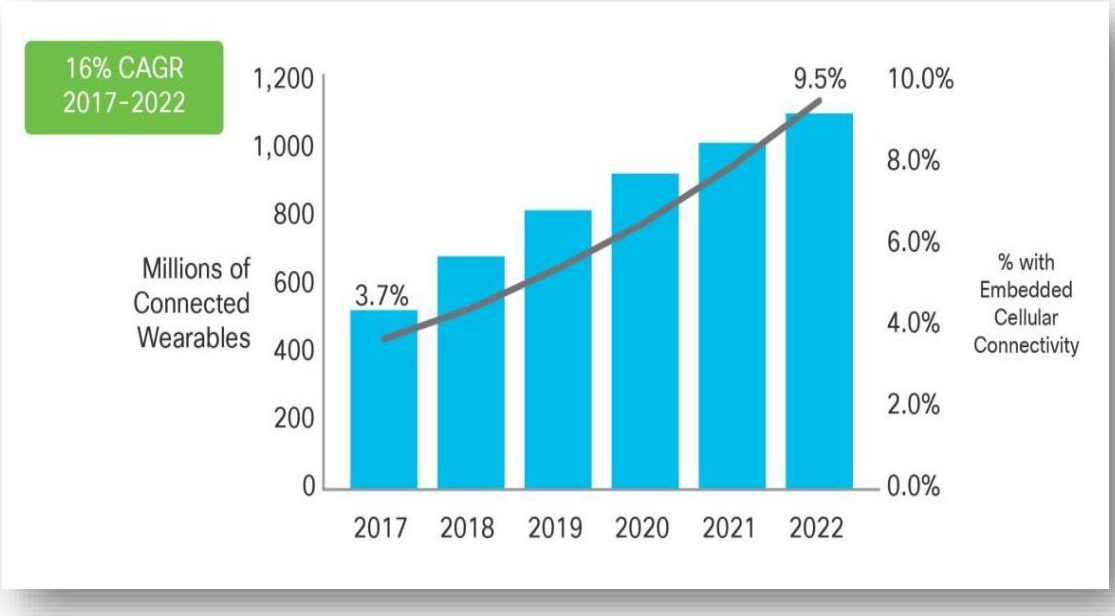

Ilustración 13 - Dispositivos portátiles conectados globalmente
Fuente: *(Cisco VNI Mobile, 2019)*

Pero todo el tráfico generado, repercute dentro de los procesos que se realizan en la Nube y en las tecnologías al borde. En México las soluciones de la Nube privada se han visto incrementadas de manera exponencial en los últimos años. Sin embargo, es la hiperconvergencia de las tecnologías lo que se muestra como una solución creciente: "*La consultora del mercado de tecnologías de la información más importante del país, IDC*[43]*, estima que crecerá siete veces más su tamaño, al pasar de 10.7 millones de dólares en 2017 a 81.1 millones para 2021*" (IDC, 2019) .

Para Monserrat Hernández, analista de infraestructura de IDC México:

[43] International Data Corporation (IDC) es la principal firma mundial de inteligencia de mercado, servicios de consultoría, y eventos para los mercados de Tecnologías de la Información, Telecomunicaciones y Tecnología de Consumo. Con más de 1,100 analistas alrededor del mundo, IDC provee experiencia mundial, regional y local sobre las tendencias y oportunidades en tecnología e industria en 110 países. El análisis y conocimiento de IDC ayuda a los profesionales de TI, ejecutivos de negocios y la comunidad de inversión, a tomar decisiones fundamentadas sobre tecnología y a alcanzar los objetivos clave de negocio. Fundada en 1964, IDC es una subsidiaria de IDG, la empresa líder en medios de tecnología, investigación y eventos. Para conocer más acerca de IDC, por favor visita www.idc.com y www.idclatin.com

> *El mercado nacional es uno de los más dinámicos de América Latina y a nivel global, pues la adopción de soluciones de hiperconvergencia (HCI) en la región presenta una tasa de crecimiento promedio anual de 34%, entre 2017 a 2023; pero en México se estima será de 35% en el mismo periodo, mientras que el promedio mundial será de 27%* (IDC, 2019).

Lo que nos indica que en México y en la región de América Latina, el proceso de crecimiento y de inversión en las soluciones tecnológicas de hiperconvergencia van en aumento de una manera exponencial, esto es debido a los usos que tienen las organizaciones en soluciones basadas en la Nube, pero también se debe a la inversión que las mismas organizaciones están realizando para poder modernizar sus centros de datos para poder generar valor a las organizaciones.

El mercado de los centros de datos en México, está pasando por un punto de inflexión entre la adquisición de servidores de manera tradicional a la contratación de servicios de infraestructura basadas en la Nube, tal y como sucede con los servicios de *IaaS*.

En la encuesta que es realizada anualmente por la compañía IDC en 2018, se entrevistaron a diversas compañías del país, en donde se les pregunto acerca de las inversiones de sus presupuestos anuales en su infraestructura propia y la inversión destinada a los centros de datos externos, y se encontró una tendencia cambiante para los próximos años: ”*Los directivos respondieron que cerca de 58% de sus recursos era para infraestructura propia; pero en 2020, los entrevistados proyectan que la tendencia cambiará, 48% será para su centro de datos y 52% para centros externos*” (IDC, 2019).

3.3 Computación en la Nube vs Computación al Borde.

3.3.1 Computación en la Nube (*Cloud Computing*).

A pesar de que el concepto de la Nube para la gran mayoría de los usuarios implica una infraestructura no tangible dentro de sus instalaciones esto no es del todo cierto, debido a que la Nube está compuesta por diversos macro centros de datos, centralizados en empresas especializadas en comunicaciones a nivel mundial.

Pero el incremento exponencial de los dispositivos conectados a Internet aunado a los modelos basados en la Nube que utilizan muchas empresas y organizaciones, han aumentado de manera exponencial el flujo de datos dentro de la misma, lo cual representa un reto para la administración de los centros de datos que actualmente la conforman.

Para el Equipo Editorial Reporte Digital, (2019) en su publicación titulada: ***"Los mitos sobre el almacenamiento de datos la Nube que deben tener en cuenta los CEO"*** en donde se presentaron diez conceptos que predominan en la evaluación del uso de la Nube los cuales enunciaremos brevemente a continuación y que nos servirán de pauta para comprender las razones por las cuales la Nube no es apta para ser considerada como parte fundamental para el almacenamiento de la información que genera *IoT*, como se muestra en ***la Tabla 16 - Mitos sobre la Nube*** en donde se muestra un resumen de las razones por las cuales las organizaciones migran a la Nube a saber:

Tabla 16 - Mitos sobre la Nube

La Nube siempre ahorra dinero.	En muchos casos esto solo significo el 14% de ahorro en costos de dinero.
Tiene que estar en la Nube para ser bueno.	Aun cuando el *Cloud Computing* se ha propagado con fuerza, no es referente principal para la toma de decisiones para las grandes empresas. Dado que muchas empresas mantienen un concepto equivocado

	de que cualquier servicio web es la Nube (*Cloud*), lo cual es erróneo.
Se debe usar la Nube para todo.	No es necesario que se utilicen todos los servicios y almacenamiento en la Nube especialmente si no existe ganancia para la organización, es decir que sea redituable realmente.
Si el CEO lo dijo…	No se pueden plantear estrategias basadas en la Nube si no existe un fin.
Estrategia de Nube.	Es necesario comprender que existen diversos modelos basados en la Nube como lo son *IaaS (*por sus siglas en inglés *Infraestructure as a Service*)*, SaaS (*por sus siglas en inglés *Software as a Service*) y *PaaS* (por sus siglas en inglés *Plataform as a Service*) como soluciones de almacenamiento en la Nube ya sea pública, privada o mixta.
La seguridad de almacenamiento en la Nube.	La seguridad de la información almacenada en la Nube deberá ser garantizada por el proveedor confiable por lo cual es parte fundamental la consideración de que tipo de información se almacenara en la Nube y cuál será la seguridad que el proveedor de la misma nos brindara al respecto.
Uso crítico de la empresa.	La gran mayoría de las empresas utilizan sistemas basados en la Nube para realizar pruebas y desarrollos, sin embargo, hay otras empresas como Netflix y Uber que las utilizan los servicios de almacenamiento para otros fines.
La Nube como un centro de datos.	Las estrategias que se utilizan en un centro de datos local no aplican de la misma forma en la Nube, por lo que no es del todo recomendable utilizar la Nube como un medio de almacenamiento masivo de información.

Migrar a la Nube es obtener todos sus beneficios.	Esto es un error, ya que depende de las necesidades reales de la organización será la estrategia que se utilizará para adquirir los servicios necesarios para su funcionamiento.
Virtualización es igual a Nube privada.	Esto es un error, dado que se necesita la implementación de mayor tecnología para que las aplicaciones de aprovisionamiento bajo demanda puedan adaptarse a las necesidades del procesamiento y monitoreo del uso de datos.

Fuente: *(Equipo Editorial Reporte Digital, 2019)*

De acuerdo con Zambrana, (2019, págs. 74-76) en su publicación titulada **"*Nube Hibrida*"** quien nos proporciona un esbozo de la situación actual de las empresas en México basado en el reporte que fue realizado por la empresa Vanson Bourne[44] a mediados del 2018. En la que nos indica que para mantenerse dentro del mercado competitivo uno de los elementos fundamentales para poder lograrlo es el concepto de Nube híbrida.

En México, se habla de que un alto porcentaje de organizaciones, alrededor del 37 por ciento que continúan operando bajo una arquitectura de centro de datos de manera tradicional, a pesar de que la mayoría está considerando realizar un cambio en su infraestructura dentro de los próximos 12 a 24 meses, el 11 por ciento considera continuar el mismo esquema de trabajo con un centro de datos de manera tradicional y no utilizar una Nube de tipo hibrida para implementarla en sus organizaciones.

Asimismo, solo el 20 por ciento de las empresas mexicanas hacen uso de una Nube publica para sus negocios. Pero es el tema de la escalabilidad en donde el factor de crecimiento se vuelve un tema importante al momento de crear nuevos servicios;

[44] Véase (VansonBourne + NUTANIX, 2018)

que requieren crecer de acuerdo a las necesidades propias de la organización. Adicionado a la preocupación de garantizar la seguridad de los datos y el cumplimiento de las normas, es cuando la Nube híbrida se podría convertir en el mejor aliado de las organizaciones.

El beneficio que obtienen las organizaciones al operar una Nube de datos hibrida, reditúa en un menor costo de operación total, aunado al hecho de que no dependen de un único proveedor del servicio. Es importante tomar en consideración varios puntos con referencia al uso de la Nube híbrida dentro de las organizaciones. Ya que de primera instancia trae consigo múltiples beneficios; sin embargo, también nuevos retos para la operación, ya que una Nube pública y una Nube privada se gestionan de maneras completamente distintas, pero esto no implica que no puedan convivir simultáneamente.

Con respecto al control y la optimización de costos, el 22 por ciento de las empresas aseguran que sobrepasaron sus presupuestos de *IT* en consumos de Nube porque no contaban con las herramientas necesarias para poder controlarlos adecuadamente. Lo que representa un gran riesgo para las organizaciones al momento de realizar una implementación de este tipo de soluciones.

3.3.2 Computación al Borde (*Edge Computing*).

De acuerdo con la revista Ventas de seguridad, (2019) la cual presenta en su sección de noticias de Tecnología y avances, una estadística basada en que para el 2022 existirán 483 millones de dispositivos de automatización de edificios conectados a nivel mundial, nos indica que basado en el informe de investigación de la firma analista de *IoT Berg Insight*, en donde muestra que la base instalada de sensores, actuadores, módulos, pasarelas y otros dispositivos conectados implementados como parte de la automatización de edificios basadas en *IoT* en edificios comerciales inteligentes y conectados se estima en 151 millones de unidades en todo el mundo para finales del 2018.

Este estudio de *Berg Insight* realiza un análisis del mercado de la automatización a lo largo de múltiples verticales que van desde los más conocidos como la calefacción, ventilación y aire acondicionado (*HVAC*)[45], iluminación interior, incendios y seguridad, acceso y seguridad, hasta los menos conocidos como son: La carga de vehículos eléctricos, sistemas de riego y monitoreo de piscinas. Las soluciones más exitosas hasta el momento, incluyen acceso y seguridad, incendios y seguridad, sistemas de climatización y ascensores y administración de escaleras mecánicas. El control automático se puede realizar a través de un sistema centralizado, como un sistema de administración de edificios (BMS).

> *Con un crecimiento anual compuesto (CAGR) del 33 por ciento, la base instalada alcanzara 483 millones de unidades en 2022. Cerca de 4.5 millones de estos dispositivos se conectaron a redes celulares en 2018. La cantidad de conexiones celulares en el mercado de la automatización de edificios aumentara a un CAGR del 44 por ciento hasta alcanzar los 19.4 millones en 2022. En términos de ingresos, Berg Insight estima que los dispositivos conectados al mercado mundial de BIoT (por sus siglas en inglés, Business Internet of Things) generaron ingresos de más de $1,200 millones de dólares americanos en 2018. Esta cifra aumentará a un CAGR del 21 por ciento a casi $2,700 millones de dólares americanos en 2022* (Citado por Ventas de seguridad, 2019).

La automatización de edificios ha existido por décadas; pero existe una nueva urgencia debido a factores como el ahorro de energía y los mandatos para la construcción ecológica. Las últimas soluciones de construcción inteligente aprovechan las nuevas tecnologías como lo son: *IoT* , *Big Data*, Computación en la Nube, análisis de datos, aprendizaje profundo e *IA* para los beneficios de ahorrar energía, reducir gastos operativos, aumentar la comodidad de la ocupación y

[45] Véase (ASHRAE Technical Committee, 2016)

cumplir con las normas globales y estándares de sostenibilidad más estrictos (Ventas de seguridad, 2019, pág. 20).

Kaladhar Vorunganti, vicepresidente de Tecnología e Innovación de la empresa TECBeat, apela directamente al *IoT* como el principal catalizador del cambio en este segmento de actividad:

> *Mantener una baja latencia es una de las principales razones por las que las compañías están moviendo grandes cantidades de datos desde dispositivos IoT más cercanos al procesamiento y analítica en la Nube. Pero llevar la interconexión al propio objeto también ahorrará en costes de red, ya que las empresas podrán depurar volúmenes de datos inútiles del Internet de las Cosas cerca de la fuente para obtener el acceso más rápido a información valiosa y necesaria para tecnologías tan importantes como los hospitales inteligentes. Y en un número creciente de regiones, los datos deben procesarse en el borde para cumplir con los requisitos de protección de datos* (Sarenet, 2018).

La Computación al Borde, se presenta como una solución viable para la integración de los dispositivos del *IoT*, sobre todo por las regulaciones que existen en diversos países de que la información deberá concentrarse en su lugar de origen, a diferencia de la Computación en la Nube en donde los datos son almacenados en diversos macrocentros de datos ubicados geográficamente en todo el mundo.

Para Quirk, (2018) en su artículo titulado: ***"Managing IoT: A problem and solution for data center and IoT managers"***, nos indica que:

> *De acuerdo a las proyecciones sobre el crecimiento en el Internet de las cosas en los próximos años, podremos observar que los proyectos de Cisco contarán con 123 mil millones de dispositivos conectados a redes mediante el protocolo Internet (IP) para el 2021, Gartner nos*

> *indica que existirán 20.8 millones de dispositivos para el 2020, mientras que IDC pronostica que existirán 28.1 mil millones de dispositivos conectados a Internet en el 2020* (Quirk, 2018, págs. 18 - 20).

Si bien existe discrepancia entre las cifras que se presentan, hay poco debate entre una tecnología que está creciendo rápidamente en todos los sectores; ya sea que se encuentre habilitando hogares inteligentes, fabricas inteligentes o ciudades inteligentes, el crecimiento se da por el impulso del potencial que tiene el *IoT* para mejorar la eficiencia, la productividad y la disponibilidad.

Pero las mismas aplicaciones de los dispositivos *IoT* pueden generar grandes volúmenes de datos que deben ser transmitidos, procesados y almacenados; lo que está generando grandes desafíos para la administración de datos de manera profesional en *TI*.

De acuerdo a los datos del índice de redes visuales de Cisco[46],

> *El tráfico IP a nivel mundial aumentará de 12 Exabytes mensuales que teníamos en el año 2017 a 77 Exabytes por mes para el año 2022, lo que representa un incremento de siete veces el nivel de tráfico que teníamos en el año 2017. Si bien no todos los datos se originarán o terminarán en un centro de datos tradicional, un gran porcentaje de los datos que se generen por IoT; por ejemplo, se generará, procesará y almacenará en el borde de la red. Por lo que solamente una fracción de los datos tendrá que ser transmitido hacia un centro de datos central para su archivo y análisis más detallado* (Cisco VNI Mobile, 2019).

[46] Véase (Cisco VNI Mobile, 2019)

El impacto que se tiene con los dispositivos de *IoT*, puede resultar más beneficioso que negativo, ya que los centros de datos son el entorno ideal para el *IoT* con su amplia gama de dispositivos y sistemas interdependientes y, a menudo interconectados entre ellos por medio de cableado estructurado vía *UTP* (por sus siglas en inglés *Unshielded Twisted Pair*), enlaces de fibra óptica y comunicación vía WiFi. El hardware del centro de datos como son: servidores, unidades de energía o sistemas de administración térmica, generan datos que son valiosos para la administración de *TI* y que sirven de base para su posterior análisis y toma de decisiones.

El hardware del centro de datos, genera continuamente información que es valiosa para la operación de los mismos sobre el estado de los equipos que los conforman, como son el estado de las temperaturas, sistemas de refrigeración[47], consumo de energía[48] y otros parámetros que se pueden utilizar para su análisis y toma de decisiones en la operación de los mismos. Sin embargo, los centros de datos son un entorno que resulta extremadamente complejo y diverso que ha dejado gran parte de los datos operativos dentro de los dispositivos derivado de la variedad de protocolos que se utilizan y a la falta de una capa de control a nivel de sistema.

Juan Luis Peñaloza Figueroa, profesor de la asignatura *Arquitectura del Big Data* del Máster en *Analítica Web y Big Data* de *Spain Business School*, adelanta otro elemento en esta ecuación hacia la computación en el borde: los *content delivery network*.

> *Junto con los proveedores de banda ancha inalámbrica, serán los demandantes de los nuevos formatos de CPD (Centro de Procesamiento de Datos) que guiarán su ubicación según la demanda de servicios. Esto supone que las nuevas aplicaciones se alojarán en infraestructuras convergentes, híperconvergentes, y de conversación,*

[47] Véase (Acciardo, 2016)
[48] Véase (42U, 2009)

donde los micro data centers facilitarán la gestión de los mismos y proporcionarán seguridad y escalabilidad (Citado por Sarenet, 2018).

El uso de una estrategia de *IoT* proporciona un marco para capturar y usar estos datos para mejorar la confiabilidad y la eficiencia; así como para permitir la automatización. También soportan el monitoreo continuo para mejorar la disponibilidad. Estos sistemas se pueden administrar dinámicamente como parte de una Nube privada o híbrida sin aumentar el riesgo. A medida que esas implementaciones y planes limitados se conviertan en implementaciones amplias, las infraestructuras de *TI* más allá del centro de datos tradicional se enfrentarán al desafío de lidiar con los enormes volúmenes de datos que se generan.

Las aplicaciones al borde, por su naturaleza, tienen un conjunto de requisitos de carga de trabajo centrados en los datos, que cuando se filtran a través de los requisitos de disponibilidad, seguridad y la naturaleza de la aplicación, demuestran ser fundamentales para comprender y categorizar las aplicaciones al borde.

Esto ha llevado al reconocimiento de cuatro arquetipos de borde que pueden guiar las decisiones con respecto a la infraestructura de borde, particularmente a nivel local. Estos cuatro arquetipos se describen en la ***Tabla 17 - Arquetipos de Edge.***

Tabla 17 - Arquetipos de *Edge*

Uso intensivo de datos	Utiliza los casos en que la cantidad de datos es tan grande que se requieren capas de almacenamiento y computación entre el punto final y la Nube para reducir los costos de ancho de banda o la latencia.
Sensible a la latencia humana	Incluye aplicaciones en donde la latencia afecta negativamente la experiencia de los humanos que utilizan una tecnología o un servicio.
Sensible a la latencia de máquina a máquina	Similar al arquetipo sensible a la latencia humana, excepto que la tolerancia a la latencia en las

	máquinas es incluso menor que para los humanos debido a la velocidad a la que las máquinas procesan los datos.
Vida crítica	Aplicaciones que afectan la salud o la seguridad humana y por lo tanto, tienen una latencia muy baja y requisitos de disponibilidad muy altos.

Fuente: (Quirk, 2018)

Las características de los datos de las tecnologías de punta colocan cada tecnología en uno de los cuatro arquetipos: intensivo en datos, sensible a la latencia humana, sensible a la latencia de la máquina o crítico para la vida. Los centros de datos locales desempeñan un papel fundamental en la gestión del ancho de banda y el costo, y en la adaptación de la latencia a los requisitos de la aplicación.

Estos arquetipos resaltan el papel fundamental que desempeñarán los centros de datos locales en la gestión del ancho de banda, el costo y la latencia correspondiente a los requisitos de la aplicación. Al hacerlo, permiten el desarrollo de diseños de referencia específicos para estos centros de datos locales que ayudarán a acelerar la implementación y garantizarán la estandarización de este enlace crítico entre los dispositivos de borde y la Nube.

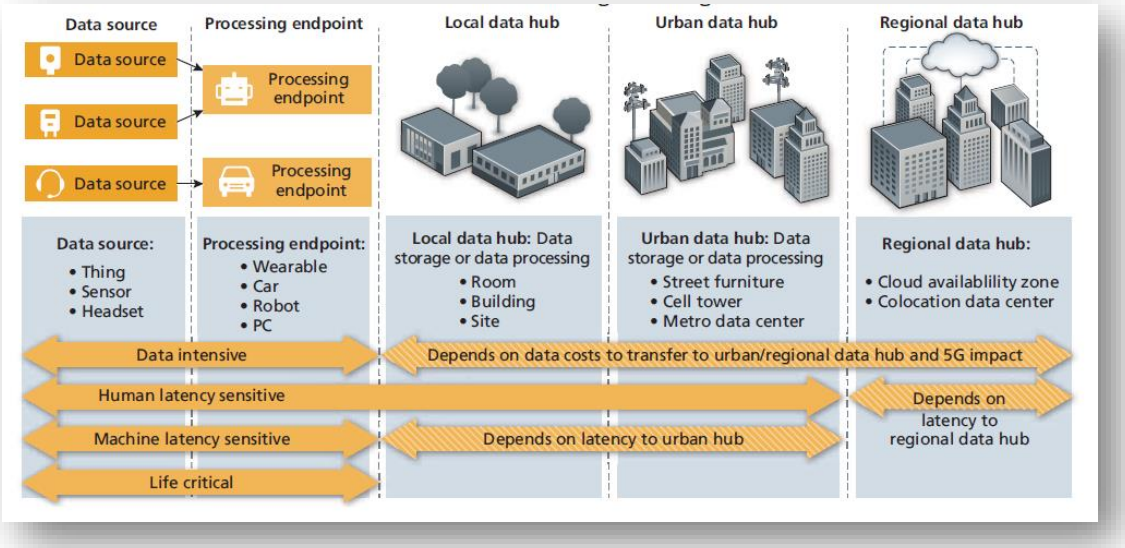

Ilustración 14 - Características de los datos de las tecnologías de punta
Fuente: (Quirk, 2018)

En general, *IoT* es la colección de dispositivos y/o aplicaciones en red que no son utilizados por humanos, también conocidos como comunicaciones de máquina a máquina o *M2M* (por sus siglas en inglés *Machine to Machine*). Pueden ser sensores que envían información, controles que pueden tomar medidas, o ambos.

Los dispositivos pueden operar en hogares, edificios de oficinas, almacenes o en exteriores desde las calles de la ciudad hasta los campos agrícolas. La mayoría de los dispositivos de *IoT* son independientes y están optimizados para su uso previsto.

Por ejemplo, se puede detectar una aplicación bancaria cuando un consumidor ingresa a la sucursal, y la experiencia con el personal se adapta a ellos. Finalmente, hay muchas aplicaciones instaladas en los teléfonos inteligentes que son esencialmente sensores móviles que recopilan datos para plataformas *IoT* mucho más grandes (King, 2019).

La cantidad de dispositivos que se encuentran actualmente en funcionamiento aunado a los que se encuentran pronosticados en un futuro próximo, hacen

necesario realizar cambios en la infraestructura de las organizaciones para poder integrar a sus centros de datos con la Computación al Borde.

Como podemos observar en la ***Ilustración 15 - Características de Edge en los sectores***, la cual nos proporciona un panorama de las necesidades de infraestructura y requerimientos para la implementación de la Computación al Borde en las organizaciones.

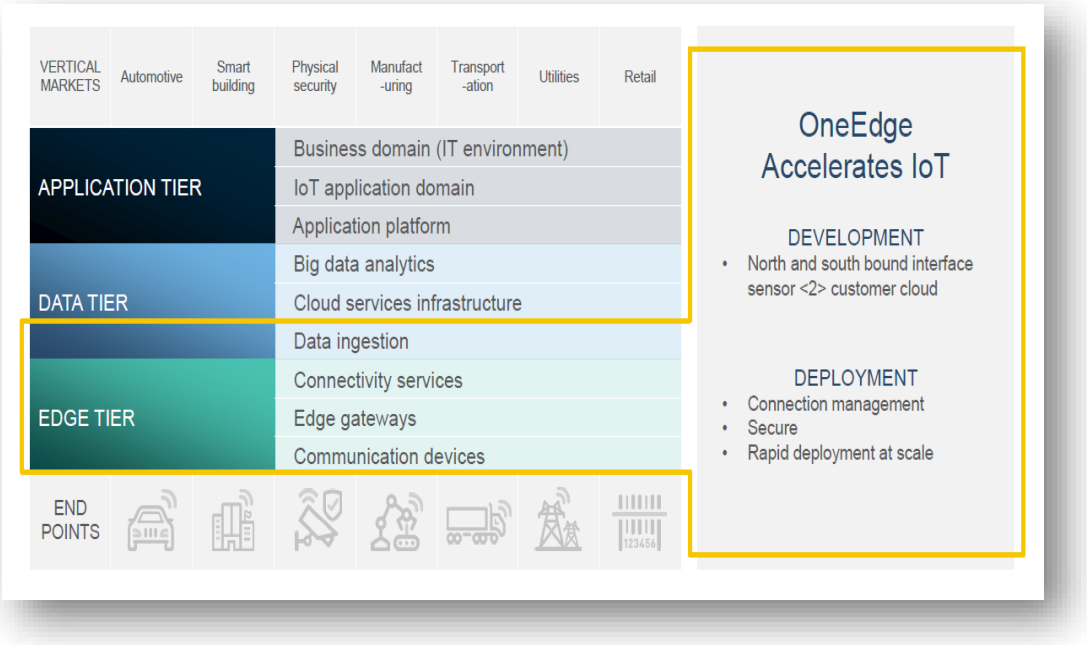

Ilustración 15 - Características de Edge en los sectores
Fuente: (Watson, Segal, & Tatara, 2019)

La Computación al Borde, proporciona una capacidad de interacción excepcional para los dispositivos de *IoT* y principalmente para las organizaciones, al tener la capacidad de obtener información de datos casi en tiempo real, lo que es indispensable para el correcto funcionamiento de los diversos dispositivos y sensores de *IoT*, como podemos observar en la ***Ilustración 16 - Los bordes emergentes***.

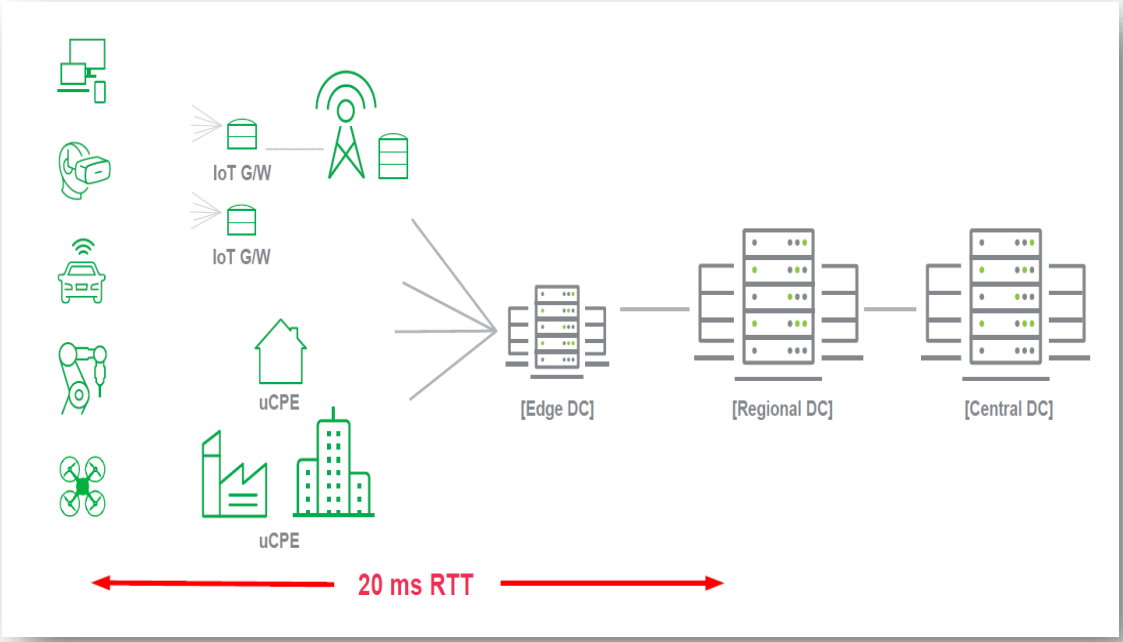

Ilustración 16 - Los bordes emergentes
Fuente: (Grossner, Thoen, & Tatara)

Sin embargo; es esta misma capacidad la que requiere la Computación al Borde subsanar en cuestiones de latencia. La latencia de la red se refiere al tiempo y/o retraso que está implicado en la transmisión de datos a través de una red. En otras palabras, el tiempo que tarda un paquete de datos para ir de un punto a otro. Hoy día esto es normalmente medido en milisegundos, sin embargo, pueden ser segundos dependiendo de la red por lo tanto mientras más baja sea la latencia de transmisión de datos se requiere de una respuesta casi inmediata y/o en tiempo real (Jackson, 2019)

Como podemos observar en la ***Ilustración 17 – Requerimientos de una baja latencia***, el porcentaje de los sectores y los tipos de aplicación, requieren de bajos tiempos de latencia en su desempeño, lo que en síntesis implica mayor tráfico de datos dentro de la infraestructura del centro de datos de las organizaciones, por lo que la Computación al Borde implica romper el actual paradigma del centro de datos de manera tradicional.

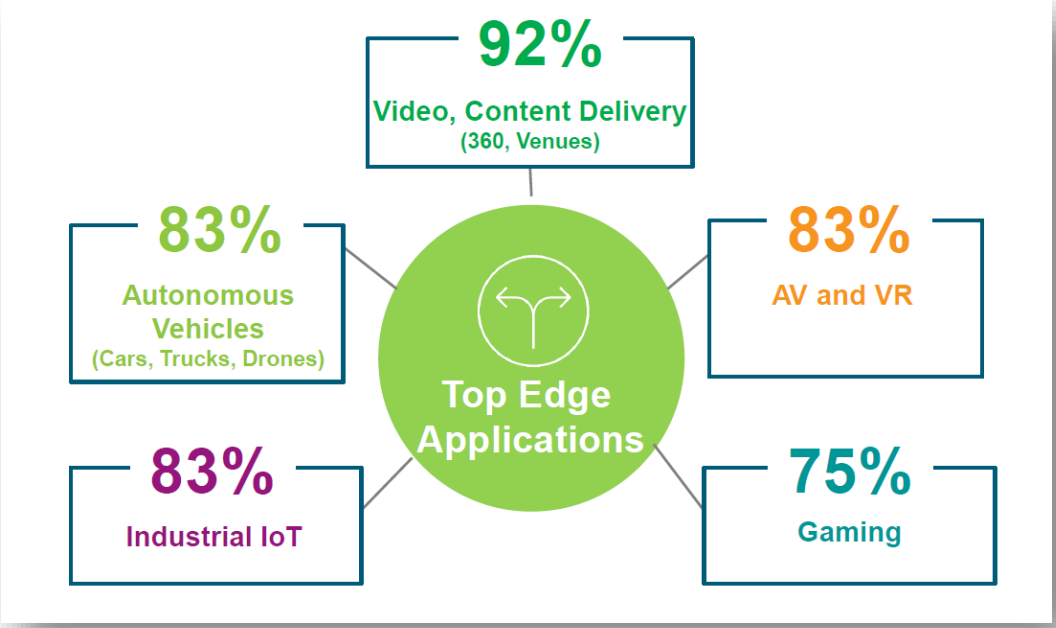

Ilustración 17 – Requerimientos de una baja latencia
Fuente: (Grossner, Thoen, & Tatara)

Las aplicaciones de misión crítica del *IoT*, se encuentran moviéndose a la Nube, al borde o una combinación de ambos conceptos para poder utilizar sus beneficios de una manera óptima y adecuada a las necesidades de las organizaciones, lo cual representa varios desafíos como son el acceso de los servicios a redes heterogéneas, aplicaciones sensibles a diferentes parámetros y que no siempre actúan correctamente a los saltos entre los equipos de direccionamiento; pero principalmente a que los destinos de las aplicaciones varían en su ubicación física.

Los medios de transmisión de datos hacia los centros de datos o a las aplicaciones que son las encargadas de realizar su análisis y recopilación de datos, han comenzado a ser diversos; entre los más utilizados tenemos Internet, MPLS (*Multiprotocol Switching*) y las actuales redes 4G/LTE como podemos observar en la ***Ilustración 18 - Medios de transmisión Edge y Cloud***.

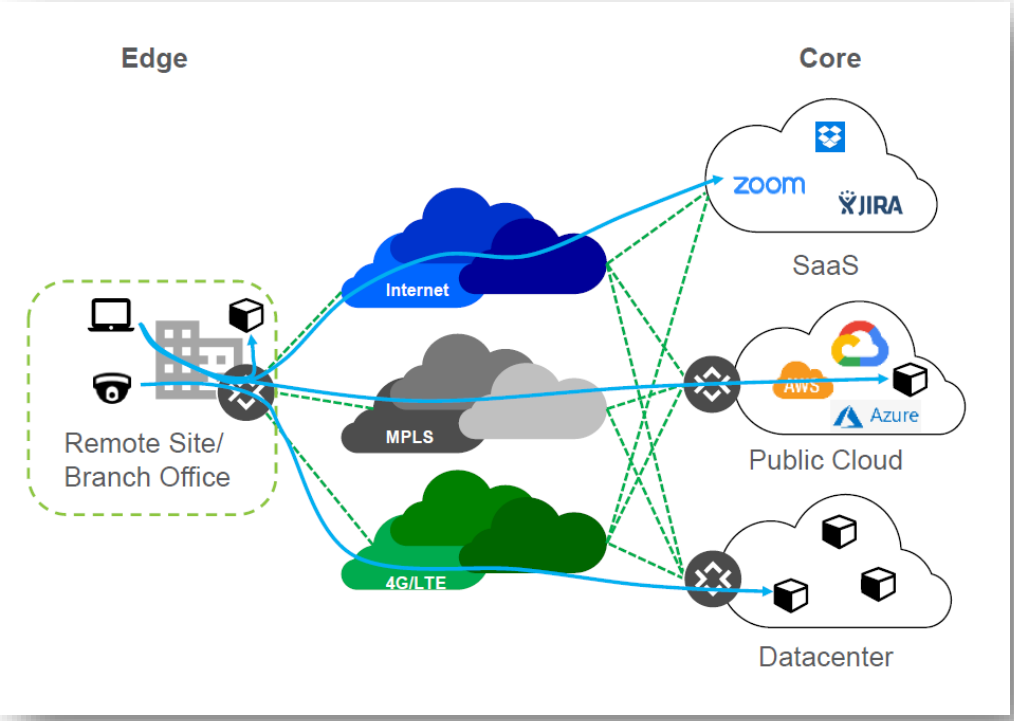

Ilustración 18 - Medios de transmisión Edge y Cloud
Fuente: (Grossner, Thoen, & Tatara)

Lo que ha permitido la proliferación de diversas aplicaciones y que a su vez ha redituado en la aparición de problemas de comunicación al saturar el ancho de banda requerido para las aplicaciones y transmisión de datos, debido a la mala planeación de los proyectos de *TI*.

Esto es derivado de que no todo es factible de ser almacenado en la Nube ya que no se toma en consideración los niveles de latencia de las aplicaciones la gran mayoría de las veces. Lo que representa un desafío para las organizaciones y para los departamentos de *TI* poder integrar las nuevas tecnologías a sus centros de datos con una infraestructura deficiente.

4 Capítulo IV – Principales desafíos de las organizaciones.

4.1 Tendencias de la industria de centros de datos

Las organizaciones y en general para todas las entidades el principal activo y del cual viven es la información, es precisamente este flujo de información que debe tener ciertas características, como son: confiabilidad, certeza y disponibilidad para su análisis y así pueda ser una herramienta útil en la toma de decisiones corporativas.

El centro de datos tradicional, brinda las características necesarias para la administración y almacenaje de dicha información que es vital para la operación de las organizaciones. Sin embargo; en la última década el centro de datos tradicional se ha visto en la necesidad de transformarse y renovarse debido a la aparición de nuevas tecnologías y las cuales requieren de romper el paradigma del centro de datos centralizado.

El *Uptime Institute*[49] es la empresa consultora de mayor renombre a nivel mundial, y es la organización más confiable que la industria ha adoptado para sus departamentos de *TI* para el diseño, construcción y el funcionamiento adecuados de los centros de datos; realizó recientemente la publicación de los resultados de su investigación titulada **"*Top 10 Data Center Industry Trends*"**, realizada en diciembre del 2018 (Uptime Institute, 2018).

En donde presenta recomendaciones a las organizaciones basada en las diez áreas clave de los centros de datos debido a su potencial para transformar los diseños y centros operativos tradicionales de centros de datos y en las cuales las organizaciones deberán prestar atención en el futuro y en donde podemos observar las principales tendencias de la industria aplicadas a las organizaciones y que

[49] La sede central mundial en *Uptime Institute* está en Seattle, Washington. Su red global de consultores realiza certificación de centros de datos, capacitación en centros de datos y consultoría de TI en más de 80 países alrededor del mundo. Nota del autor.

afectan directamente el centro de datos de las organizaciones de una manera importante en su desempeño tecnológico en un futuro inmediato.

4.1.1 Limites

Las construcciones de *Big Cloud* empujan el ecosistema a sus límites

> *Las demandas aceleradas de los grandes operadores de la Nube para una mayor capacidad del centro de datos, están distorsionando y agotando el ecosistema de proveedores, constructores, operadores y compañías eléctricas. Los requisitos de los centros de datos de hiperescala ya han rediseñado la cadena de suministro de la industria. En 2019, se espera que los operadores y proveedores se centren en una mayor estandarización: los diseños de centros de datos y equipos, los enfoques de construcción, los requisitos de potencia incremental, etc.* (Uptime Institute, 2018).

Lo cual nos indica que existe la preocupación real por parte de las organizaciones en el sentido de la migración y utilización de una manera exponencial de los procesos de la Nube. Sin embargo, es este mismo proceso del uso de los recursos de la Nube, la que se encuentra afectando los procesos del centro de datos, sobre todo a los centros de datos que no se encuentran debidamente estandarizados por malas prácticas de instalación, procesos obsoletos, personal poco capacitado en el manejo adecuado de la infraestructura informática y un largo etcétera.

4.1.2 Gobierno

Los gobiernos preocupados intensifican la supervisión y la regulación

> *Los gobiernos de todo el mundo están cada vez más preocupados por las ganancias y el poder de las grandes empresas de TI, y por la dependencia de las sociedades de la infraestructura invisible. En los*

> *últimos años, los gobiernos vieron la adopción generalizada de TI en general, como una fuerza positiva en casi todos los sentidos. TI promueve la innovación, la productividad y un flujo comercial positivo (para algunos), y crea empleos, riqueza e inversión en infraestructura. Cualquier inconveniente, en la privacidad, en el poder de monopolio, en el uso de energía o las emisiones de carbono, en las prácticas de empleo o en la evasión fiscal; se ha minimizado en gran medida.*
>
> *Los gobiernos de todo el mundo ya han promulgado una serie de nuevas regulaciones e impuestos, y esto tendrá el efecto de aumentar su control e influencia en Internet. Estas regulaciones son necesarias, dice el argumento, porque a las grandes empresas de TI que desempeñan funciones sociales y económicas clave se les ha otorgado demasiada libertad, forzan la infraestructura local y carecen de procedimientos suficientes para garantizar la disponibilidad de los servicios necesarios que brindan. Las nuevas regulaciones e impuestos están destinados a proteger la privacidad individual, mejorar la ciberseguridad, aumentar la inversión en infraestructura, mitigar los incidentes de tiempo de inactividad y/o limitar las interrupciones sociales* (Uptime Institute, 2018).

Lo cual nos indica que las regulaciones en materia fiscal para los proveedores de servicios por Internet para que paguen impuestos por tales servicios, se han convertido en una realidad en la cual, el gobierno busca regularizar el uso de Internet. Sin embargo, esto no solo afecta a las empresas proveedoras, también al comercio electrónico y a las Pymes.

En México actualmente las organizaciones deberán pagar impuestos por cada transacción que realicen utilizando una plataforma electrónica. Por otro lado, tenemos la modernización de los centros de datos que almacenan dichos servicios, ya que al generarles un nuevo impuesto; el cual busca regular y estandarizar los

centros de datos, obliga a las organizaciones a realizar una inversión en dicha modernización.

4.1.3 Resiliencia

La transición a la resiliencia distribuida no será fácil

> *Las interrupciones disruptivas y a menudo de alto perfil continuarán a medida que los operadores lidien con las complejidades de implementar sistemas híbridos distribuidos en múltiples centros de datos y servicios. La industria de TI está en medio de una transición grande y difícil: desde centros de datos únicos, seguros y estrechamente administrados, a una red de sistemas distribuidos, interconectados dinámicamente, que despliegan Nubes, micro servicios y redes definidas por software (SDN). La nueva arquitectura está emergiendo con el tiempo, construyéndose en parte con nuevos centros de datos, redes y sistemas, y en parte construyendo sobre la infraestructura existente. El resultado es una cuadrícula distribuida complicada que admite una variedad de aplicaciones y servicios. La evidencia sugiere que la mejor manera de garantizar la resistencia; pero no necesariamente la más barata, es combinar redundancia a nivel de sitio y red con TI distribuida y arquitecturas resistentes utilizando tecnologías en la Nube* (Uptime Institute, 2018).

Las organizaciones al buscar la modernización de sus centros de datos, debido a las nuevas necesidades del sector, poco a poco han convertido la administración de los centros de datos en una tarea titánica de administrar, esto debido a la complejidad con la cual deben lidiar los departamentos de *TI* día con día. La integración de nuevas soluciones para la administración, migración a la Nube, incorporación de procesos basados en la analítica de datos, *Big Data*, *Machine Learning*, Inteligencia Artificial y principalmente la incorporación de los dispositivos del *IoT*; han tenido el efecto en las organizaciones de una resistencia al cambio debido a sus costos de implementación o en algunos casos de realizar

implementaciones con la base de infraestructura existente, lo cual ha complicado las cosas debido a que su infraestructura en algunos de los casos no se encuentra apta para tal cambio.

4.1.4 Implementación

La exageración del centro de datos perimetrales supera la implementación

> *La demanda de pequeños centros de datos periféricos está llegando más lentamente de lo previsto. Los problemas con la seguridad, los costos, los modelos comerciales, la integración, las redes y la implementación de 5G limitarán la adopción. Se está produciendo un resurgimiento en la TI distribuida desde el IoT, la aparición de la informática de borde móvil (MEC) y otros enfoques nuevos. De estos, IoT está teniendo el primer impacto; La proliferación de dispositivos conectados, sensores, medidores, teléfonos móviles y dispositivos médicos son algunos ejemplos de tecnologías que ahora se implementan a gran escala con la introducción de otras como la realidad virtual y la realidad aumentada. Los datos generados están impulsando la demanda de centros de datos de todo tipo: los cercanos ("local edge" o "edge") para el procesamiento, análisis y enrutamiento de primera línea; aquellos dentro de un área local ("near" o "regional edge") para conectar, integrar y redirigir; y aquellos que están lejos, como instalaciones económicas de hiperescala ("core") para su posterior procesamiento, análisis y archivo. Los micro centros de datos, que pueden implementarse como bolsas de capacidad discreta o como bloques modulares e incrementales de implementaciones grandes, encontrarán muchos casos de uso: para actualizaciones eficientes de armarios de red y para soportar el análisis, almacenamiento y resistencia de datos de dispositivos IoT. Fábricas inteligentes, edificios y otros lugares* (Uptime Institute, 2018).

Las ventajas competitivas en la utilización de la Computación al Borde, han permitido el incremento de los dispositivos del *IoT* de una manera exponencial, sin embargo, la adopción de la Computación al Borde, ha sido implementada por las organizaciones de manera paulatina, esto es debido a que los centros de datos a pesar de verse beneficiados con la baja latencia y respuesta que les proporciona la Computación al Borde, han encontrado una complejidad de interacción con los centros de datos tradicionales que no cumplen con las características necesarias de confiabilidad en su infraestructura y que a su vez no cuentan con los procesos adecuados para realizar una integración exitosa debido a la complejidad que se ha presentado en la implementación de los centros de datos al borde.

Aunado a esto, debemos tomar en consideración que los centros de datos se encuentran con problemas de infraestructura, debido a la revisión poco eficiente de su infraestructura y de sus procesos de seguridad. Por lo que la integración de los micro centros de datos que proporciona la Computación al Borde también representa un gran reto de integración y de administración por parte de las organizaciones.

4.1.5 Conectividad

La conectividad es la reina, los operadores trabajan para construir la estructura de red

> *La demanda de conexiones de red rápidas y seguras para socios comerciales y operadores de Nube continúa creciendo a medida que la red se convierte en el componente crítico de la infraestructura híbrida. Las redes SDN[50] son plataformas seguras en línea que permiten que las interconexiones privadas virtuales a otros en la plataforma se aprovisionen rápidamente, de modo que las organizaciones puedan conectarse fácilmente a Nubes públicas, proveedores de servicios, socios y proveedores en diferentes centros*

[50] Redes definidas por Software. Nota del autor.

> *de datos y regiones. Esto debería extender la capacidad de enrutar el tráfico de forma segura y previsible entre diferentes centros de datos y, en última instancia, reducir los costos de las organizaciones para conectarse. Con el rango de aplicaciones y socios en crecimiento, algunos que requieren conexiones de baja latencia o gran ancho de banda para aplicaciones como IoT o resiliencia distribuida, la buena conectividad ahora es una prima para el sector de colocación. A medida que las huellas digitales de las organizaciones continúan expandiéndose, la demanda y la dependencia de los tejidos SDN crecerán* (Uptime Institute, 2018).

Las necesidades que en la actualidad demandan las organizaciones de una red rápida y confiable, han ocasionado que se tengan que tomar medidas de administración de los servicios de conexión entre las diversas soluciones, lo que ha implicado que se tengan que utilizar redes definidas por software para mejorar la conectividad entre los diversos equipos y servidores, mejorando los tiempos de respuesta, pero incrementando el tráfico de la red de Internet, lo cual a pesar de brindar un beneficio para las organizaciones, al mediano plazo, incrementara el flujo de datos que se generan, saturando el ancho de banda si este no se encuentra debidamente soportado por la infraestructura del centro de datos.

4.1.6 Habilidades

La escasez de habilidades forzará nuevas estrategias de fuerza laboral

> *Incluso con la automatización y la Inteligencia Artificial, la escasez de personal del sector del centro de datos se intensificará. Para mantener el ritmo de la demanda hoy y para evitar un déficit precipitado mañana, los operadores de centros de datos trabajarán para diversificar el grupo de talentos con nuevas iniciativas, estrategias de contratación y capacitación de la fuerza laboral. Los resultados de la encuesta de Uptime Institute Research sugieren que los centros de datos*

> *continuarán luchando para reclutar y retener suficiente personal calificado para mantener y desarrollar operaciones confiables. En nuestra encuesta de 2018, el 45% de los encuestados dijo que la escasez de personal de las instalaciones del centro de datos limitará el crecimiento de la industria del centro de datos en los próximos cinco a siete años. En otra encuesta, el 38% de los operadores de centros de datos dijeron que tenían dificultades para encontrar candidatos calificados para trabajos abiertos y el 17% tenían problemas para retener al personal. La escasez de habilidades se sentirá en toda la industria, con empresas que luchan por cubrir puestos de instalaciones tradicionales como operaciones y administración, seguridad, conectividad de red, aprovisionamiento de Nube e ingeniería mecánica; pero también cumplimiento, contratos / SLA / gestión de proveedores, software, gestión financiera, gestión de la cadena de suministro y responsabilidad social y corporativa* (Uptime Institute, 2018).

Uno de los grandes problemas que se han suscitado con el crecimiento exponencial de los dispositivos del *IoT*, la Inteligencia Artificial, el *Big Data* y el *Machine Learning*, ha sido principalmente que en los centros de datos se han modernizado de tal forma que la administración se ha vuelto más compleja. Sin embargo, las organizaciones dada la complejidad, no han logrado brindar un nivel de capacitación adecuado al personal; por lo que el mismo no se encuentra debidamente entrenado para poder administrar la complejidad que ahora se presenta en los centros de datos.

De igual forma, es esta misma falta de capacidad del personal que las implementaciones de los nuevos dispositivos, principalmente del *IoT* no tengan la adecuada implementación en las organizaciones, dejando brechas de seguridad que podrían afectar a los centros de datos de las organizaciones.

4.1.7 Amenazas

Las amenazas crecientes requerirán nuevos enfoques de "confianza cero"

> *Las vulnerabilidades de seguridad ahora afectan las instalaciones de misión crítica. Las organizaciones deberán adoptar políticas más estrictas con respecto a los equipos, servicios, contratistas, proveedores y personal del centro de datos. Los operadores de centros de datos son cada vez más conscientes de que, si bien los sistemas de TI son objetivos obvios, de alto perfil y probablemente bien entendidos para piratas informáticos y delincuentes, necesitan invertir más dinero y atención en la infraestructura física. La seguridad del perímetro físico, el acceso al centro de datos y la seguridad privada interna y la gobernanza siguen siendo un foco de atención; sin embargo, otras áreas a menudo se descuidan. Hay una creciente preocupación por la necesidad de examinar y vigilar no solo a las personas sino a todo el equipo que se lleva a un centro de datos. A medida que los centros de datos se vuelven más inteligentes y más conectados, utilizando controles y equipos basados en IP, las formas en que pueden verse comprometidos aumentan. Las organizaciones a menudo se conectan a los controles a través de redes privadas y otorgan acceso al mundo exterior para obtener soporte de proveedores de sistemas y equipos de gestión / automatización de edificios. Las amenazas están creciendo, desde contratistas externos hasta servicios operativos en la Nube y equipos cada vez más automatizados, basados en software: la inversión en seguridad y el enfoque deberán mantenerse a la par* (Uptime Institute, 2018).

Por lo que podemos observar el nivel de las amenazas a los diversos centros de datos que surgen derivado de malas implementaciones de la seguridad informática, año con año crecen de manera exponencial. Esto es debido al alto número de dispositivos nuevos que son incorporados de manera deficiente a la infraestructura de red de las organizaciones, de igual forma, las medidas de auditoria y seguridad

informática de las mismas, en la gran mayoría de los casos no toma en consideración los dispositivos del *IoT* de una manera adecuada.

En donde los mismos encargados de la seguridad informática, dejan pasar por alto políticas y procesos que dejan abierta una brecha en la seguridad de la organización. Como pueden ser: software sin actualizaciones importantes, parches de seguridad en los sistemas, *passwords* de fábrica en los dispositivos y un largo etcétera, por lo que se debe actuar no en periodos programados sino en tiempo real de una manera constante.

El Instituto de Ciberdefensa, (2019) es una institución enfocada en promover la educación en seguridad informática, propone que la gestión completa de la ciberseguridad bajo el marco de trabajo del "*Cybersecurity Framework*" del *National Institute of Standards & Technology* (*NIST*), del Departamento de Comercio de los Estados Unidos, es el mejor método de llevarla a buen término y consiste en una serie de políticas divididas en cinco fases: Identificar, Proteger, Detectar, Responder, y Recuperar.

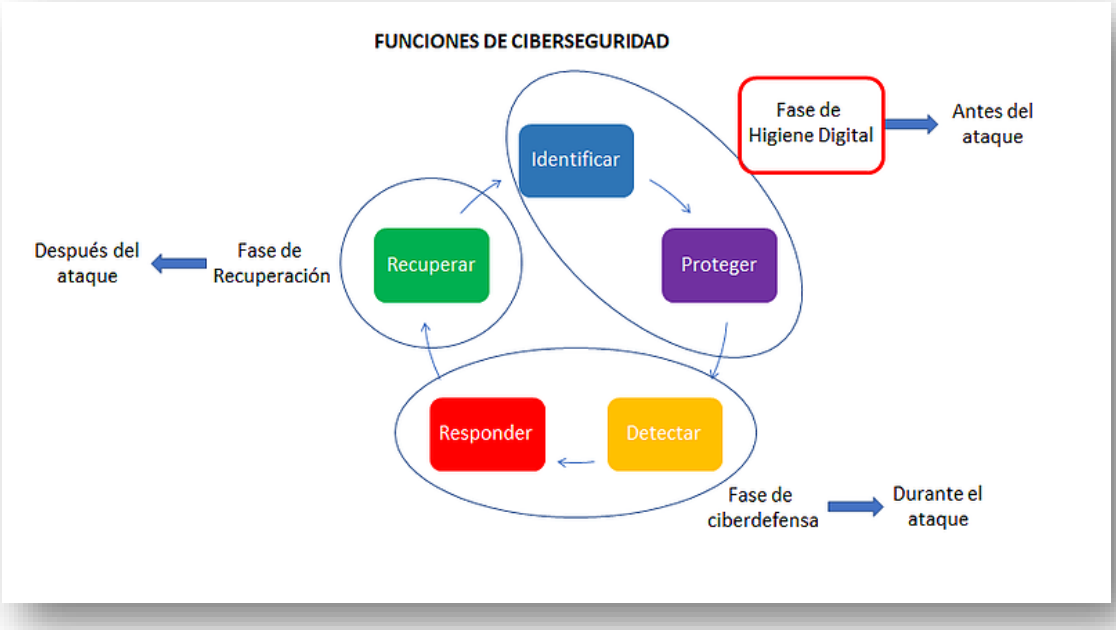

Ilustración 19 - Método de NIST
Fuente: (Instituto de Ciberdefensa, 2019)

De acuerdo con el Instituto de Ciberdefensa, (2019):

> *Muchas compañías se enfocan más en las funciones de Detectar, Responder y Recuperar, porque lógicamente la operación de seguridad te obliga a ello. En la función de Detectar es donde detectamos todos los incidentes, los cuales son siempre muchos. Luego en la función de Responder los atendemos, haciendo respuesta a incidentes y threat hunting (caza de amenazas). Y luego, cuando se cuela un ataque, pasamos a la función de Recuperar. Todo esto se hace en tiempo real. Por otro lado, las funciones de Identificar y Proteger muchas veces no son atendidas en tiempo real, porque no existe tal presión operativa inmediata. Durante la función de Identificar, identificamos todos los activos (hardware y software) y todos los usuarios en la red. Y la función de Proteger consiste en implementar la arquitectura de seguridad informática. Estas*

> *actividades generalmente no las administramos en un ciclo diario. Y esto es un error* (Instituto de Ciberdefensa, 2019).

Aquí es donde podemos observar que la gran mayoría de las organizaciones en la parte de seguridad informática, son reactivas a las amenazas, debido a que las previsiones de los problemas se realizan por medio de periodos de verificación. Sin embargo, dejan de lado la parte de la higiene digital en donde los procedimientos deberían de realizarse e implementarse en tiempo real y antes de que exista la posibilidad de un ataque.

La ANSSI (*Agence nationale de la sécurité des systèmes d'information*) (2019) del gobierno francés desarrolló una Metodología de Higiene Digital que consiste en 40 políticas divididas en 12 categorías:

1) Conocer todos los usuarios y sistemas
2) Controlar la red
3) Actualizar el software
4) Autenticar a los usuarios
5) Asegurar los puntos de acceso
6) Asegurar la red
7) Proteger la red de la Internet
8) Monitorear los sistemas
9) Administrar la red en forma segura
10) Control de acceso físico
11) Entrenar a los usuarios
12) Hacer auditorías

En donde se definen un total de 94 controles que debemos implementar y revisar continuamente para tener una Higiene Digital bien implementada dentro de las organizaciones (Agencia Nacional de Seguridad de Sistemas de Información (ANSSI), 2019).

4.2 Tendencias de las nuevas tecnologías en el centro de datos

4.2.1 La Inteligencia Artificial (IA)

En su publicación titulada: **"La Inteligencia Artificial revoluciona la gestión del Centro de Datos"** Revilla, (2019) comenta que los centros de datos se han visto beneficiados con la aplicación de proyectos de Inteligencia Artificial (*IA*) lo cual ha mejorado sus niveles de servicio de los proveedores que ofrecen servicios de *Cloud Computing* y por ende han reducido significativamente su impacto al medio ambiente.

Es gracias a estas tecnologías que ha sido posible mejorar de manera sensible la eficiencia energética, optimizar la distribución de carga o a mejorar la detección oportuna y resolución de incidentes debido al análisis que proporciona la Inteligencia Artificial. A medida que los centros de datos se han vuelto más complejos, grandes y cada vez más interconectados a la Nube, la *IA* se ha convertido en una herramienta esencial la cual evita el sobrecalentamiento de los equipos instalados dentro del centro de datos, de esta forma ahorran energía y se reducen los gastos inherentes del consumo energético de manera substancial.

La *IA* ayuda en el análisis predictivo en una de las tareas del área operativa que son criticas del centro de datos como lo es la distribución de las cargas de trabajo al conseguir que estas mismas sean más predecibles y fáciles de gestionar ya que las nuevas herramientas de la *IA* tienen la capacidad de aprendizaje de las experiencias y datos del pasado para así poder ejecutar una distribución de cargas de manera más eficiente en el futuro.

Lo que nos brinda un mejor seguimiento del rendimiento de los servidores, la utilización de discos de almacenamiento y principalmente la congestión de la red de datos. Así como la optimización de los sistemas de almacenamiento del servidor, la búsqueda de posibles puntos de falla en el sistema, la mejora de los tiempos de

procesamiento y la reducción de factores de riesgo que se harán más rápidos y eficientes facilitando la máxima optimización del servidor.

Los tiempos de inactividad de los centros de datos de manera no planificada, representan pérdidas económicas a las organizaciones, debido a esto los administradores de los centros de datos, deben de contar con una identificación rápida de los problemas que son el origen de las fallas, priorizar su resolución y recuperar el sistema antes de que se produzca una pérdida de datos significativa que represente un impacto directo a la organización.

En este sentido, los Centros de Datos que se auto gestionan hacen uso de aplicaciones de Aprendizaje Profundo (*Deep Learning*) para predecir fallos antes de tiempo. Además, utilizando sistemas de recomendación basados en *Machine Learning*, las soluciones a cualquier incidente se localizan y atajan rápidamente o, incluso, antes de que se extiendan y provoquen degradaciones de servicios.

Al realizar una incorporación del aprendizaje automático, la *IA* puede asumir el trabajo rutinario del monitoreo de enormes cantidades de datos que se generan y hacer más eficientes los procesos de los administradores de los centros de datos en cuestión de calidad de las tareas que manejan.

La *IA* tiene el potencial de tomar decisiones más inteligentes sobre la optimización del almacenamiento o la organización por niveles. Esto ayuda a transformar la administración del almacenamiento aprendiendo los patrones de E/S y los ciclos de vida de los datos, ayudando a mejorar las soluciones de almacenamiento.

La *IA* también permite mejorar la seguridad en los datos. Gracias a la introducción de sondas recolectoras de datos capaces de correlacionar *logs*, es posible detectar y bloquear automáticamente ataques difíciles de detectar. Como, por ejemplo, en las Amenazas Persistentes Avanzadas (*APT*), uno de los principales retos de seguridad en la Computación en la Nube.

Con el uso de la *IA* en la gestión de la infraestructura del Centro de Datos, es posible anticipar en la predicción, prevención y resolución de cualquier contratiempo en las instalaciones, dando lugar a un aumento significativo de la eficiencia, consiguiendo mejoras operativas y una infraestructura más inteligente y fiable.

4.2.2 La Nube en el centro de datos

Los centros de datos están cambiando en sus necesidades de espacio y la creciente demanda de almacenamiento que se ha generado en los últimos años, además de la adopción de los servicios de la Nube por parte de las empresas que es una tendencia creciente. Debido a esto, se traducirá en una reducción del espacio de almacenamiento en las empresas; pero provocara una mayor demanda del espacio requerido por las empresas que brindan los servicios en la Nube.

Por otro lado, el número de dispositivos conectados a Internet cada día es mayor y continua en crecimiento día con día, por lo que la generación de datos y toda la información necesaria que debe procesarse en los próximos años se pronostica que se quintuplicarán en el 2021 de acuerdo a los estudios realizados por Cisco[51].

Adicionalmente a lo anteriormente expuesto, la cantidad de datos almacenados en los dispositivos será de 4.5 veces mayor que los datos almacenados en los centros de datos en la actualidad. Lo que representa un cambio global en la forma en la que la información deberá procesarse y principalmente almacenarse hacia una infraestructura externa.

Las empresas buscan una forma de almacenar la información generada utilizando los diversos servicios en la Nube, como son las Nubes públicas o privadas o en última instancia haciendo uso de Nubes hibridas en las cuales puedan diversificar sus datos de forma que realineen sus estrategias y recursos de forma óptima. Debido a que la latencia de los dispositivos interconectados a la Nube representa

[51] Véase (Cisco VNI Mobile, 2019)

un factor fundamental para realizar una transición de una infraestructura propia a una externa como es la Nube.

El *IoT* trae consigo aplicaciones y cargas de trabajo que exigen respuestas de forma casi inmediata, lo que significa que estarían trabajando en tiempo casi real debido a la baja latencia de los dispositivos. Lo que está obligando a las empresas a remplazar la capacidad de cómputo y su infraestructura de redes lo más cercana de los dispositivos para minimizar el impacto que la baja latencia ocasiona en las transmisiones de datos.

Con este tipo de aplicaciones que son sensibles al rendimiento o a la latencia, el modelo de transmisión directa de dispositivo a Nube, es realmente insuficiente o en definitiva poco rentable en su ejecución. Por lo tanto, un buen número de dispositivos de *IoT* terminarán siendo almacenados en los centros de datos corporativos desplazando la integración a la Nube de los mismos en su mayoría.

El impacto de la Nube y el *IoT* han llevado a un proceso de digitalización casi completa de las empresas, lo que representa una generación de valor a las mismas al poder contar con la información necesaria para la toma de decisiones. De esta manera pueden generar valor, mejorar su eficiencia, trabajar de manera más rápida y mejorar sus resultados. La arquitectura más actual de los centros de datos responde ya a estas necesidades

De acuerdo con Canal Comstor, (2019) durante el año de 2018, se realizaron diversos estudios e investigaciones de las principales herramientas que impulsaron el crecimiento de la Computación en la Nube y los centros de datos. En las cuales se observa que existe la garantía de que la consolidación de la Nube hibrida por parte de las organizaciones mexicanas será la principal opción de la Computación en la Nube, ya que la misma responde a los cuestionamientos principales de seguridad de los usuarios con las Nubes públicas y privadas; así como la forma más

adecuada de almacenamiento de datos para alojar las cargas de trabajo de las empresas.

A pesar de que uno de los grandes desafíos de la Nube, es la seguridad y confiabilidad de los datos, la posibilidad de programar la carga de trabajo ganando escalabilidad con la Nube pública y mejorando la seguridad al interior de la Nube privada, han significado un ambiente único, el cual posibilita la utilización de dos Nubes de tipos distintos para realizar procesos completamente diferentes de manera simultánea.

Por otra parte, los centros de datos, adquieren mayor importancia para el almacenamiento de datos importantes y relevantes que serían considerablemente más costosos si fueran trasferidos a la Nube. Por lo cual las empresas están apostando hacia la modernización de sus infraestructuras convirtiendo los centros de datos de manera más versátil y más poderosos para poder recibir los conjuntos de datos masivos, con análisis de Inteligencia Artificial y *Machine Learning*, así como *Business Intelligence* (*BI*)

El nivel de maduración de la Computación al Borde, es otro punto que debe destacarse en el 2019 en México. Aunque se requiere todavía un modelo de negocios más eficiente, los empresarios comienzan a observar en sus infraestructuras una manera de aumentar la velocidad de las conexiones del *IoT*. Esto derivado de las previsiones a futuro que indican un total de 5,635 millones de sensores inteligentes y otros dispositivos de *IoT* siendo utilizados en el mundo para el 2020, generando cantidades inmensas de datos.

Un estudio realizado por Gartner (2019), apunta que *SaaS* está impulsando el crecimiento en casi todos los segmentos de software, particularmente en el *CRM*, plataforma de relación con el cliente.

> *El software en la Nube creció cerca del 22% durante el 2018, comparado con el 6% de crecimiento de todas las otras formas de software. El SaaS impulsa a todo el mercado de TI, colaborando para que las estimaciones de crecimiento durante el 2019 sean de 3.8% mayores que el año anterior* (Gartner, 2019).

Los centros de datos deberán estar más preparados para recibir cargas de trabajo diversificadas y que no se detengan como conjuntos de datos que puedan ser transferidos hacia la Nube; así también, verán el fortalecimiento del *SaaS* y el *Edge Computing* como una opción para respaldar al *IoT*.

4.2.3 El Internet de las Cosas en el centro de datos

Las expectativas que se tiene para el Internet de las cosas *IoT* se centran en torno a un modelo descentralizado de implementación que es la Computación al Borde en el que los diversos dispositivos del *IoT* se ubican en los puntos cercanos y que se resumen a continuación:

En su artículo titulado: ***¿Qué está haciendo el IoT a tu centro de datos?*** Gold, (2018) nos comenta que el centro de datos y la Nube continúan siendo partes críticas dentro de la infraestructura de las organizaciones y es debido al enorme crecimiento que las implementaciones del *IoT* que continúan teniendo un gran impacto en las mismas.

Incluso los despliegues que se han tenido en relación a la utilización de la Computación al Borde que tienen la capacidad de transmisión de datos a una infraestructura central para un análisis más detallado indican que es difícil argumentar que el aumento de los dispositivos de *IoT* no han cambiado los requisitos y las expectativas en el centro de datos.

Uno de los principales factores claves es la conectividad y redes que deben existir como áreas principales en las organizaciones y debe ser considerado como el factor

principal que se requiere en los centros de datos, para que los dispositivos de *IoT* funcionen de manera adecuada.

> *La conectividad es la respuesta corta a la pregunta, pero es una especie de conectividad consciente, dependiendo de lo que el negocio está haciendo y de dónde quieren poner el resto, por lo tanto, es posible que parte de esa información deba ir a algún tipo de almacenamiento profundo, por lo que puede demandar una ubicación muy ecológica, de bajo costo y alta latencia. O es posible que deseen una ubicación transaccional muy rápida y de gran volumen, en cuyo caso (los centros de datos o las instalaciones de los clientes) probablemente estarán cerca de los centros de las ciudades o se ubicarán a poca distancia* (Gold, 2018)

El impacto holístico que tienen en los centros de datos los dispositivos de *IoT* es principalmente en su infraestructura de *TI*, la cual incluye los servidores de datos, el almacenamiento, las redes, la seguridad y la administración de los sistemas involucrados. Los cuales pueden generar cantidades impresionantes de datos que van en una sola dirección de manera pasiva, en lugar de aplicaciones de *IoT* más activas que involucraran acciones y respuestas de manera automatizada que se encuentran basadas en el estado de los sensores que son los que proporcionan los datos.

Pero la principal manera en que *IoT* afecta a los centros de datos seguirá siendo como controlador de capacidad, en particular para implementaciones que requieren coordinación en múltiples sitios combinados con baja latencia. Las implementaciones de *IoT* cada vez son más frecuentes dentro de las organizaciones, lo que implica que debemos de ver más allá del simple hecho de una implementación, ya que se exigirá a los centros de datos ya sea en cómputo, almacenamiento o conectividad la necesidad de aprender a manejar funcionalidades completamente nuevas principalmente en la administración de *TI.*

Esa es una gran tarea, complicada por el hecho de que las implementaciones de *IoT*, a pesar de su rápido crecimiento, aún se encuentran en las primeras etapas, y nadie está completamente seguro de cómo caracterizar su impacto general en las operaciones del centro de datos.

Las investigaciones realizadas en los últimos años apuntan a que el 60 por ciento de los proyectos de *IoT* están fallando o se encuentran detenidos en estado de prueba de concepto. Lo cual indica la necesidad que la tecnología requiere ser mejorada para destrabar los procesos de implementación de los proyectos basados en el *IoT*. (Canal Comstor, 2018)

La empresa de consultoría James Brehm & Associates, citado por Canal Comstor, (2018) enumera tres puntos que deberán de ser mejorados en el *IoT*, las cuales son:

1) ***La falta de liderazgo en el proceso:*** *son muchos los profesionales y los procesos existentes que se encuentran enfocados al IoT, lo cual motiva que los procesos de implementación de la tecnología pierdan su centralización en la mano de un gerente o de una persona especifica que coordine las acciones.*
2) ***Crear un proyecto de IoT solamente para decir que existe:*** *el IoT está siendo utilizado en el mercado para mejorar la experiencia del cliente en la relación con la marca. Por ello, crear toda una estructura que contemple acciones de IoT, pero con una tasa de retorno insuficiente para la empresa, no colabora para las estrategias y mucho menos para las metas del negocio.*
3) ***La falta de visión sólida del IoT:*** *no tener la seguridad de cómo el Internet de las Cosas conseguirá las metas del objetivo, puede traer inseguridades para el negocio y para todas las inversiones que fueron hechas. Las metas muy por debajo de la potencialidad de las herramientas o crear plataformas tan sólo para un uso del IoT en los*

> *negocios, pueden ser el fin de un plan y la insatisfacción con la tecnología empleada* (Citado por Canal Comstor, 2018).

La falta de infraestructura interfiere en el mercado de *IoT*; además de los tres puntos citados por la consultora James Brehm & Associates y que se encuentran directamente relacionados a la administración interna de los negocios. Nos indican que los factores externos pueden interrumpir el desarrollo de los dispositivos del *IoT*, adicionalmente, los administradores necesitan conocer todo el potencial que se puede obtener con el uso del *IoT* y como pueden ser utilizadas de forma que den valor a sus negocios.

De igual forma, otro de los puntos cruciales es el desarrollo de la mano de obra especializada, por lo que las organizaciones se encuentran ligeramente perdidas con la cantidad de tecnologías, herramientas y sus usos, confundiendo los planes de los administradores de *TI* que necesitan realizar muchas pruebas de efectividad para echar a andar un proyecto de manera exitosa.

5 Capítulo V - Análisis de resultados

Con base en lo anteriormente expuesto, se procede a realizar el análisis de las preguntas de investigación para fundamentar las hipótesis de la presente investigación.

5.1 Preguntas de Investigación.

5.1.1 Primera pregunta de Investigación

> *¿Cómo impacta la implementación del IoT en un centro de datos con más de cinco años de antigüedad?*

Los centros de datos de las organizaciones se consideran como parte medular de las mismas. Sin embargo, la tecnología avanza a grandes pasos; tanto que las implementaciones de tecnología a pesar de que cada vez son más ágiles, sus complejidades en la integración cada día van dando la pauta a nuevos desafíos para los administradores de los centros de datos al interior de las organizaciones.

Además, derivado del crecimiento exponencial de los canales de comunicaciones, lo cual también afecta la complejidad de la infraestructura de red, la implementación, la administración y lo que podemos definir como Computación al Borde. Por lo que el panorama para las empresas actualmente, es de que al día de hoy deben de prepararse para los retos actuales y futuros que las nuevas tecnologías representan, comenzando por ofrecer capacidades flexibles de expansión y transmisión de datos, sin dejar de lado la seguridad como un factor crucial de la organización.

Las organizaciones tienen en promedio en sus centros de datos un ciclo de vida de tres a cinco años para poder cambiar sus sistemas y parte tecnológica, es decir, en un periodo de tres años los sistemas que fueron diseñados o adquiridos para las organizaciones, presentaran cambios sustanciales en su forma de trabajar, sin embargo, para la parte tecnológica el ciclo de vida de los equipos es más largo, de cinco años en promedio.

Lo que representa en términos económicos un plazo amplio para la adquisición de nuevas tecnologías en el centro de datos. Pero la parte de la infraestructura tiene un tiempo de vida mucho más amplio, el cableado estructurado se diseña para durar entre diez y veinte años. Lo que conlleva a un “cuello de botella” en cuanto a desempeño y velocidades de transmisión de datos derivado de los cambios de tecnología y una mala planeación a futuro.

Las nuevas tecnologías, principalmente el *IoT* presenta unas características muy especiales en su implementación con centros de datos que tienen más de cinco años de haber sido implementados; como son: la integración de los nuevos dispositivos al centro de datos y sus respectivos *racks* o gabinetes, el manejo de la energía eléctrica necesaria para poder suministrarse a los dispositivos de manera correcta, la introducción de dispositivos *PoE* (Por sus siglas en inglés, *Power over Ethernet*), la complejidad en la administración de los dispositivos de *IoT* y su integración a los sistemas actuales de administración de las organizaciones, solo por mencionar algunas de ellas.

El impacto que ocasiona la implementación de la tecnología del *IoT* es bastante considerable, si este no es debidamente planificado. El principal impacto que tiene se encuentra en la parte económica, derivado de un cableado estructurado que no se encuentra debidamente implementado y certificado.

Adicionalmente a esto, muchas de las implementaciones que se realizan dentro de los centros de datos no cuentan con el cableado requerido para así poder funcionar adecuadamente, derivando en fallas de administración, conectividad, funcionalidad y desempeño.

Los niveles de transmisión de datos hacia los centros de datos, han derivado que las implementaciones del *IoT* tendrán un impacto significativo dentro de los centros de datos, al forzar a romper el paradigma de un centro de datos tradicionalmente centralizado. Lo cual cambiara la forma de gestionarlos en un futuro cercano.

Es debido a la continua expansión derivada del crecimiento en los centros de datos que una infraestructura de cableado estructurado tiene que ser bien planificada y es una parte fundamental para el éxito de las organizaciones en el presente y en un futuro cercano. De igual forma, la confiabilidad, la capacidad de administración, la escalabilidad y la flexibilidad son factores importantes para así dar cabida a los cambios en el crecimiento de la infraestructura

Por lo que la infraestructura de cableado estructurado de los centros de datos actualmente, deberá de estar diseñada para ofrecer una ventaja competitiva y a su vez, generar un menor costo de propiedad del mismo. Debido a que la evolución del centro de datos en el mediano plazo, ha generado que se tengan velocidades de transmisión de datos cada vez más altas, como las velocidades de 40G y 100G para poder soportar las nuevas aplicaciones de futuras generaciones.

De igual forma, la Computación en la Nube y la cada vez creciente virtualización, al igual que la Computación al Borde, deben de garantizarse desde un inicio del proceso de planeación y diseño de la infraestructura del cableado del centro de datos.

La creciente instalación de los dispositivos de *IoT*, ha demostrado que existen problemas de implementación hacia los centros de datos que tienen más de cinco años de antigüedad, derivados de una mala planeación, una administración deficiente y principalmente que se ha dejado de lado la integración de los mismos a las políticas de seguridad informática.

Como podemos observar del creciente número de ataques que los dispositivos del *IoT* han tenido en los últimos años. Además de generar costos adicionales que no se tenían contemplados en las planeaciones iniciales de las organizaciones en sus centros de datos.

El *IoT*, ha estado esperando por bastante tiempo la implementación de la red *5G*, lo cual le permitiría tener un “boom” exponencial en su implementación, sin embargo, esto mismo incrementara la cantidad de dispositivos que puedan enlazarse al centro de datos, aumentando el tráfico de datos, así como la complejidad en la gestión de los mismos por parte de los administradores de sistemas.

No podemos dejar de lado las tecnologías que son inherentes al *IoT* las cuales también tienen una implicación en el centro de datos como son la Inteligencia Artificial, *Machine Learning* y *Big Data*. Las cuales también tienen un gran impacto en el desempeño y funcionalidad del centro de datos, debido a que las organizaciones cada vez hacen más uso de dichas tecnologías para generar valor a las mismas.

En conclusión, podemos decir que el impacto que tienen las nuevas tecnologías y principalmente el *IoT* en los centros de datos con más de cinco años de antigüedad, es muy alto en cuestión de infraestructura y modernización; la cual no se ha realizado durante años recientes, debido al alto costo que se requiere para la modernización de los centros de datos. Por lo mismo, si las planeaciones de los centros de datos no se realizan con una visión a futuro, al mediano plazo las nuevas tecnologías comenzaran a incrementar la complejidad y las fallas inherentes a la transmisión de datos en las organizaciones.

5.1.2 Segunda pregunta de Investigación

¿Qué consecuencias tiene el IoT en la seguridad de los centros de datos en las organizaciones?

La seguridad al interior de las organizaciones es uno de los factores fundamentales que deben tomarse en cuenta por los administradores de sistemas y realizar una planeación adecuada de los procesos que deben seguirse en la planificación y administración de los dispositivos del *IoT*.

Por lo mismo, siempre la seguridad será una constante preocupación al interior de las organizaciones, si bien se tienen implementadas medidas de seguridad en las mismas para proteger la información sensible, esto no ocurre de manera adecuada para los dispositivos del *IoT*.

El rápido crecimiento que ha sostenido de manera exponencial el *IoT*, ha propiciado una serie de ataques a los dispositivos interconectados a los centros de datos de las organizaciones, lo cual ha representado todo un reto para la seguridad informática de las mismas.

Dado el crecimiento exponencial que ha tenido en la actualidad la implementación de los dispositivos del *IoT*, se tienen actualmente instalados más de 150 billones de dispositivos que se encuentran conectados a los centros de datos de las organizaciones y que actualmente se registran 15 millones de ataques diarios a nivel mundial como nos lo indican las estadísticas presentadas por eSemanal (2019).

Por lo que podemos definir que los ataques a las vulnerabilidades que se generan con los dispositivos del *IoT* se incrementaran exponencialmente a medida que estos sean implementados por cada vez más organizaciones. Esto es derivado de que durante años la seguridad física era analógica, sin embargo, los equipos de *TI* poco se preocupaban por las cámaras de video vigilancia, por dar un ejemplo.

La situación de las organizaciones con la introducción del *IoT* ha cambiado radicalmente, dado la popularidad que tiene estos dispositivos y las implementaciones inherentes a la misma, como son la Inteligencia Artificial, el *Machine Learning* y el *Big Data*.

Por lo mismo se necesita que se les dé la importancia adecuada a dichas implementaciones en cuestión de seguridad y adicionalmente que estos mismos dispositivos sean considerados de manera adecuada en los procesos de Auditoria Informatica dentro de las organizaciones.

Se ha demostrado fehacientemente que las vulnerabilidades de los dispositivos instalados del *IoT* presentan un gran riesgo para las organizaciones, derivado del problema de que estos dispositivos no cuentan hasta el momento con procesos de seguridad incorporados de fábrica.

Lo que deja una puerta abierta para personal no autorizado de ingresar e instalar por este medio algún tipo de software malicioso lo que derivaría en la denegación de servicios (*DoS* por sus siglas en inglés *Denied of Service*) causando un grave daño a las organizaciones que no les brinden la importancia requerida a los dispositivos del *IoT*.

Si bien se habla de las posibilidades y el potencial que brinda el *IoT*, no deben perderse de vista las consecuencias derivadas de dichas implementaciones que se realizaran de manera exponencial en los próximos años. Tomando en cuenta que, en el futuro cercano, la utilización de la red 5G permitirá el crecimiento exponencial de los dispositivos del *IoT* en todos los sentidos, generando más puntos de falla de seguridad al interior de los centros de datos y por ende afectando a las organizaciones en sus procesos.

Por otro lado, tenemos las ciudades inteligentes (*Smart Cities*) las cuales harán uso de una gran cantidad de dispositivos inteligentes para su mejor aprovechamiento y generar valor a la sociedad, sin embargo, todos estos dispositivos del *IoT* deberían de estar debidamente protegidos mediante mecanismos de seguridad informática, para evitar accesos no autorizados a los mismos, dando pauta de que se altere información valiosa o esta misma sea utilizada para otros fines.

Aunado a la falta de experiencia del personal de *TI* que por ser un ámbito novedoso no cuenta con la suficiente experiencia en seguridad informática en materia del *IoT*, sin embargo, a pesar de que existen procesos y procedimientos de seguridad ya

probados y confiables, estos no se han implementado en su totalidad a las implementaciones de los dispositivos del *IoT.*

En conclusión, falta mucho por hacer en materia de seguridad por parte de las organizaciones y los fabricantes de dispositivos del *IoT*, pero principalmente centrarse en realizar cambios a los procesos y procedimientos internos de seguridad en las organizaciones para poder incorporar y auditar los dispositivos implementados del *IoT*.

Tomando en consideración que los mismos se encuentren conectados o enlazados por algún medio de comunicación a los centros de datos de las organizaciones. Ya que, de no comenzar a implementarse medidas, las consecuencias de una intrusión a los centros de datos, podría generar graves consecuencias derivadas de la falta de previsión y seguridad.

5.1.3 Tercera pregunta de Investigación

¿Qué efectos tendrá para el centro de datos de las organizaciones la implementación del IoT en la Nube?

Muchas organizaciones tienen un concepto erróneo de lo que es la Nube (*Cloud*) y la Computación en la Nube (*Cloud Computing*), suponen que la Nube es un lugar intangible que se encuentra en algún lugar del mundo y que siempre estará disponible y a su vez cuenta con un almacenamiento ilimitado, sin embargo, la Nube es en realidad un macro centro de datos que se encuentra ubicado en alguna parte del mundo.

Por lo que podemos definir que cuando hablamos de la Nube, nos estamos refiriendo al almacenamiento de páginas web y repositorios. Sin embargo, la Computación en la Nube se refiere a los servicios y procesos que pueden ejecutarse desde la Nube o mediante el uso de diversos tipos de Nube ya sea privada, pública

o hibrida, es decir, la Computación en la Nube hace uso de los recursos de almacenamiento de las diversas formas de Nube.

Durante los últimos años, hemos visto como las nuevas tecnologías poco a poco han transformado la forma en la que vemos la vida cotidiana, con el uso de teléfonos inteligentes (*Smartphone*), Servicios de Geolocalización, Nubes públicas, el incremento del uso de las redes sociales, el *IoT*, Inteligencia Artificial, reconocimiento facial, Voz sobre IP (*VoIP*) entre muchas otras que en gran medida han transformado la manera en que los procesos de las organizaciones se han transformado.

Por lo que para las organizaciones representa enfrentarse a un gran desafío para la incorporación de las nuevas características de negocio potencial que se tienen con el uso de las recientes tecnologías y así generar valor que redunde en ventajas competitivas y aumento de productividad.

En la actualidad, es difícil pensar que alguna de las organizaciones no haga uso de alguna manera del *IoT* en el corto plazo, es decir en un periodo de dos a cinco años, las organizaciones implementaran cada vez más dispositivos relacionados con el *IoT* en sus centros de datos.

Por lo que es necesaria la transformación de los centros de datos de las organizaciones las cuales deberán garantizar el aprovisionamiento y gestión de ambientes en donde el poder de cómputo, servicios de red, seguridad y almacenamiento sean la base fundamental de la modernización. En donde es necesario hacer funcionar el centro de datos y la Nube privada con la misma agilidad que ofrecen las Nubes públicas lo que ya no es una opción, y es una demanda que se convierte en vital para los negocios de las organizaciones.

De igual forma, es necesario aprovechar y potencializar el uso de las arquitecturas actuales de la Nube principalmente la Nube híbrida. En donde las tecnologías

permitan la administración, monitoreo y operación de ambientes híbridos de una manera consistente, en donde se puedan mover cargas de trabajo de una Nube publica a una Nube privada sin necesidad de reescribir aplicaciones o el conjunto de herramientas necesarias para su administración sin tener un mayor impacto en las organizaciones.

Una de las características principales y fundaméntales del uso del *IoT* es la baja latencia que requieren para poder funcionar adecuadamente y así optimizar sus tiempos de respuesta casi entiempo real. Derivado de la cantidad de datos que se generan y a lo anteriormente expuesto, la utilización de la Nube no es el medio idóneo para poder realizar implementaciones de los diversos dispositivos del *IoT*.

Uno de los principales problemas que impactaran en un futuro a los centros de datos es la cantidad masiva de información que se generara en los siguientes cinco años, lo que se derivara directamente de la cantidad dispositivos del *IoT* y que representaran todo un desafío a las redes de telecomunicaciones, adicionalmente a los administradores de *TI* en las organizaciones para poder gestionar la complejidad de la red.

Por lo que la Computación al Borde se presenta como la mejor solución viable para realizar la integración de manera adecuada de los diversos dispositivos del *IoT*, sin embargo, esto no quiere decir que la Nube no pueda ser utilizada para el almacenamiento de la información consolidada, ya que puede ser utilizada en conjunto con la Computación al Borde para potencializar y maximizar los beneficios de la utilización de dispositivos del *IoT*.

En conclusión, a pesar de las facilidades y características estratégicas que se presentan con la Nube, realizar una implementación del *IoT* en la Nube tendría efectos negativos en el rendimiento y desempeño de la red de cómputo, forzando a los centros de datos a ralentizar los procesos de procesamiento de la información

generada y a su vez afectar a los dispositivos que requieren de una respuesta en tiempo real.

5.2 Objetivos

Debido a que la Nube y adicionalmente el uso cada vez mayor de los servicios de que encuentran en la Nube han crecido de manera exponencial en los últimos años, ha provocado la modernización de los centros de datos tanto pequeños como los grandes centros de datos corporativos. Sin embargo, muchos de estos centros de datos no han tenido la adecuada modernización que los tiempos actuales requieren. Esto es debido a que, durante años los centros de datos, especialmente en México, no eran considerados para una modernización sustancial, debido a los altos costos que implica.

Las modernizaciones que los centros de datos han tenido en pocos años, han sido por lo general en cambios sustanciales en equipos activos, es decir servidores cada vez más potentes, pero de menor tamaño, *switches* con mayores capacidades de transmisión de datos y algunos que tienen la capacidad de enviar energía por medio del cableado estructurado existente, entre otros cambios sustanciales al interior de los centros de datos de las organizaciones.

Sin embargo, una de las partes fundamentales que no se le ha dado la debida atención, es el cableado estructurado existente en los centros de datos de las organizaciones. Lo cual implica un “cuello de botella” al momento de brindar todas las capacidades necesarias de transmisión de datos. Es ahí en donde el tiempo que se aumenta en la eficiencia del centro de datos, está causando un impulso a la consolidación de los centros de datos con los equipos de nueva tecnología. Lo que ha llevado a una hiperconvergencia de diversas tecnologías en los centros de datos.

Desde hace una década, las empresas han visto un crecimiento de manera exponencial en el uso del Internet y otras han tenido un éxito increíble en sus modelos de negocio que dependen de la presencia de un servicio ubicuo de Internet

combinado con un acceso rápido a las diversas aplicaciones que se ejecutan en los centros de datos. Lo que ha llevado a las organizaciones a obtener una mejor productividad, eficiencia energética y principalmente una rentabilidad al poder gestionar las necesidades derivadas del rápido crecimiento, las cargas de trabajo cambiantes, la creciente necesidad de almacenamiento y principalmente las nuevas tecnologías existentes de equipos en los centros de datos.

La modernización de un centro de datos de las organizaciones, no es una tarea sencilla de aplicar, derivado de las nuevas tecnologías tan cambiantes hoy en día, es necesario realizar una planeación estratégica de manera adecuada, debido a que las necesidades de comunicación y transmisión de datos, así como los requerimientos de tener la información actualizada en tiempo real, se vuelven cada vez más críticos para las organizaciones.

La cada vez más creciente necesidad de combinar aplicaciones que requieren soporte dentro del centro de datos, las cuales generan grandes volúmenes de información, pueden fomentar nuevas cargas de trabajo adicionales a los equipos instalados en los centros de datos, como son la Inteligencia Artificial (*IA*), el análisis de grandes volúmenes de datos (*Machine Learning*) y especialmente los dispositivos del *IoT* han convertido la gestión de los centros de datos demasiado compleja en los últimos años.

Los centros de datos en la actualidad, están ejecutando cargas de trabajo mucho más grandes y complejas, que a menudo son muy diferentes entre sí, por lo que los requisitos de equipo para poder ejecutarlos y administrarlos pueden variar demasiado entre una carga de trabajo a otra, en donde unas pueden requerir de mayor capacidad de procesamiento, almacenamiento o memoria, mientras que otras pueden requerir almacenamiento en la Nube o equipos especializados para su tratamiento.

El *IoT* ha venido a revolucionar diversos sectores en varios rubros de las industrias y es precisamente esta diversidad la que impacta la forma de administrar y gestionar los centros de datos, derivado de la gran cantidad de dispositivos que pueden ser interconectados entre si y que tienen que ser administrados por personal de *TI* en los centros de datos.

Los procesos de las organizaciones en sus centros de datos, no han tenido la adecuada revisión para poder gestionar de manera adecuada los dispositivos del *IoT* en la gran mayoría de los casos, lo cual representa una falla de seguridad en la auditoria Informática y principalmente en la seguridad de la información sensible de las organizaciones. Esto es derivado a que los diversos dispositivos instalados del *IoT* no cuentan con un sistema de seguridad de fábrica hasta el momento.

Aunado a que los centros de datos no han tenido una adecuada modernización, instalación y principalmente a la falta de revisión de procesos y procedimientos de seguridad que se requieren al interior de los mismos. Se ha dejado de lado lo principal que es la seguridad de que todos los dispositivos sean debidamente configurados e implementados con las medidas de seguridad que deberían tener todos los centros de datos con sus equipos de misión crítica. Lo que ha redundado en una proliferación de ataques masivos a los dispositivos del *IoT* de forma incremental año con año, en algunos casos con consecuencias económicas considerables.

Adicionalmente y derivado de las nuevas tecnologías, las normas del cableado estructurado han tenido que realizar ajustes en la manera de implementación de los diversos tipos de cableado en los centros de datos y en general en las organizaciones. Al actualizar las normas para permitir el adecuado manejo de los medios de transmisión de datos con velocidades superiores a los 40Gbps. Esto para poder hacer frente a la modernización necesaria que las nuevas tecnologías han impuesto a nivel mundial.

Recientemente, se han realizado innovaciones en el uso de los diversos equipos de cómputo para tratar de minimizar los costos de las organizaciones y así poder utilizar el cableado estructurado existente con los diversos dispositivos del *IoT* y así poder minimizar el gasto de implementación requerida para la modernización de los centros de datos y en general de las organizaciones.

Debido al potencial que tiene el *IoT*, podemos ver cada vez mayores implementaciones del mismo en las ciudades, lo cual implica que sean llamadas ciudades inteligentes (*Smart Cities*). Esto ha sido y será una constante creciente en los próximos años, para así poder brindar diversos factores de información que lleven a las organizaciones ya sean públicas o privadas a brindar valor a la sociedad en diversos ámbitos.

Sin embargo, es necesaria la implementación de manera correcta de los diversos medios de almacenamiento, transferencia de información y medios de comunicaciones entre las organizaciones y la sociedad en tiempo real, por lo que implica romper el paradigma del centro de datos tradicionalmente centralizado y a su vez hacer uso de las distintas herramientas existentes en la Nube y la Computación al Borde para la creación de centros de datos de manera reducida, pero con las capacidades suficientes de almacenamiento, procesamiento y gestión que permitan de alguna manera el procesamiento de los datos en el lugar donde estos se generan, lo que permitiría reducir el nivel de transferencia de los datos a la Nube y así poder generar análisis de datos de una manera eficaz, eficiente y confiable para las organizaciones.

En conclusión, cubrimos nuestro objetivo general, al demostrar que las nuevas tecnologías, en especial en *IoT* tendrán un gran impacto en la forma de administrar los centros de datos de las organizaciones y en especial en cuestiones de seguridad informática. Lo que implica romper el paradigma del centro de datos tradicional, de manera centralizada dentro de las organizaciones. De igual forma se cumplen los objetivos particulares al demostrar que las nuevas tecnologías en específico el *IoT*,

implican mayor uso de recursos informáticos y de procesamiento de datos, los cuales no todos tiene la capacidad de ser enviados a la Nube, debido a su baja latencia. Lo cual requiere de procesamiento de datos en tiempo casi real, lo que implica una adecuada planeación dentro de las organizaciones para adecuar que tecnologías y cuál sería la forma de manejarlas adecuadamente para que no represente un gasto innecesario; pero si una inversión correcta, tanto de recursos informáticos, como de inversión económica que reditúen en la generación de valor para las organizaciones.

5.3 Hipótesis

5.3.1 Hipótesis de la primera pregunta.

Las organizaciones están preparadas para enfrentar los retos de la administración de las TI al implementar las nuevas tecnologías emergentes específicamente los dispositivos del IoT en sus centros de datos derivado directamente de los pronósticos del incremento exponencial de dispositivos a nivel mundial

La infraestructura de las organizaciones, no ha tenido un proceso de modernización constante en los últimos años, derivado de los altos costos de la propia modernización que es necesaria, así como de los nuevos requerimientos de las tecnologías emergentes que deben estar alineados con la estrategia corporativa. Lo cual ha ocasionado que exista un alto impacto en los desempeños y funcionalidades de los centros de datos de las organizaciones. Por lo mismo, si las planeaciones de los centros de datos no se realizan con una visión a futuro, al mediano plazo las nuevas tecnologías comenzaran a incrementar la complejidad y las fallas inherentes a la transmisión de datos en las organizaciones.

Demostramos la hipótesis de la primera pregunta de investigación, la cual nos indica que las organizaciones no se encuentran debidamente preparadas para enfrentar los nuevos retos de las tecnologías emergentes. Principalmente el *IoT* al interior de sus centros de datos, debido que es una tecnología relativamente nueva, la cual no

cuenta con todas las medidas de seguridad necesarias para su implementación y que a su vez no existe hasta el momento alguna forma de buenas prácticas para su adecuada implementación en las organizaciones.

Lo que ha fomentado en que no se explote adecuadamente todo su potencial; sin embargo, basado en los pronósticos para los siguientes años, el incremento exponencial del uso de los dispositivos que tendrán como medio de comunicación el Internet, verán una afectación sustancial en sus rendimientos derivado directamente del ancho de banda necesario y de las implementaciones incorrectas del *IoT*, ya que muchas organizaciones están apostando por el envío de toda la información a la Nube, lo cual incrementara el tráfico de datos de manera significativa en los próximos años.

En conclusión, se demuestra que ***la hipótesis planteada NO se cumple en su totalidad***. Derivado de que las organizaciones a pesar de que se encuentran conscientes de que es necesario la modernización de sus centros de datos, están dejando de lado la infraestructura principal que es el cableado estructurado, la planeación estratégica de los procesos que deben utilizarse en la Nube (*Cloud Computing*) y los dispositivos que se integran a sus centros de datos con el *IoT*.

5.3.2 Hipótesis de la segunda pregunta.

Las organizaciones tienen un adecuado proceso de auditoria informática y seguridad para poder implementar con éxito los dispositivos del IoT en sus centros de datos actuales.

Las organizaciones no tienen un adecuado planteamiento para incorporar las tecnologías del *IoT* dentro de los procesos de auditoria informática, ya que están dejando de lado uno de los fundamentos primordiales de toda red: "*Todos los equipos y dispositivos que se encuentren conectados a una red deberán de estar debidamente protegidos contra amenazas internas y externas, mediante los mecanismos de protección informáticos adecuados*" (elaboración propia).

Por lo mismo, la seguridad es un factor determinante para los centros de datos de las organizaciones, debido a que almacenan y manejan información sensible y confidencial para las mismas, lo cual es un gran factor de riesgo de no realizarse un adecuado planteamiento de la seguridad Informatica en los dispositivos del *IoT* al incorporarse a los centros de datos, tal como lo hemos visto en los últimos años, los ataques que se han tenido hacia dichos dispositivos se incrementaran exponencialmente en los próximos años. Por lo cual las organizaciones y principalmente los administradores de *TI* deberán tomar medidas para minimizar los riesgos de una mala implementación de los dispositivos del *IoT*.

En conclusión, se demuestra que ***la hipótesis planteada NO se cumple***, ya que falta mucho por hacer en materia de seguridad por parte de las organizaciones, los fabricantes de dispositivos del *IoT* y los departamentos de *TI,* pero principalmente las organizaciones deben de enfocar sus recursos en realizar cambios a los procesos y procedimientos internos de seguridad en las organizaciones para poder incorporar y auditar los dispositivos implementados del *IoT* en los centros de datos.

5.3.3 Hipótesis de la tercera pregunta.

> *Las organizaciones tienen considerado migrar sus procesos de un centro de datos tradicionalmente centralizado hacia la Nube lo cual representa un ahorro considerable en su administración y marca la tendencia de la desaparición del centro de datos de manera tradicional (centralizado).*

Las organizaciones tienen un concepto erróneo de lo que significa la migración de los procesos a la Nube derivado de eso, se deben de realizar planteamientos muy puntuales de los beneficios de realizar migraciones a la Nube dado que la gran mayoría de las organizaciones no tienen una planeación estratégica de que procesos y cómo gestionar la administración de los recursos que se encuentren en la Nube publica, adicionalmente a esto, no todo es susceptible de ser migrado a la

Nube como es el caso del *IoT*, esto derivado de los niveles de baja latencia en los tiempos de respuesta que requieren dichos dispositivos y que deben ser casi en tiempo real.

Se ha hablado que la proliferación del uso de la Nube redituara a la larga en la desaparición de los centros de datos tradicionales, lo cual es completamente erróneo, si bien, fungirá como un factor alternativo de procesos y almacenamiento, este no será un factor determinante para que los centros de datos desaparezcan en el largo plazo; debemos recordar que la Nube está conformado por una serie de macrocentros de datos distribuidos geográficamente en todo el mundo y que la legislación de ciertos países, incluyendo México, prohíben el almacenamiento fuera de territorio nacional de datos que sean sensibles a las organizaciones.

En conclusión, se demuestra que ***la hipótesis planteada SI se cumple***, debido a que las facilidades y potencial que encuentran las organizaciones en el uso de la Nube (*Cloud Computing*) representan un gran valor a las mismas, cuando estas son adecuadamente implementadas mediante un análisis por parte de los departamentos de *TI* y que se encuentre alineada a la estrategia corporativa. Sin embargo, a pesar de las facilidades y características estratégicas que se presentan con la Nube, realizar una implementación del *IoT* en la Nube tendría efectos negativos en el rendimiento y desempeño de la red de cómputo, forzando a los centros de datos a ralentizar los procesos de procesamiento de la información generada y a su vez afectar a los dispositivos que requieren de una respuesta en tiempo real. Adicionalmente a esto, el uso de los procesos en la Nube (*Cloud Computing*) no es un factor determinante que marque una tendencia hacia la desaparición del centro de datos tradicional el cual se verá forzado a romper el paradigma de la centralización mediante la utilización cada vez mayor de la Computación al Borde (*Edge Computing*) y el incremento del uso de los dispositivos del *IoT* en los próximos años.

6 Conclusiones.

Las organizaciones tienen la necesidad de contar con información actualizada y que la misma cumpla con ciertos requisitos de confiabilidad, seguridad y certeza para que las mismas sean capaces de brindar información en la toma de decisiones al interior de las organizaciones.

Es debido a esta necesidad que los centros de datos forman parte neurálgica dentro de las mismas al mantener de forma centralizada el almacenamiento de los datos generados en la organización; sin embargo, en los últimos años los centros de datos se han visto en la necesidad de realizar integraciones de diversas tecnologías denominadas emergentes al interior de las mismas.

Los centros de datos han implementado nuevos requerimientos por la necesidad de mejorar y ampliar su cobertura derivado del uso de las nuevas tecnologías emergentes en la vida corporativa, lo que ha ocasionado que los estándares de implementación de los centros de datos sufrieran modificaciones recientemente; esto para poder soportar de manera adecuada las nuevas necesidades y requerimientos de velocidad y de conectividad en los centros de datos.

Las tecnologías emergentes han brindado un valor agregado a las organizaciones, como son la analítica de datos mediante el uso del *Big Data* que les permite manejar grandes volúmenes de datos y así tener la facilidad de generar un análisis con mayor grado de certeza al tener datos que derivan en información útil y valiosa, en conjunto con el *Machine Learning* y la Inteligencia Artificial (*IA*) se convierten en una herramienta indispensable para el análisis de la información y generar valor en la toma de decisiones.

El uso exponencial del Internet de las cosas en conjunto con la Inteligencia Artificial (*IA*), Machine Learning (*ML*) y el uso del Big Data, les ha proporcionado a las organizaciones una gran cantidad de dispositivos inteligentes que son útiles en diversos sectores de la industria; sin embargo, al generar grandes volúmenes de

datos representaran un gran reto en los niveles de transmisión de datos al utilizar como medio de transmisión la red de Internet.

Sin embargo, existe una brecha de seguridad con los nuevos dispositivos instalados basados en el *IoT*, lo que representara un reto en ciberseguridad y administración de los dispositivos al ser integrados a los centros de datos, ocasionando que el centro de datos rompa el paradigma de la centralización al utilizar la Computación al Borde para poder soportar las necesidades de mantener la información y transferencia de datos en tiempo real.

Las tecnologías emergentes, principalmente el Internet de las cosas tendrán en un futuro cercano una penetración en todos los sectores tan alta, que los datos generados serán exorbitantes basados en los pronósticos esperados para los próximos años.

Lo cual también representara un gran desafío para los centros de datos de las organizaciones en un futuro, aunado a que la Nube no es apta para almacenar la información generada por la mayoría de los dispositivos de *IoT*, que se encuentran en diversos sectores. Lo que representara un gran reto para los administradores de *TI* en un futuro cercano, para la administración y gestión de los anchos de banda de los centros de datos en las organizaciones.

Las tecnologías emergentes brindaran una gran capacidad de desarrollo para las organizaciones, principalmente el *IoT* ya que es esta tecnología la que mayor uso de datos requiere al utilizar la Inteligencia Artificial (*IA*), *Big data* y *Machine Learning* para su desarrollo.

Así, la aparición de las comunicaciones 5G, será el detonador que el *IoT* necesita para crecer exponencialmente en los próximos años. Lo cual representara un aumento en las telecomunicaciones y transmisión de datos que utilizan como medio

de transmisión la red de Internet, para lo cual las organizaciones deberán comenzar a preparar sus centros de datos para el futuro cercano.

Los usos de las nuevas tecnologías emergentes van dando la pauta a la modernización y agilidad en los procesos que anteriormente se venían realizando de forma manual. Lo que nos ha brindado la posibilidad de realizar una mayor integración con la tecnología inalámbrica y de comunicación vía celular. Sin embargo, esta modernización en los centros de datos y principalmente en los procesos de gestión de la infraestructura de las organizaciones, no se ha dado de manera constante en la gran mayoría de las organizaciones, lo que en el futuro representara un gran problema en las comunicaciones, rendimiento y desempeño de los centros de datos.

Por lo que la presente investigación proporciona los fundamentos teóricos y estadísticos para poder considerar el uso de las nuevas tecnologías emergentes, especialmente el *IoT* como una herramienta de cambio dentro de las organizaciones.

Adicionalmente proporciona información fundamentada en la industria de telecomunicaciones y las propias organizaciones para poder generar conocimiento de los retos actuales y futuros de la implementación de las tecnologías emergentes. Aportando el conocimiento necesario para una mejor comprensión de las necesidades de las organizaciones en torno de la implementación de las nuevas tecnologías emergentes, principalmente el *IoT*, al proporcionar el fundamento teórico/práctico que se requiere para una adecuada planeación y organización en la implementación de las tecnologías emergentes, para que las mismas sean un valor agregado a las organizaciones y no una carga financiera con el tiempo.

Hablar de las nuevas tecnologías y su implementación adecuada al interior de las organizaciones, implica un gran desafío que con el tiempo deberá de ser

subsanado, principalmente en la seguridad informática y una adecuada planeación dentro de los departamentos de *TI*.

El *IoT* afecta directamente en la planeación de los centros de datos y sus capacidades de almacenamiento, rendimiento de sus recursos propios como son el ancho de banda, la capacidad tecnológica de transmisión de datos, entre otras. De igual forma abre la puerta de que no todo es factible de ser migrado a la Nube y que de hacerlo implicará mayores problemas que soluciones al mediano plazo. Especialmente todo aquello que se encuentre relacionado con el *IoT*, lo cual será necesario profundizar en futuras investigaciones para subsanar los problemas de seguridad informática dentro de las organizaciones al implementar soluciones de *IoT*.

7 Referencias

42U. (febrero de 2009). *What is PUE / DCiE? How to Calculate, What to Measure*. Recuperado el 26 de febrero de 2019, de Solutions for the Next Generation Data Center: https://www.42u.com/measurement/pue-dcie.htm

451 Research. (18 de septiembre de 2019). *Newest Datacenter Market Study From 451 Research Finds That Over Half of Global Utilized Racks Will Be Off-Premises by 2024.* Recuperado el 01 de diciembre de 2019, de https://451research.com/newest-datacenter-market-study-finds-that-over-half-global-utilized-racks-will-be-off-premises-by-2024

ABB. (2018). *Centro de datos.* Recuperado el Mayo de 2018, de ABB: http://new.abb.com/data-centers/es

ABB Data Centers. (2018). *The two sides of highly efficient data centers.* Recuperado el Mayo de 2018, de ABB White paper: http://www.lead-central.com/AssetManager/02427e68-6f15-4f3a-9749-d37abf613741/Documents/Data%20Centers/ABB-355-WPO-DataCenterEfficiency.pdf

Acciardo, R. (3 de Mayo de 2016). *Schneider-Electric.* Recuperado el Mayo de 2018, de Data Center Downtime is Too Expensive to Forget about a Cooling Equipment Maintenance Plan: https://blog.schneider-electric.com/datacenter/2016/05/03/data-center-downtime-expensive-forget-cooling-equipment-maintenance-plan/

Agencia Nacional de Seguridad de Sistemas de Información (ANSSI). (18 de noviembre de 2019). *GESTIÓN DE RIESGOS DIGITALES: EL ACTIVO FIDUCIARIO.* Recuperado el 20 de diciembre de 2019, de https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance/

Alcalá, O. (8 de junio de 2010). *¿Por qué no está ya operando IPv6 en el mundo?* Recuperado el 25 de junio de 2019, de Magazcitum: https://www.magazcitum.com.mx/?p=568#.XRLPH-gza70

ALESTRA. (27 de febrero de 2019). *Centro De Datos*. Recuperado el 27 de febrero de 2019, de http://www.alestra.mx/centro-de-datos/

American National Standards Institute, Inc. (4 de junio de 2009). *American National Standard for Information Technology.* Recuperado el 17 de febrero de 2019, de Fibre Channel Backbone - 5 (FC-BB-5): https://www.fcoe.com/09-056v5.pdf

Anixter Latinoamerica. (2016). *TECHNOLOGY APPLICATION GUIDE.* Recuperado el Mayo de 2018, de Network Cabling Architectures for Data Centers: https://www.anixter.com/es_la/resources/literature/technology-application-guides/network-cabling-architectures-for-data-centers.html

Anixter Latinoamerica. (Mayo de 2017). *Standards Reference Guide.* Recuperado el Mayo de 2018, de Anixter: https://www.anixter.com/es_la/resources/literature/technical-references/standards-reference-guide.html

ANSI/TIA/EIA 568-B. (2018). *Commercial Building Telecommunications Cabling Standard.* Recuperado el Mayo de 2018, de Cablingdb.com: http://www.csd.uoc.gr/~hy435/material/Cabling%20Standard%20-%20ANSI-TIA-EIA%20568%20B%20-%20Commercial%20Building%20Telecommunications%20Cabling%20Standard.pdf

ARC ELECTRONICS. (2019). *NEBS*. Recuperado el 17 de febrero de 2019, de Network Equipment Building System: https://arcelect.com/NEBS.htm

Arroyo Gómez, I. M. (20 de diciembre de 2018). *Siete Edificios Inteligentes Que Se Encuentran En México Y Que Te Sorprenderán*. Recuperado el 18 de julio de 2019, de TeamVOX: https://teamvox.com/siete-edificios-inteligentes-que-se-encuentran-en-mexico-y-que-te-sorprenderan/

ASCE. (2019). *Minimum Design Loads and Associated Criteria for Buildings and Other Structures (ASCE/SEI 7-16)*. Recuperado el 17 de febrero de 2019, de American Society of Civil Engineers: https://www.asce.org/asce-7/

ASHRAE. (2016). *ASHRAE Bookstore.* Recuperado el 17 de febrero de 2019, de Standard 90.1-2016 (I-P Edition) -- Energy Standard for Buildings Except Low-Rise Residential Buildings (ANSI Approved; IES Co-sponsored): https://www.techstreet.com/ashrae/standards/ashrae-90-1-2016-i-

p?ashrae_auth_token=&product_id=1931793&utm_campaign=landingpage&utm_content=86274&utm_medium=landingpage&utm_source=promotion&utm_term=86274

ASHRAE Technical Committee. (2016). *Data Center Power Equipment Thermal Guidelines and Best Practices.* Recuperado el 17 de febrero de 2019, de https://tc0909.ashraetcs.org/documents/ASHRAE_TC0909_Power_White_Paper_22_June_2016_REVISED.pdf

Asociación de Normalización y Certificación, A. (. (15 de Julio de 2014). *Diario Oficial de la Federación (DOF).* Recuperado el 27 de Agosto de 2018, de DECLARATORIA de vigencia de la Norma Mexicana NMX-J-C-I-489-ANCE-ONNCCE-NYCE-2014: http://www.dof.gob.mx/nota_detalle.php?codigo=5352377&fecha=15/07/2014

AXARNET. (30 de enero de 2018). *¿Qué es un hosting y que un housing?* Recuperado el 27 de febrero de 2019, de https://www.axarnet.es/blog/hosting-vs-housing/

Barreiro Varela, A. (13 de febrero de 2013). *Instituto Politecnico Nacional.* Obtenido de [Tesis de Ingeniería], Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán: http://tesis.ipn.mx/bitstream/handle/123456789/15080/I.C.E.%2037-13.pdf?sequence=1

Barrueta, H. A. (14 de enero de 2019). *El Heraldo de México.* Recuperado el 25 de junio de 2019, de Se consolidan 5 smart cities mexicanas: https://heraldodemexico.com.mx/estados/se-consolidan-5-smart-cities-mexicanas/

BICSI. (2018). *BICSI International Standards Program*. Recuperado el 17 de febrero de 2019, de https://www.bicsi.org/standards/bicsi-standards/available-standards-store/single-purchase/ansi-bicsi-002-2014

Bjeletich, S., & Mable, et al., G. (1999). *Microsoft SQL Server 7.0 Al Descubierto.* Madrid: Prentice Hall. doi:ISBN 84-8322-136-5

Building Standards Commission. (2018). *California Building Standards Code*. Recuperado el 17 de febrero de 2019, de https://www.dgs.ca.gov/BSC/Codes

Cabling Installation & Maintenance. (27 de junio de 2017). *TIA-942-B Data Center Cabling Standard approved for publication.* Recuperado el Mayo de 2018, de Cabling Installation & Maintenance: http://www.cablinginstall.com/articles/2017/06/tia-942b-data-center-cabling-standard.html

Canal Comstor. (10 de septiembre de 2018). *TRES PUNTOS QUE TODAVÍA NECESITAN SER MEJORADOS EN EL MERCADO DE IOT.* Recuperado el 20 de agosto de 2019, de https://blogmexico.comstor.com/tres-puntos-que-todavia-necesitan-ser-mejorados-en-el-mercado-de-iot

Canal Comstor. (04 de febrero de 2019). *PREVISIONES PARA DATA CENTER Y CLOUD COMPUTING EN MÉXICO DURANTE EL 2019.* Recuperado el 20 de agosto de 2019, de Comstor Americas: https://blogmexico.comstor.com/previsiones-para-data-center-y-cloud-computing-en-mexico-durante-el-2019

Carey, S. (23 de febrero de 2018). *¿Cuál es la diferencia entre IaaS, SaaS y PaaS?* Recuperado el 02 de julio de 2019, de CIO From IDG: https://www.ciospain.es/gobierno-ti/cual-es-la-diferencia-entre-iaas-saas-y-paas

Castillo Devoto, L. R. (noviembre de 2008). *Pontificia Universidad Católica del Perú.* Recuperado el Mayo de 2018, de Tesis de Ingeniería, Facultad de Ciencias e Ingeniería: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/196/CASTILLO_LILIANA_DISENO_INFRAESTRUCTURA_DATA_CENTER.pdf?sequence=2

Cendón, B. (16 de Enero de 2017). *Pensamientos y tecnología*. Recuperado el Mayo de 2018, de http://www.bcendon.com/el-origen-del-iot/

CIS. (2018). *THE EUROPEAN STANDARD EN 50600*. Recuperado el 17 de febrero de 2019, de http://www.cis-cert.com/Pages/com/System-Zertifizierung/Data-Centers/Certification/European-Standard-EN-50600.aspx

Cisco VNI Mobile. (18 de febrero de 2019). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper*. Recuperado el 12 de junio de 2019, de VNI Global Fixed and Mobile Internet Traffic Forecasts: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html

CISCO VNI Mobile. (18 de febrero de 2019). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper*. Recuperado el 12 de junio de 2019, de VNI Global Fixed and Mobile Internet Traffic Forecasts: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html

Conectrónica. (13 de Mayo de 2017). *Conectronica.* Recuperado el Mayo de 2018, de ¿Qué es OM5?: https://www.conectronica.com/fibra-optica/redes-opticas/que-es-om5

Córdova Flores, D. C. (julio de 2012). *Universidad Técnica de Ambato, Ecuador.* Recuperado el Mayo de 2018, de Tesis de Ingeniería, Facultad de Ingenieria en Sistemas Electrónica e Industrial: http://repositorio.uta.edu.ec/bitstream/123456789/2379/1/Tesis_t729si.pdf

Corning. (2018). *Evaluación del Centro de Datos*. Recuperado el Mayo de 2018, de Corning: http://www.corning.com/cala/es/products/communication-networks/applications/data-center/evaluate-data-center-options.html

De Castro-Acuña Lasheras, T. (Enero de 2013). *Universidad Carlos III de Madrid.* Recuperado el Mayo de 2018, de Tesis de Ingeniería, Departamento de Ingeniería Telemática: https://e-archivo.uc3m.es/handle/10016/17346

Definición de Datacenter. (29 de Abril de 2015). *Definista*. Recuperado el Mayo de 2018, de conceptodefinicion.de: http://conceptodefinicion.de/data-center/

Definicion.de. (2019). *Definicion.de*. Recuperado el 02 de diciembre de 2019, de https://definicion.de/decadencia/

DiMinico, C. (2018). *Telecommunications Infrastructure Standard for Data Centers.* Recuperado el Mayo de 2018, de MC Communications: http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf

Domótica Integrada. (14 de febrero de 2018). *¿Qué son los edificios inteligentes y qué características los diferencian?* Recuperado el 15 de julio de 2019, de https://domoticaintegrada.com/edificios-inteligentes/

Dora. (18 de 05 de 2009). *alegsa*. Recuperado el Mayo de 2018, de http://www.alegsa.com.ar/Diccionario/C/3282.php

Econodía. (mayo de 2011). *¿Qué es la tasa de crecimiento anual compuesto?* Recuperado el 20 de julio de 2019, de Econodía: http://www.econodia.com/2011/05/que-es-la-tasa-de-crecimiento-anual.html

ehCOS. (5 de octubre de 2016). *Concluye con éxito la implantación de la Historia Clínica Electrónica en Ciudad de México*. Recuperado el 5 de febrero de 2019, de https://www.ehcos.com/concluye-exito-la-implantacion-la-historia-clinica-la-ciudad-mexico/

Electronic Components. Assemblies & Materials Association. (Diciembre de 2005). *IHS MARKIT Standards Store.* Recuperado el 17 de febrero de 2019, de EIA/ECA Standard Gabinets, Racks, Panels, and Associated Equipment: https://global.ihs.com/doc_detail.cfm?gid=SBSSIBAAAAAAAAAA

Equipo Editorial Reporte Digital. (3 de abril de 2019). *Los mitos sobre el almacenamiento de datos la nube que deben tener en cuenta los CEO*. Recuperado el 12 de junio de 2019, de REPORTEDIGITAL: https://reportedigital.com/cloud/mitos-cloud-computing-que-deben-ceos/

eSemanal. (28 de noviembre de 2019). *Ciberseguridad, un reto y prioridad para México: Schneider Electric.* Recuperado el 12 de diciembre de 2019, de eSemanal Noticias del canal: https://esemanal.mx/2019/11/ciberseguridad-un-reto-y-prioridad-para-mexico-schneider-electric/

Espeso, P. (8 de mayo de 2014). *En el principio fue el mainframe*. Recuperado el 09 de julio de 2019, de Xataka: https://www.xataka.com/historia-tecnologica/en-el-principio-fue-el-mainframe

Fiber Optical Networking. (2019). *Differences Between 12-fiber and 24-fiber MTP/MPO Connectivity.* Recuperado el 22 de agosto de 2019, de Fiber Optical Networking: http://www.fiber-optical-networking.com/2865.html

Fluke Networks. (19 de Abril de 2017). *What's the Deal with OM5 Cable Standards – WBMMF?* Recuperado el Mayo de 2018, de http://www.flukenetworks.com/blog/cabling-chronicles/what-is-the-deal-with-om5?mkt_tok=eyJpIjoiWkdJNE1HRTVOelEwWmpWayIsInQiOiJ4VlJ2MkdwUXliQUV6Q2ZjU05SbFpsY29PMDVEXC9RZ2haRGJHNjJcL0d4TXNOOXlCNk80VEh4dkZJUlpDWW9PRWQyYUxkTko5ME51N0NRNjZBbng5WGZyUWVQcnV0WUZC

Forcepoint. (2019). *What is Cybersecurity?* Recuperado el 03 de junio de 2019, de Cybersecurity Defined, Explained, and Explored: https://www.forcepoint.com/es/cyber-edu/cybersecurity

Fraga, A. I. (12 de Enero de 2017). *El gasto mundial en TIC crecerá un 2.7% en 2017, según Gartner*. Recuperado el Mayo de 2018, de Ticbeat: http://www.ticbeat.com/tecnologias/el-gasto-mundial-en-tic-crecera-un-27-en-2017-segun-gartner/

Fredricks, D. (2018). *CABLExpress.* Recuperado el Mayo de 2018, de Data Center Infraestructure Architect: http://www.cablexpress.com/blog/migration-concerns-to-the-16-fiber-mpo-connector/

Frigola, R. (18 de enero de 2017). *Claves para entender las "smart cities"*. Recuperado el 11 de junio de 2019, de ie University: https://www.ie.edu/insights/es/articulos/claves-entender-las-smart-cities/

Frost & Sullivan. (13 de noviembre de 2018). *La LAN moderna... reconsiderando el diseño de las redes en la era moderna*. Recuperado el 09 de julio de 2019, de Innovación Seguridad Electrónica: https://revistainnovacion.com/nota/10251/la_lan_moderna_reconsiderando_el_diseno_de_las_redes_en_la_era_moderna

Gartner. (28 de enero de 2019). *Newsroom.* Recuperado el 19 de junio de 2019, de Gartner Says Global IT Spending to Reach $3.8 Trillion in 2019:

https://www.gartner.com/en/newsroom/press-releases/2019-01-28-gartner-says-global-it-spending-to-reach--3-8-trillio

Gold, J. (02 de noviembre de 2018). *¿Qué está haciendo el IoT a tu centro de datos?* Recuperado el 08 de agosto de 2019, de Network World: https://www.networkworld.es/networking/que-esta-haciendo-el-iot-a-tu-centro-de-datos

Gomar, J. (13 de octubre de 2018). *Qué es un Exabyte.* Recuperado el 20 de julio de 2019, de Profesional Review: https://www.profesionalreview.com/2018/10/13/que-es-un-exabyte/

Gómez Vieites, Á. (2014). *Enciclopedia de la Seguridad Informática* (2a. Edición Actualizada ed.). México: Alfaomega Grupo Editor, S.A de C.V. doi:ISBN: 978-607-707-181-5

Grossner, C., Thoen, E., & Tatara, A. (s.f.). *WEBINAR - Cloudifying the enterprise edge for performance and efficiency.* Recuperado el 28 de julio de 2019, de HIS Markit: https://technology.ihs.com/Events/608689

Guillarte, M. (14 de Marzo de 2013). *¿Qué es un Tier?* Recuperado el Mayo de 2018, de MCPRO: https://www.muycomputerpro.com/2013/03/14/que-es-un-tier

Hatton, B. (10 de Noviembre de 2014). *Datacave.* Recuperado el Mayo de 2018, de Understanding the Impact of Data Center Downtime: https://www.thedatacave.com/understanding-the-impact-of-data-center-downtime

Historia y Vida. (27 de junio de 2018). *¿QUÉ APORTÓ A LA CIENCIA ALAN TURING?* Recuperado el 11 de julio de 2019, de https://www.lavanguardia.com/historiayvida/quien-fue-y-que-aporto-alan-turing_12321_102.html

HojadeRouter.com. (08 de junio de 2014). *Un ordenador hace historia al superar por primera vez el test de Turing*. Recuperado el 18 de julio de 2019, de Eldiario.es: https://www.eldiario.es/hojaderouter/tecnologia/eugene-goostman-humano-maquina-ordenador-test-turing_0_275772528.html

HPAC Info-Dex. (13 de septiembre de 2016). *ANSI/ASHRAE Standard 90.4-2016, Energy Standard for Data Centers.* Recuperado el 17 de febrero de 2019, de https://www.hpac.com/air-conditioning/energy-standard-data-centers-published-ashrae

Iberdrola. (2019). *¿QUÉ ES LA INTELIGENCIA ARTIFICIAL?* Recuperado el 01 de julio de 2019, de ¿Somos conscientes de los retos y principales aplicaciones de la Inteligencia Artificial?: https://www.iberdrola.com/innovacion/que-es-inteligencia-artificial

Iberdrola. (2019). *QUÉ ES EL 'MACHINE LEARNING'.* Recuperado el 19 de julio de 2019, de Descubre los principales beneficios del 'Machine Learning': https://www.iberdrola.com/innovacion/machine-learning-aprendizaje-automatico

IDC. (28 de octubre de 2019). *Crecerán 7 veces las inversiones de nube privada en México, con hiperconvergencia, entre 2017 y 2021: IDC.* Recuperado el 14 de diciembre de 2019, de IDC Releases: http://mx.idclatin.com/releases/news.aspx?id=2547

IDG. (02 de Noviembre de 2017). *Computerworld Red de Conocimiento.* Recuperado el Mayo de 2018, de La evolución del Data Center en 2017: http://red.computerworld.es/actualidad/la-evolucion-del-data-center-en-2017

IEEE. (1 de agosto de 2016). *IEEE Xplore digital*. Recuperado el 17 de febrero de 2019, de C2-2017 - 2017 National Electrical Safety Code(R) (NESC(R)) - Redline: https://ieeexplore.ieee.org/document/7802541

IEEE. (30 de enero de 2019). *IEEE 802 LAN/MAN Standards Committee.* Recuperado el 17 de febrero de 2019, de http://www.ieee802.org/

IEEE Standard Association. (21 de junio de 2000). *IEEE 446-1995 - IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*. Recuperado el 17 de febrero de 2019, de https://standards.ieee.org/standard/446-1995.html

Institute of Electrical and Electronics Engineers, Inc. (29 de diciembre de 2005). *IEEE Recommended Practice for Powering and Grounding Electronic Equipment.* Recuperado el 17 de febrero de 2019, de

http://www2.elo.utfsm.cl/~ipd411/archivos/apuntes/Std%201100-2005_01638205.pdf

Instituto de Ciberdefensa. (28 de octubre de 2019). *¿Qué es la Higiene Digital?* Recuperado el 20 de diciembre de 2019, de https://www.ciberdefensa.org/

Instituto Nacional de Ciberseguridad. (06 de junio de 2017). *IoT: riesgos del internet de los trastos.* Recuperado el 20 de junio de 2019, de https://www.incibe.es/protege-tu-empresa/blog/iot-riesgos-del-internet-los-trastos

Integrity. (2018). *Integrity.* Recuperado el Mayo de 2018, de DATA CENTER Y SU CLASIFICACIÓN TIER/RATED: https://integrity.pe/data-center-y-su-clasificacion/

INTERNATIONAL CODE COUNCIL, INC. (2019). *Standard Development Process*. Recuperado el 17 de febrero de 2019, de Standard Development Policy and Procedures: https://www.iccsafe.org/codes-tech-support/codes/code-development-process/standards-development/standard-development-process/

International Organization for Standardization (ISO). (febrero de 2012). *ISO/IEC 14763-2:2012.* Recuperado el 28 de junio de 2019, de Information technology -- Implementation and operation of customer premises cabling -- Part 2: Planning and installation: https://www.iso.org/standard/55024.html

ISO. (2011). *ISO 50001:2011(es) Sistemas de gestión de la energía — Requisitos con orientación para su uso.* Recuperado el 17 de febrero de 2019, de https://www.iso.org/obp/ui/#iso:std:iso:50001:ed-1:v1:es

ISO/IEC. (abril de 2014). *ISO/IEC 24764.* Recuperado el 2019 de febrero de 2019, de Information technology — Generic cabling systems for data centres AMENDMENT 1: https://www.iso.org/obp/ui/#iso:std:iso-iec:24764:ed-1:v1:amd:1:v1:en

IT Trends. (06 de agosto de 2019). *Cómo lograr que las ciudades inteligentes sean seguras.* Recuperado el 13 de diciembre de 2019, de IT Trends: https://www.ittrends.es/seguridad/2019/08/como-lograr-que-las-ciudades-inteligentes-sean-seguras

ITU. (2019). *ITU-T, Smart Sustainable Cities at a Glance.* Recuperado el 25 de junio de 2019, de Committed to connecting the world: https://www.itu.int/en/ITU-T/ssc/Pages/info-ssc.aspx

Jackson, B. (23 de abril de 2019). *Latencia de la Red – Comparando el Impacto sobre su Sitio WordPress.* Recuperado el 29 de julio de 2019, de Kinsta: https://kinsta.com/es/blog/latencia-de-la-red/

Jiménez-Hernández, C. N., Castellanos-Domínguez, O. F., & Villa-Enciso, E. M. (2011). *La Gestión de Tecnologías Emergentes en el Ámbito Universitario.* doi:ISSN 0123-7799

Kaspersky. (2019). *¿Qué es la ciberseguridad?* Recuperado el 03 de julio de 2019, de DEFINICIÓN DE SEGURIDAD: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

King, A. (enero de 2019). *The practical IoT.* Recuperado el 28 de julio de 2019, de Cabling Installation & Maintenance: https://digital.cablinginstall.com/cablinginstall/201901/MobilePagedReplica.action?pm=2&folio=Cover#pg1

Lamudi. (7 de Julio de 2017). *Arquitectura y diseño, Ciudades de México.* Recuperado el Mayo de 2018, de Edificios inteligentes en México: http://www.lamudi.com.mx/journal/edificios-inteligentes-en-mexico/

Lanner. (29 de enero de 2019). *Redes 5G y su Impacto en el Internet de las Cosas.* Recuperado el 18 de diciembre de 2019, de Lanner: https://www.lanner-america.com/es/blog-es/redes-5g-y-su-impacto-en-el-internet-de-las-cosas/

Lavin, M. (10 de diciembre de 2013). *¿Qué es BYOD?, ventajas e inconvenientes*. Recuperado el 03 de julio de 2019, de Computer Hoy: https://computerhoy.com/noticias/moviles/que-es-byod-ventajas-e-inconvenientes-7250

LEED (Leadership in Energy and Environmental Design). (2019). *LEED Certification*. Recuperado el 17 de febrero de 2019, de https://www.usgbc.org/help/what-leed

Lerner, A. (16 de Julio de 2014). *Gartner.* Recuperado el Mayo de 2018, de The Cost of Downtime: https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

Maroto, C. (2015). *BIG DATA Aqui y ahora 2015. Situación Mundial y Foco en el mercado de Colombia.* Recuperado el 19 de julio de 2019, de OBS Business School: http://emsub.edu.co/descargables/3eie/InvestigacionOB_SBigData2015_SituacionDelSectorYDelMercadoDeColombia.pdf

Martínez, C. A. (5 de enero de 2018). *'Data centers': no es oro todo lo que brilla.* Obtenido de SEGURILATAM: http://www.segurilatam.com/seguridad-aplicada/entidades-financieras/data-centers-no-es-oro-todo-lo-que-brilla

Martínez, H. (21 de agosto de 2017). *Schneider Electric.* Recuperado el 01 de diciembre de 2019, de Modernizar o externalizar: Evaluar las opciones para su centro de datos: https://blogespanol.se.com/gestion-de-la-energia/2017/08/21/modernizar-externalizar-evaluar-las-opciones-centro-datos/

National Fire Proteccion Association. (2017). *NFPA 75 Standard for the Fire Protection of Information Technology Equipment.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=75

National Fire Protection Association. (2016). *NFPA 76 Standard for the Fire Protection of Telecommunications Facilities.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=76

National Fire Protection Association. (2017). *NFPA 25 Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=25

National Fire Protection Association. (2017). *NFPA 70 National Electrical Code.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-

standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=70

National fire Protection Association. (2018). *NFPA 101 Life Safety Code.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=101

National Fire Protection Association. (2018). *NFPA 90A Standard for the Installation of Air-Conditioning and Ventilating Systems.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=90A

National Fire Protection Association. (2019). *NFPA 13 Standard for the Installation of Sprinkler Systems.* Recuperado el 17 de febrero de 2019, de https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=13

Normalización y Certificación NYCE, S.C. (2019). *Normalización y Certificación NYCE*. Recuperado el 21 de junio de 2019, de https://www.nyce.org.mx/quienes-somos/

Normalización y Certificación NYCE, S.C. (2019). *Normas Mexicanas NMX.* Recuperado el 21 de junio de 2019, de http://www.nyce.org.mx/formatos/normalizacion/CatalogoNormasNYCE2014.pdf

Observatorio Digital. (15 de enero de 2015). *Una visión crítica sobre las ciudades inteligentes: ¿Acabarán por destruir la democracia?* Recuperado el 12 de junio de 2019, de Territorios Inteligentes, Beyond Smart Cities: http://smart-cities.euroresidentes.com/2015/01/la-verdad-sobre-las-ciudades.html

Oficina de Seguridad del Internauta (OSI). (21 de agosto de 2018). *¿Qué son los ataques DoS y DDoS?* Recuperado el 12 de julio de 2019, de https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos

Oxford. (2019). *Lexico*. Recuperado el 02 de diciembre de 2019, de https://www.lexico.com/en/definition/tco

Palo Alto Networks, Inc., Cyberpedia. (2019). *WHAT IS CYBERSECURITY?* Recuperado el 03 de junio de 2019, de A Definition of Cybersecurity: https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

Panduit, Inc. (abril de 2018). *Edge Computing: El "Behind-the-Scenes" del IoT.* Recuperado el 20 de junio de 2019, de White Paper: https://pages.panduit.com/rs/349-EQI-366/images/2018-EdgeComputing-IoT-WP_D-CPAT30--SA-SPA-WEB.pdf

Peña, M. (19 de abril de 2019). *Qué es el Internet de las Cosas y cómo afecta tu vida diaria*. Recuperado el 13 de junio de 2019, de Digital Trends ES: https://es.digitaltrends.com/tendencias/que-es-el-internet-de-las-cosas/

Pérez Orozco , M. (marzo de 2018). *Inteligencia Artificial.* Recuperado el 11 de julio de 2019, de Oficina de Información Científica y Tecnológica para el Congreso de la Unión (INCyTU): https://www.foroconsultivo.org.mx/INCyTU/index.php/notas/ciencia-y-tecnologia/50-12-inteligencia-artificial

Poon, L. (22 de junio de 2018). *Sleepy in Songdo, Korea's Smartest City*. Recuperado el 12 de junio de 2019, de CityLab: https://www.citylab.com/life/2018/06/sleepy-in-songdo-koreas-smartest-city/561374/

Power, E. N. (19 de Enero de 2016). *Vertiv Co.* Recuperado el Mayo de 2018, de Emerson Network Power Study Says Unplanned Data Center Outages Cost Companies Nearly $9,000 Per Minute: https://www.vertivco.com/en-us/about/newsroom/corporate-news/emerson-network-power-study-says-unplanned-data-center-outages-cost-companies-nearly-$9000-per-minute/

PowerData. (2019). *Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad*. Recuperado el 15 de julio de 2019, de https://www.powerdata.es/big-data

PowerData. (2019). *Cloud: definiciones, servicios, despliegue, su seguridad y privacidad.* Recuperado el 01 de julio de 2019, de https://www.powerdata.es/cloud

Puente García, M. (22 de diciembre de 2017). *Riesgos y retos de ciberseguridad y privacidad en IoT*. Recuperado el 17 de julio de 2019, de Incibe-Cert_: https://www.incibe-cert.es/blog/riesgos-y-retos-ciberseguridad-y-privacidad-iot

Quirk, P. (Julio de 2018). *Managing IoT: A problem and solution for data center and IT managers*. Recuperado el 20 de julio de 2019, de Cabling Installation & Maintenance: https://digital.cablinginstall.com/cablinginstall/201807/MobilePagedReplica.action?articleId=1410977&pm=2&folio=Cover#pg1

Revilla, L. (29 de julio de 2019). *La Inteligencia Artificial revoluciona la gestión del Centro de Datos.* Recuperado el 31 de julio de 2019, de DatacenterDynamics: https://www.dcd.media/opinion/la-inteligencia-artificial-revoluciona-la-gestion-del-centro-de-datos/

Reyes, E. (Mayo de 2015). *Mundo HVACR.* Recuperado el 27 de Agosto de 2018, de Nueva Norma para centros de datos de alto desempeño: https://www.mundohvacr.com.mx/2015/05/nueva-norma-para-centros-de-datos-de-alto-desempeno/

Rittal. (26 de enero de 2018). *Edge Computing y su relación con el IoT.* Recuperado el 25 de junio de 2019, de INFRAESTRUCTURA: https://www.rittaltic.es/edge-computing-y-su-relacion-con-el-iot/

Ritter Kraft. (2013). *Cableado Estructurado*. Recuperado el 01 de marzo de 2019, de http://ritterkraft.com/Cableado.html

Romero, S. (2019). *Muy Interesante.* Recuperado el 10 de enero de 2020, de https://www.muyinteresante.es/cultura/arte-cultura/articulo/8-frases-celebres-de-john-nash-241432551660

Salazar, A. (26 de Abril de 2016). *Green House Data.* Recuperado el Mayo de 2018, de Stamping Out the Main Causes of Data Center Downtime: https://www.greenhousedata.com/blog/stamping-out-the-main-causes-of-data-center-downtime

Sánchez-Caballero, E. (12 de febrero de 2019). *5G: un cambio de paradigma en el papel del Internet de las Cosas.* Recuperado el 18 de diciembre de 2019, de

Periodico El País, sección Economía (Madrid): https://retina.elpais.com/retina/2019/02/11/tendencias/1549879163_844879.html

Santos, P. (2019). Cinco Tecnologías que influirán en 2019. *Ventas de Seguridad, 23*(2), 55-56. Recuperado el 12 de junio de 2019

Sarenet. (11 de enero de 2018). *Tendencias en centro de datos para 2018.* Recuperado el 16 de diciembre de 2019, de Noticias: https://www.sarenet.es/noticias/2018/01/11/tendencias-centro-datos-para-2018.html

Scully, P. (25 de enero de 2018). *New Research on 1,600 Enterprise IoT Projects: Upsurge in Smart City and Connected Building Related IoT Project*. Recuperado el 12 de junio de 2019, de IoT Analitycs: https://iot-analytics.com/global-overview-1600-enterprise-iot-projects/

Secretaria de energia. (2012). *NORMA OFICIAL MEXICANA NOM-001-SEDE-2012, INSTALACIONES ELECTRICAS (UTILIZACION).* Recuperado el 17 de febrero de 2019, de Comité Consultivo Nacional de Normalización de Instalaciones Eléctricas y por la Dirección General de Distribución y Abastecimiento de Energía Eléctrica, y Recursos Nucleares de la Secretaría de Energía: http://dof.gob.mx/nota_detalle_popup.php?codigo=5280607

Secretaria de Gobernación. (15 de julio de 2014). *Norma Mexicana NMX-J-C-I-489-ANCE-ONNCCE-NYCE-2014*. Recuperado el 27 de febrero de 2019, de Diario Ofoicial de la Federación: http://www.dof.gob.mx/nota_detalle.php?codigo=5352377&fecha=15/07/2014

Secretaria de Gobernación. (15 de julio de 2014). *Norma Mexicana NMX-J-C-I-489-ANCE-ONNCCE-NYCE-2014.* Obtenido de Diario Oficial de la Federación: http://www.dof.gob.mx/nota_detalle.php?codigo=5352377&fecha=15/07/2014

Secretaria de gobernación. (26 de agosto de 2016). *Diario Oficial de la Federación.* Recuperado el 17 de febrero de 2019, de NORMA MEXICANA

NMX-I-163-NYCE-2016, EQUIPO ELECTRÓNICO-SISTEMAS ELECTRÓNICOS DE ENERGÍA ININTERRUMPIDA (S.E.E.I.): https://www.dof.gob.mx/nota_detalle.php?codigo=5449890&fecha=26/08/2016

Skaff, E. (2015). *Las mejores frases de Bill Gates que inspirarán tu trabajo.* Recuperado el 25 de diciembre de 2019, de Postcron: https://postcron.com/es/blog/frases-de-bill-gates-que-inspiraran-tu-trabajo/

Smart cities México. (2019). *Smart Cities México.* Recuperado el 12 de diciembre de 2019, de https://smartcitiesmexico.mx/hacemos.html

Statista. (2019). *Inversión en tecnologías de la información en Latinoamérica desde 2014 hasta 2019*. Recuperado el 27 de febrero de 2019, de El portal de estadísticas: https://es.statista.com/estadisticas/638124/servicios-de-ti-en-latinoamerica/

Tecnología. (22 de enero de 2018). *Dinero.* Recuperado el Mayo de 2018, de https://www.dinero.com/empresas/articulo/gasto-mundial-en-tecnologia-para-el-2018-segun-gartner/254476

TELECOMMUNICATIONS INDUSTRY ASSOCIATION. (26 de agosto de 2011). *ANSI/TIA-607-B-2011.* Recuperado el 17 de febrero de 2018, de Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises: http://www.raqi.ca/~ve2rae/tech_hf/tia-607-b.pdf

TELECOMMUNICATIONS INDUSTRY ASSOCIATION. (27 de marzo de 2012). *ANSI/TIA-758-B-2012.* Recuperado el 17 de febrero de 2019, de Customer-Owned Outside Plant Telecommunications Infrastructure Standard: http://innovave.com/wp-content/uploads/2016/01/TIA-758-B.pdf

Telecommunications Industry Association. (Julio de 2017). *Telecommunications Infraestructure Standard for Data Centers.* Recuperado el Mayo de 2018, de TIA-942-B (Revision of TIA-492-A): https://global.ihs.com/doc_detail.cfm?&csf=TIA&item_s_key=00414811&item_key_date=820519&input_doc_number=TIA-942&input_doc_title=

TeleSemana.com. (2018). *PANORAMA DE MERCADO - MÉXICO*. Recuperado el 27 de febrero de 2019, de https://www.telesemana.com/panorama-de-mercado/mexico/

Terán, D. (2014). *Redes Convergentes Diseño e implementación* (Sexta reimpresión ed.). México: Alfaomega. doi:ISBN: 978-607-7854-89-0

Thirty, M. (2018). *Data Center Modernization: From Smart Data Centers to Enterprise Smart Grids.* Recuperado el Mayo de 2018, de ABB White paper: http://search-ext.abb.com/library/Download.aspx?DocumentID=3BUS095716&LanguageCode=en&DocumentPartId=&Action=Launch

Tilves, M. (28 de octubre de 2019). *De 12 a 105 millones de ataques a dispositivos IoT en un año.* Recuperado el 12 de diciembre de 2019, de Silicon.es: https://www.silicon.es/de-12-a-105-millones-de-ataques-a-dispositivos-iot-en-un-ano-2407003

Toledo, V. (20 de Septiembre de 2017). *DCD Security + Risk.* Obtenido de Uptime Institute crea un programa Tier para DCs prefabricados: https://www.dcd.media/noticias/uptime-institute-crea-un-programa-tier-para-dcs-prefabricados/

UIT. (13 de diciembre de 2019). *Sobre la Unión Internacional de Telecomunicaciones (UIT).* Recuperado el 13 de diciembre de 2019, de https://www.itu.int/es/about/Pages/default.aspx

UL. (2 de octubre de 2013). *Standard for Fire Test for Heat and Visible Smoke Release for Discrete Products and Their Accessories Installed in Air-Handling Spaces.* Recuperado el 17 de febrero de 2019, de https://standardscatalog.ul.com/standards/en/standard_2043_4

UL. (11 de marzo de 2015). *Standard for Audio/Video, Information and Communication Technology Equipment Cabinet, Enclosure and Rack Systems.* Recuperado el 17 de febrero de 2018, de Standards: https://standardscatalog.ul.com/standards/en/standard_2416_1

UNE Normalización española. (1 de julio de 2018). *Tecnología de la información. Sistemas de cableado genérico.* Recuperado el 17 de febrero de 2019, de

UNE-EN 50173-5:2018 (Ratificada): https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0060271

Uptime Institute. (diciembre de 2018). *Top 10 Data Center Industry Trends for 2019.* Recuperado el 30 de julio de 2019, de UptimeInstitute: https://es.uptimeinstitute.com/top-10-data-center-industry-trends-for-2019

Uptime Institute. (2019). *Tier Standard: Topology*. Recuperado el 17 de febrero de 2019, de https://es.uptimeinstitute.com/resources/assets?filter%5Blanguage_id%5D=0&filter%5Bcategory_id%5D=1&filter%5Bpublished_on%5D=0&task=search&filter_order=a.published_on

VansonBourne + NUTANIX. (2018). *Enterprise Cloud Index.* Recuperado el 22 de julio de 2019, de Nutanix: https://www.nutanix.com/enterprise-cloud-index

Ventas de seguridad. (2019). Tecnología y Avances (Noticias). *Ventas de seguridad, 23*(3), 90. Recuperado el 22 de julio de 2019

Vertiv Co. (2018). *INTRODUCING THE DATA CENTER PERFORMANCE BENCHMARK SERIES.* Recuperado el Mayo de 2018, de 2016 Cost to Support Compute Report: https://www.vertivco.com/en-us/insights/articles/pr-campaigns-reports/benchmark-series/

Vieites, Á. G. (2014). *Enciclopedia de la Seguridad Informática.* México: Alfa o editor.

Voice of the industry. (2018). *Data Center Frontier.* Recuperado el Mayo de 2018, de The Top Causes of Data Center Downtime: https://datacenterfrontier.com/top-causes-of-data-center-downtime/

Watson, J., Segal, A., & Tatara, A. (2019). *How to navigate complexity in IoT edge deployments*. Recuperado el 28 de julio de 2019, de IHS Markit: https://ihsmarkit.com/events/How-to-navigate-complexity-in-IoT-edge-deployments/overview.html

WireNet. (2018). *¿Cómo se clasifican los datacenter?* Recuperado el Mayo de 2018, de WireNet: https://www.wirenetchile.com/Como-se-clasifican-los-datacenter-

Zambrana, F. (2019). Nube Híbrida. *Ventas de Seguridad, 23*(3), 74-76. Recuperado el 22 de julio de 2019, de https://www.cablinginstall.com/magazine/5ca3d82c75a25456040041a9

9 Anexo I – Principales estándares del cableado estructurado

9.1 ANSI/TIA 942-A

Estándar de Infraestructura de Telecomunicaciones para Centros de Datos (*Telecommunications Infraestructure Standard for Data Centers*).[52]

9.1.1 Infraestructura del centro de datos

Los elementos básicos de un sistema de cableado estructurado del centro de datos incluyen lo siguiente:

- Cableado horizontal
- Cableado de red troncal
- Conexión cruzada en la sala de entrada o en el área de distribución principal
- Conexión cruzada principal (MC) en el área de distribución principal
- Transconexión horizontal (HC) en las telecomunicaciones
- Área de distribución horizontal o área de distribución principal
- Salida de zona o punto de consolidación en el área de distribución de zona
- Salida en el área de distribución de equipos

Los centros de datos consumen una cantidad desproporcionada de energía en base a pies cuadrados en comparación con otras áreas de un edificio. El mayor consumo de energía se debe en gran parte a la densidad del hardware de cómputo y los sistemas asociados de alimentación y enfriamiento necesarios para respaldar las operaciones del centro de datos. Por lo tanto, se recomienda que las prácticas de diseño sostenible se incorporen en el diseño del centro de datos para mejorar la eficiencia de la energía y la refrigeración. Los siguientes sistemas deben optimizarse para garantizar que se logre la eficiencia energética.

- **Cableado de telecomunicaciones:** el cableado de telecomunicaciones aéreas puede mejorar el flujo de aire en los centros de datos al eliminar las

[52] Traducción propia. (Standards Reference Guide, 2017)

posibles obstrucciones que podrían estar presentes en las vías bajo el suelo. De lo contrario, las vías de cable deben diseñarse para acomodar los cables que podrían alterar el flujo de aire y la presión estática dentro de un entorno de piso elevado.

- **Iluminación:** se recomienda utilizar un protocolo de iluminación de tres niveles en los centros de datos, dependiendo de la ocupación humana.
    - **Nivel 1:** centro de datos desocupado
    - **Nivel 2:** entrada inicial en el centro de datos
    - **Nivel 3:** espacio ocupado
    - **Anulación opcional:** iluminación en todas las zonas en el nivel tres.

9.1.2 Pasillos calientes y fríos

Los gabinetes y los racks deben estar dispuestos en un patrón alterno con los frentes de gabinetes y bastidores uno frente al otro en una fila para crear pasillos fríos y calientes.

- **Pasillos fríos están en frente de bastidores y armarios.** Si hay un piso de acceso, distribución de energía los cables deben instalarse aquí debajo del piso de acceso en la losa.
- **Pasillos calientes están detrás de bastidores y armarios.** Si hay un piso de acceso, las bandejas de cable para el cableado de telecomunicaciones deben ubicarse debajo del piso de acceso en los pasillos calientes.

1. Se debe proporcionar un mínimo de 1 m (3.28 pies) de espacio libre delantero para la instalación del equipo. Un espacio libre frontal de 1.2 m (4 pies) es preferible para acomodar un equipo más profundo.
2. Se debe proporcionar un mínimo de 0.6 m (2 pies) de espacio libre trasero para acceso de servicio en la parte posterior de los bastidores y gabinetes.
3. Es preferible un espacio libre trasero de 1 m (3.28 pies). Algunos equipos pueden requerir distancias de servicio superiores a 1 m (3.28 pies).

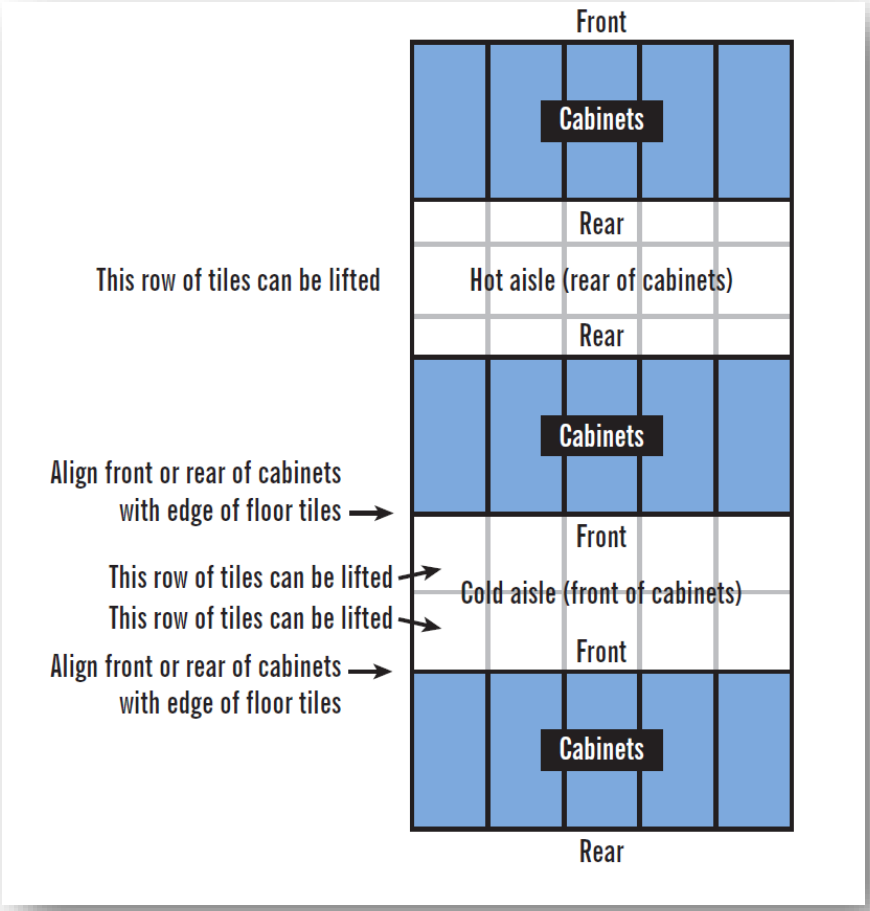

Ilustración 20 - Pasillos calientes y fríos
Fuente: *(Anixter Latinoamerica, 2017, pág. 119)*

9.1.3 Cableado horizontal

El cableado horizontal es la parte del sistema de cableado de telecomunicaciones que se extiende desde la terminación mecánica en el área de distribución del equipo hasta la conexión cruzada horizontal en el área de distribución horizontal o la conexión cruzada principal en el área de distribución principal. El cableado horizontal incluye cables horizontales, terminaciones mecánicas y cables de conexión o puentes. También puede incluir una salida de zona o un punto de consolidación en el área de distribución de la zona.

La siguiente lista parcial de servicios y sistemas comunes debe considerarse al diseñar el cableado horizontal:

- Servicio de telecomunicaciones de voz, módem y facsímil
- Equipo de conmutación de locales
- Conexiones de administración de computadoras y telecomunicaciones
- Conexiones de teclado / video / mouse (KVM)
- Transmisión de datos
- Redes de área amplia (WAN)
- Redes de área local (LAN)
- Redes de área de almacenamiento (SAN)
- Otros sistemas de señalización de edificios (sistemas de automatización de edificios) como fuego, seguridad, energía, HVAC, etc.)

La función del cableado de *backbone* es proporcionar conexiones entre el área de distribución principal, el área de distribución horizontal y las instalaciones de entrada en el sistema de cableado del centro de datos. El cableado de red troncal consiste en los cables troncales, las conexiones cruzadas principales, las conexiones cruzadas horizontales, las terminaciones mecánicas y el cable de interconexión o los puentes utilizados para las conexiones cruzadas de la red troncal a la red troncal.

9.1.4 Medios reconocidos de cableado

Los cables reconocidos, el hardware de conexión asociado, los puentes, los cordones de interconexión, los cables de los equipos y los cables de área de zona deben cumplir con todos los requisitos aplicables especificados en ANSI / TIA-568-C.2 y ANSI / TIA-568-C.3.

- Cable de par trenzado de 4 pares de 100 ohmios (ANSI / TIA-568-C.2), categoría 6 o categoría 6A, con categoría 6A recomendada
- 50/125 µm cable de fibra óptica multimodal optimizado para láser de 850 nm OM3 u OM4 (ANSI / TIA-568-C.3) con OM4 recomendado
- Cable de fibra óptica monomodo
- Medios coaxiales reconocidos:

- Cable coaxial de 75 ohmios (tipo 734 y 735)
- (Telcordia Technologies GR-139-CORE) y conector coaxial
- (ANSI T1.404)

9.1.5 Redundancia

Los centros de datos que están equipados con diversas instalaciones de telecomunicaciones pueden continuar su función en condiciones catastróficas que de lo contrario interrumpirían el servicio de telecomunicaciones del centro de datos. Este estándar incluye cuatro niveles relacionados con varios niveles de disponibilidad de la infraestructura de la instalación del centro de datos. Los niveles están relacionados con la investigación realizada por el *Uptime Institute*, que define cuatro niveles de rendimiento Además de los requisitos de redundancia base especificados por el marco de niveles de *Uptime Institute*, ANSI / TIA-942-A también recomienda niveles de niveles para sistemas arquitectónicos, eléctricos, mecánicos y de telecomunicaciones.

Desde una perspectiva de redundancia de infraestructura de telecomunicaciones, proporcionar áreas redundantes de conexión cruzada y rutas separadas físicamente puede aumentar la confiabilidad de la infraestructura de comunicaciones. Es común que los centros de datos tengan múltiples proveedores de acceso que proporcionan servicios, enrutadores redundantes, distribución central redundante e interruptores de borde. Aunque esta topología de red proporciona un cierto nivel de redundancia, la duplicación en servicios y hardware por sí sola no garantiza que se eliminen los puntos únicos de falla.

El propósito principal del estándar de la ANSI/TIA 942-A, es proporcionar los requisitos y directrices necesarios para el diseño y la instalación de un centro de datos y está destinado principalmente para ser utilizado por los diseñadores e integradores, que requieren de una mejor comprensión del diseño del centro de datos

El estándar permite que el diseño del centro de datos sea considerado al principio del proceso de desarrollo del edificio, contribuyendo a las consideraciones, al proporcionar información que atraviesa los esfuerzos de diseño multidisciplinarios, promover la cooperación en las fases de diseño y construcción, nos permite una planificación adecuada durante la construcción o renovación que es significativamente menos costosa y menos perjudicial que después de la instalación.

El estándar de la EIA/TIA 942-A recientemente sufrió modificaciones que amplían el rango de opciones para la implementación del centro de procesamiento de datos. Definiendo el nuevo estándar EIA/TIA 942-B, estas modificaciones incorporan el uso de cableado de alta velocidad por cobre y fibra óptica lo cual en sus diversas configuraciones permitirán un ancho de banda de hasta 400 Gbps entre los equipos activos (*switches/routers*) y los servidores de datos. (Cabling Installation & Maintenance, 2017).

Dentro de las principales modificaciones que sufrió el estándar de la EIA/TIA 942, se incluyen principalmente las siguientes:

- Se agregó MPO-16 y MPO-32 (ANSI / TIA-604-18) y MPO-24 (ANSI / TIA-604-5) como opciones para la terminación de más de dos fibras además del conector MPO-12

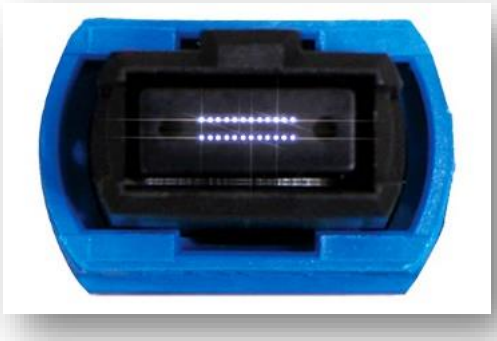

Ilustración 21 - Conector Multi-Fibre Push On (MPO)-24
Fuente: *(Fiber Optical Networking, 2019)*

- Se agregó la categoría 8 como un tipo permitido de cable de par trenzado balanceado. Cambiando la recomendación para el cable de par trenzado balanceado de categoría 6A a la categoría 6A o superior.
- Se agregó OM5 como un tipo de cable de fibra multimodal permitido y recomendado.
- Se agregaron cables y conectores coaxiales de banda ancha de 75 ohmios como se especifica en ANSI / TIA-568.4-D como tipos permitidos de cables y conectores coaxiales.
- Se agregó una recomendación para no instalar cordones y cables de fibra óptica (ambos se vuelven insensibles y no insensibles a la flexión) sin una armadura adecuada o una chaqueta suficientemente gruesa en vías que pueden crear micro curvaturas, como soportes de cables no continuos, cables bandejas de cesta y escaleras de cable sin soportes de cable redondeados o fondos sólidos.
- Reducción de la cantidad de salidas de conveniencia requeridas en las paredes de las salas de computadoras.
- Se pueden usar códigos locales de protección contra incendios en lugar de NFPA 75[53].
- Energía para sistemas de aire acondicionado y controles en salas de computadoras y salas de entrada debe ser redundante, pero no necesita ser alimentado desde las mismas PDU o panel que sirven equipos TIC en la sala.
- Las longitudes de cable máximas recomendadas para el cableado de conexión directa en EDA ha sido reducido de 10 m (33 pies) a 7 m (23 pies). Se agregó una guía adicional que se conecta directamente, no se recomienda el cableado entre filas.

[53] Véase (National Fire Proteccion Association, 2017)

- Se agregó la recomendación de que los gabinetes estén a 1200 mm (48") de profundidad y de considerar los gabinetes más anchos que 600 mm (24") de ancho.
- Se agregó una recomendación para considerar el cableado pre terminado para reducir el tiempo de instalación y mejorar la consistencia y la calidad de las terminaciones.
- Se agregó una recomendación para considerar las necesidades de etiquetado adecuado, enrutamiento de cable, administradores de cable y capacidad para insertar y eliminar cables sin interrumpir los existentes o conexiones adyacentes.
- Agrega una referencia normativa a ANSI/TIA-5017 con respecto a la seguridad física de la infraestructura central de telecomunicaciones para el centro de datos.
- Agrega una referencia normativa a ANSI/TIA-862-B con respecto a los requisitos para el cableado de sistemas de construcción inteligentes que incluyen centros de datos en red eléctricos, mecánicos y equipo de seguridad.
- Se agregó una referencia a TIA TSB 162-A para obtener directrices sobre el cableado para los puntos de acceso inalámbrico en los centros de datos.
- Se agregó una referencia a TIA TSB-5018 para obtener directrices sobre el cableado de los sistemas de antena distribuida en centros de datos.
- Se agregó una referencia a TIA TSB-184-A para obtener pautas con respecto a la entrega de potencia con un cableado de par trenzado equilibrado.
- Numerosos cambios en las tablas de calificación del Anexo F, incluidas las que especifican concurrencia de mantenimiento para Rating-3 (anteriormente Tier III) y tolerancia a fallas para Rating-4 (anteriormente Tier IV) Traducción propia, (Telecommunications Industry Association, 2017, págs. viii - ix)

Los centros de datos pueden beneficiarse de la infraestructura que se planifica con anticipación para apoyar el crecimiento y los cambios en los sistemas informáticos que los centros de datos están diseñados para apoyo. Además, de esto, el estándar aborda el diseño del piso relacionado con el logro del equilibrio adecuado entre la seguridad, densidad de rack y manejabilidad.

El estándar especifica un sistema de cableado de telecomunicaciones genérico para el centro de datos e instalaciones relacionadas cuya función principal es la tecnología de la información. Tales espacios de aplicación pueden estar dedicados a una empresa o institución privada, u ocupado por uno o más proveedores de servicios para alojar conexiones de Internet y dispositivos de almacenamiento de datos.

Los centros de datos se pueden clasificar según si sirven al dominio privado ("empresa" centros de datos) o del dominio público (centros de datos de Internet, centros de datos de coubicación y otros proveedores de servicios de centros de datos). Las instalaciones de la empresa incluyen corporaciones privadas, instituciones o agencias gubernamentales, y puede involucrar el establecimiento de intranet o extranet según sean los requerimientos de la organización.

Las instalaciones incluyen proveedores de servicios telefónicos tradicionales, proveedores de servicios competitivos no regulados y operadores comerciales relacionados. Las topologías especificadas en este estándar; sin embargo, son destinados a ser aplicables a ambos para satisfacer sus respectivos requisitos de conectividad (acceso a Internet y comunicaciones de área amplia), hosting operativo (alojamiento web, almacenamiento de archivos y copia de seguridad, administración de bases de datos, etc.) y servicios adicionales (alojamiento de aplicaciones, contenido distribución, etc.). Energía a prueba de fallas, controles ambientales, extinción de incendios, redundancia del sistema y la seguridad también son requisitos comunes para las instalaciones que prestan servicios tanto a particulares como a dominio.

La instalación del cableado estructurado se rige por la norma de la EIA/TIA 568 consta de varios rubros que la conforman, y el propósito general es el de proveer un estándar que dicta las normas de implementación e instalación de los sistemas de cableado estructurado para todos los tipos de cables existentes en el mercado, y especifica un sistema de soporte genérico del cableado de telecomunicaciones en un ambiente de múltiples productos y de un ambiente de múltiples fabricantes. Trataremos brevemente los estándares relacionados con la norma de la EIA/TIA 568 y sus diversas características esenciales.

9.2 Estándar ANSI/TIA/568-C.0.

Cableado genérico de telecomunicaciones para las instalaciones del cliente (*Generic Telecommunications Cabling for Customer Premises*)[54]

El estándar especifica los requerimientos genéricos del cableado de telecomunicaciones que incluyen:

- Estructuras del sistema de cableado.
- Topologías y distancias
- Instalación, desempeño y pruebas.
- Transmisión de Fibra Óptica (FO) y requerimientos de prueba.

La ***Ilustración 22 - Elementos de un sistema de cableado genérico***, muestra un modelo representativo de los sistemas funciónales de un típico sistema de cableado estructurado para la norma ANSI/TIA-568-C.0 y que es utilizado en edificios comerciales. Y se encuentra conformado de la siguiente forma:

- El distribuidor C representa la conexión cruzada principal (MC),
- El distribuidor B representa la conexión cruzada intermedia (IC),

[54] Véase (Standards Reference Guide, 2017)

- El distribuidor A representa la conexión cruzada horizontal (HC),
- Y la salida del equipo (EO) representa la salida y el conector de telecomunicaciones.
- Utiliza una topología de tipo estrella
- No deben existir más de dos distribuidores entre el distribuidor C y la salida del equipo (EO).

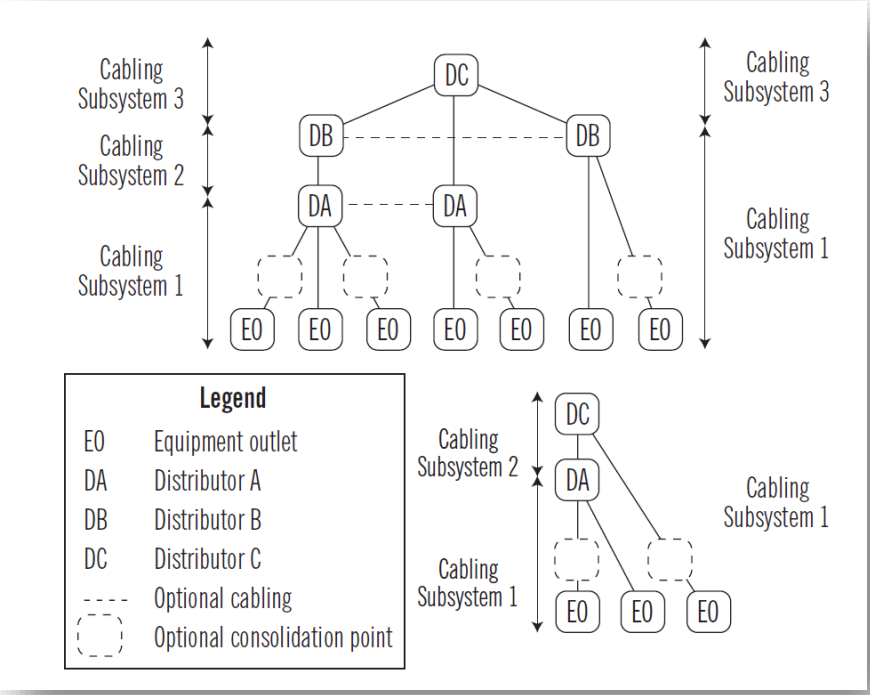

Ilustración 22 - Elementos de un sistema de cableado genérico
Fuente: *(Anixter Latinoamerica, 2017, pág. 9)*

Los distribuidores proveen una ubicación para la administración, reconfiguración y conexión de equipos y pruebas. Las cuales pueden ser interconexiones o conexiones cruzadas.

9.2.1 Subsistema de cableado

- Proporciona una ruta de señal entre el distribuidor A, el distribuidor B o el distribuidor C y un EO
- No contiene más de un punto de transición o punto de consolidación.

- Estipula que los empalmes no se deben instalar como parte de un subsistema de cableado de par trenzado balanceado y que los divisores no se deben instalar como parte de fibra óptica para el subsistema de cableado.

9.2.2 Reconocimiento de cableado

Los medios reconocidos, que se usarán individualmente o en combinación, son:

- Cableado de par trenzado balanceado de 100 ohmios
- Cableado de fibra óptica multimodal
- Cableado de fibra óptica monomodal.

Los medios de cableado de las instalaciones apropiadas pueden especificar medios de cableado distintos a los reconocidos anteriormente.

9.2.3 Longitudes del cableado

Las longitudes del cableado, dependen de la aplicación y de los medios específicos elegidos como podremos observar en la ***Tabla 18 - Distancia máxima soportada***

Tabla 18 - Distancia máxima soportada.

Cabling lengths

Application	Media	Distance m (ft.)	Comments
Ethernet 10BASE-T	Category 3, 5e, 6, 6A	100 (328)	
Ethernet 100BASE-TX	Category 5e, 6, 6A	100 (328)	
Ethernet 1000BASE-T	Category 5e, 6, 6A	100 (328)	
Ethernet 10GBASE-T	Category 6A	100 (328)	
ASDL	Category 3, 5e, 6, 6A	5,000 (16,404)	1.5 Mbps to 9 Mbps
VDSL	Category 3, 5e, 6, 6A	5,000 (16,404)	1,500 m (4,900 ft.) for 12.9 Mbps; 300 m (1,000 ft.) for 52.8 Mbps
Analog phone	Category 3, 5e, 6, 6A	800 (2,625)	
Fax	Category 3, 5e, 6, 6A	5,000 (16,404)	
ATM 25.6	Category 3, 5e, 6, 6A	100 (328)	
ATM 51.84	Category 3, 5e, 6, 6A	100 (328)	
ATM 155.52	Category 5e, 6, 6A	100 (328)	
ATM 1.2G	Category 6, 6A	100 (328)	
ISDN BRI	Category 3, 5e, 6, 6A	5,000 (16,404)	128 kbps
ISDN PRI	Category 3, 5e, 6, 6A	5,000 (16,404)	1.472 Mbps

Fuente: (Anixter Latinoamerica, 2017, pág. 11)

Cuando utilizamos cableado de Fibra Óptica (*FO*), las distancias y el tipo de aplicación para ser utilizadas, cambian radicalmente y esto es debido a que la Fibra Óptica es un medio de transmisión que no se encuentra afectado por *ElectroMagnetic Interference* (EMI) o *Radio Frequency Interference* (RFI). Tomando en cuenta lo anterior, podemos decir que solo existen dos tipos de cables de Fibra Óptica: Fibra Óptica Monomodal con un diámetro de 50/125 *Micrómetros* (µm) y Fibra Óptica Multimodal con un diámetro de 62.5/125 *Micrómetros* (µm). Las cuales pueden alcanzar una longitud de hasta diez kilómetros Como podremos observar en la ***Tabla 19 - Distancias y atenuación para Fibra Óptica*.**

Tabla 19 - Distancias y atenuación para Fibra Óptica

	Parameter	Multimode						Single-mode	
		62.5/125µm TIA 492AAAA (0M1)		50/125µm TIA 492AAAB (0M2)		850 nm laser-optimized 50/125µm TIA 492AAAC (0M3)		TIA 492CAAA (0S1) TIA 492CAAB (0S2)	
Application	**Nominal Wavelength (nm)**	**850**	**1300**	**850**	**1300**	**850**	**1300**	**1310**	**1550**
Ethernet 10/100BASE-SX	Channel attenuation (dB)	4.00		4.00		4.00			
	Supportable distance m.(ft)	300 (984)		300 (984)		300 (984)			
Ethernet 100BASE-FX	Channel attenuation (dB)		11.00		6.00		6.00		
	Supportable distance m.(ft)		2,000 (6,850)		2,000 (6,850)		2000 (6,850)		
Ethernet 1000BASE-SX	Channel attenuation (dB)	2.60		3.60		4.50			
	Supportable distance m.(ft)	275 (900)		550 (1804)		800 (2,625)			
Ethernet 1000BASE-LX	Channel attenuation (dB)		2.30		2.30		2.30	4.50	
	Supportable distance m.(ft)		550 (1,804)		550 (1,804)		550 (1,804)	5,000 (16,405)	
Ethernet 10GBASE-S	Channel attenuation (dB)	2.40		2.30		2.60			
	Supportable distance m.(ft)	33 (108)		82 (269)		300 (984)			
Ethernet 10GBASE-LX4	Channel attenuation (dB)		2.50		2.00		2.00	6.30	
	Supportable distance m.(ft)		300 (984)		300 (984)		300 (984)	10,000 (32,810)	
Ethernet 10BASE-L	Channel attenuation (dB)							6.20	
	Supportable distance m.(ft)							10,000 (32,810)	
Ethernet 10GBASE-LRM	Channel attenuation (dB)		1.90		1.90		1.90		
	Supportable distance m.(ft)		270 (720)		270 (720)		270 (720)		
Fibre Channel 100-MX-SN-I (1062 Mbaud)	Channel attenuation (dB)	3.00		3.90		4.60			
	Supportable distance m.(ft)	300 (984)		500 (1640)		880 (2,822)			

Fuente: *(Anixter Latinoamerica, 2017, pág. 12)*

9.2.4 Terminación del Cable

- Los cables deben ser terminados mediante la conexión del *hardware* de la misma categoría o superior.
- Los cables instalados, deberán ser debidamente marcados y anotados en los registros administrativos.
- La geometría del cable deberá permanecer lo más cercana posible al *hardware* de conexión y a los puntos de terminación.
- El par máximo desenrollado de cable par trenzado equilibrado, deberá de permanecer de acuerdo a la ***Tabla 20 - Máximo permitido de cable par trenzado desenrollado*.**

Tabla 20 - Máximo permitido de cable par trenzado desenrollado

Pair untwist lengths	
Category	Maximum pair untwist mm (in.)
3	75 (3)
5e	13 (0.5)
6	13 (0.5)
6A	13 (0.5)

Fuente: *(Anixter Latinoamerica, 2017, pág. 15)*

9.2.5 Cordones y jumpers

Los puentes de conexión cruzada y los cables de conexión modulares deben ser de la misma Categoría o más alta que la Categoría del cableado para la cual se conectan. Se recomienda que los cables modulares sean manufacturados directamente por la fábrica.

9.2.6 Requisitos de conexión para cableado apantallado

- La pantalla de los cables de par trenzado apantallado (ScTP) se debe unir a la barra colectora de conexión a tierra de telecomunicaciones (TGB) o a la barra colectora de conexión a tierra principal (TMGB) de telecomunicaciones.

- Un voltaje superior a 1 voltio eficaz entre la pantalla del cable y la toma de tierra de la toma de corriente correspondiente utilizada para proporcionar alimentación al equipo indica una conexión a tierra incorrecta.

9.3 Estándar ANSI/TIA/568-C.1.

Estándar de cableado de telecomunicaciones para edificios comerciales (*Commercial Building Telecommunications Cabling Standard*)[55]

El propósito de este estándar es el de proveer una guía sobre la planeación e instalación de un sistema de cableado estructurado para edificios comerciales.

9.3.1 Instalaciones de entrada

- Las instalaciones de entrada (EF) contienen los cables, punto (s) de demarcación de la red, hardware de conexión, dispositivos de protección y otros equipos que se conectan al proveedor de acceso (AP) o al cableado de la red privada.
- Las instalaciones de entrada incluyen conexiones entre la planta exterior y dentro del cableado de edificios.

9.3.2 Salas de equipos (ER)

- Las salas de equipos se consideran distintas de las salas de telecomunicaciones (TR) y los recintos de telecomunicaciones (TE) debido a la naturaleza o complejidad del equipo que contienen. Un ER puede alternativamente proporcionar cualquiera o todas las funciones de un TR o TE.
- La conexión cruzada principal (MC, Distribuidor C) de un edificio comercial se encuentra en un ER. Las conexiones cruzadas intermedias (CI, Distribuidor B), las conexiones cruzadas horizontales (HC, Distribuidor A), o ambas, de un edificio comercial también pueden ubicarse en un ER.

[55] Véase (Standards Reference Guide, 2017)

9.3.3 Cableado de backbone

- Proporciona interconexiones entre instalaciones de entrada (EF), espacios de proveedor de acceso (AP), espacios de proveedor de servicios (SP), salas de equipos comunes (CER), salas de telecomunicaciones comunes (CTR), salas de equipos (ER), salas de telecomunicaciones (TR) y recintos de telecomunicaciones (TE)
- Se asegura de que el cableado de la red troncal cumpla con los requisitos del Subsistema de Cableado ANSI / TIA-568-C.1 2 y del Subsistema de Cableado 3.
- Utiliza una topología en estrella.
- No permite más de dos niveles jerárquicos de conexiones cruzadas.

9.3.4 Longitud y distancias máximas

- La longitud del cable troncal se extiende desde la terminación del medio en el MC hasta un IC o HC.
- Las longitudes de cableado dependen de la aplicación y los medios elegidos. Se encuentran en la sección anterior que cubre ANSI / TIA-568-C.0.
- La longitud de los puentes de conexión cruzada y los cables de conexión en el MC o IC no debe exceder los 20 m (66 pies).
- La longitud del cable utilizado para conectar el equipo de telecomunicaciones directamente al MC o IC no debe exceder los 30 m (98 pies).

9.3.5 Reconocimiento de cableado

Los medios reconocidos, que se usarán individualmente o en combinación, son:

- Cableado de par trenzado balanceado de 100 ohmios (Categoría 3, 5e, 6 ó 6A)
- Cableado de fibra óptica multimodal: se recomienda un láser de 850 nm optimizado a 50/125 µm; 62.5 / 125 µm y 50/125 µm están permitidos
- Cableado de fibra óptica monomodo.

9.3.6 Longitud máxima del cable del área de trabajo

- Cables WA de par trenzado balanceados: la longitud máxima del cordón utilizada en el contexto de MUTOA y muebles de oficina abierta se muestra en la ***Tabla 21 - Longitud máxima del cable*****.**
- Cables WA de fibra óptica: la longitud máxima del cableado horizontal no se ve afectada por el despliegue de un MUTOA.

Tabla 21 - Longitud máxima del cable

Maximum length of horizontal cables and work area cords				
	24 AWG cords		26 AWG cords	
Length of horizontal cable	Maximum length of work area cord	Maximum combined length of work area cord, patch cords and equipment cord	Maximum length of work area cord	Maximum combined length of work area cord, patch cords and equipment cord
H m (ft.)	W m (ft.)	C m (ft.)	W m (ft.)	C m (ft.)
90 (295)	5 (16)	10 (33)	4 (13)	8 (26)
85 (279)	9 (30)	14 (46)	7 (23)	11 (35)
80 (262)	13 (44)	18 (59)	11 (35)	15 (49)
75 (246)	17 (57)	22 (72)	14 (46)	18 (59)
70 (230)	22 (72)	27 (89)	17 (56)	21 (70)

Fuente: (Anixter Latinoamerica, 2017, pág. 27)

9.4 Estándar ANSI/TIA/568-C.2.

Estándar de cableado y componentes de telecomunicaciones de par trenzado equilibrado (*Balanced Twisted-Pair Telecommunications Cabling and Components Standard*)[56]

El propósito de este estándar incluye especificaciones de componentes y cableado; así como los requisitos de prueba para el cableado de cobre, incluidos Categoría 3,

[56] Véase (Standards Reference Guide, 2017)

Categoría 5e, Categoría 6 y Categoría 6A. Eso recomienda la Categoría 5e para admitir aplicaciones de 100 MHz. Al utilizar un método de prueba de laboratorio para definir todas las categorías de hardware de conexión, la norma introduce parámetros de atenuación de acoplamiento que se están estudiando para caracterizar la potencia máxima radiada generada por corrientes de modo común para cables apantallados. El canal equilibrado de par trenzado y los requisitos de rendimiento permanente se trasladaron a este documento.

9.4.1 Categorías reconocidas de cableado

A medida que las velocidades de transmisión de datos han aumentado, el cableado de par trenzado de mayor rendimiento se ha convertido en una necesidad. Además, se tuvieron que establecer algunos medios para clasificar los cables de par trenzado horizontales y el hardware de conexión por capacidad de rendimiento. Estas capacidades se han desglosado en una serie de categorías. Las siguientes categorías están reconocidas actualmente.

- **Categoría 3:** cables y hardware de conexión con parámetros de transmisión caracterizados hasta 16 MHz
- **Categoría 5e:** cables y hardware de conexión con parámetros de transmisión caracterizados hasta 100 MHz
- **Categoría 6:** cables y hardware de conexión con parámetros de transmisión caracterizados hasta 250 MHz
- **Categoría 6A:** cables y hardware de conexión con parámetros de transmisión caracterizados hasta 500 MHz. Además, se especifican los requisitos para la diafonía exógena a fin de admitir los sistemas de transmisión 10GBASE-T

9.4.2 Retardo de propagación de canal sesgado

- El sesgo de retardo de propagación del canal debe ser inferior a 50 nanosegundos (*ns)* para todas las frecuencias desde 1 MHz hasta el límite de frecuencia superior de la Categoría.

- Para los canales de prueba en el terreno, es suficiente probar a 10 MHz solamente y el retardo de propagación del canal a 10 MHz no deberá exceder 50 *ns*.

9.4.3 Delay de propagación de enlace

- El sesgo de retardo de propagación del enlace permanente será inferior a 44 *ns* para todas las frecuencias, desde 1 MHz hasta el límite de frecuencia superior de la Categoría. Para los canales de prueba en el terreno, es suficiente probar a 10 MHz solamente y el retardo de propagación del enlace permanente a 10 MHz no deberá exceder 50 *ns*.

9.4.4 Retraso de propagación

- La inclinación del retardo de propagación del cable horizontal debe ser inferior a 45 ns/100m para todas las frecuencias desde 1 MHz hasta el límite superior de frecuencia de la Categoría.

Tabla 22 - Compatibilidad con la aplicación IEEE 10GBASE-T

IEEE 10GBASE-T application support				
	TIA Category 5e UTP	TIA Category 6 UTP	TIA Augmented Category 6 UTP	ISO Class E_A
Recognized by IEEE 802.3an	No	Yes	Yes	Yes
55-Meter Distance Support	No	Yes	Yes	Yes
100-Meter Distance Support	No	No	Yes	Yes
Extrapolated Test Limits for NEXT and PSNEXT to 500 MHz	No	No	No	Yes

Fuente: *(Anixter Latinoamerica, 2017, pág. 49)*

- Esta tabla resume las diversas opciones de cableado de par trenzado y sus respectivos atributos de rendimiento de 10 Gigabit, tal como lo definen los estándares más recientes. La categoría 5e no se reconoce como un medio de cableado viable para admitir la transmisión a 10 Gigabit, independientemente de la distancia de cableado instalada.
- El cableado de Categoría 6 solo admitirá 10 Gigabit Ethernet a una distancia máxima de 55 metros instalada.

9.4.5 Rendimiento de la transmisión

Límites de longitud máxima del cable de conexión y puente:

- 20 m (66 pies) en la conexión cruzada principal
- 20 m (66 pies) en conexión cruzada intermedia
- 6 m (20 pies) en la sala de telecomunicaciones
- 3 m (10 pies) en el área de trabajo

Cables de conexión ensamblados: pérdida de inserción (atenuación) por 100 m (328 pies) a 20 ° C = pérdida de inserción del cable UTP horizontal + 20 por ciento (debido a conductores trenzados) para todas las categorías de rendimiento.

Tabla 23 - Matriz de rendimiento de componentes compatibles

Matrix of backward-compatible mated component performance

		Category of modular connecting hardware performance			
		Category 3	**Category 5e**	**Category 6**	**Category 6A**
Modular plug and cord performance	**Category 3**	Category 3	Category 3	Category 3	Category 3
	Category 5e	Category 3	Category 5e	Category 5e	Category 5e
	Category 6	Category 3	Category 5e	Category 6	Category 6
	Category 6A	Category 3	Category 5e	Category 6	Category 6A

Fuente: *(Anixter Latinoamerica, 2017, pág. 50)*

La ***Tabla 23 - Matriz de rendimiento de componentes compatibles*****,** ilustra que el componente de menor calificación determina la calificación del enlace o canal permanente.

9.5 Estándar ANSI/TIA/568-C.3.

Estándar de componentes de cableado de fibra óptica (*Optical Fiber Cabling Components Standard*)[57]

El objetivo del estándar ANSI / TIA-568-C.3 es especificar los requisitos de rendimiento de transmisión de cable y componente para el cableado de fibra óptica de las instalaciones. Aunque este estándar está destinado principalmente a ser utilizado por los fabricantes de soluciones de cableado óptico, otros grupos como usuarios finales, diseñadores e instaladores también pueden encontrarlo útil.

9.5.1 Conector de fibra óptica

Sin conector especificado: 568 "SC" y otros diseños dúplex se pueden utilizar además de los conectores de matriz MPO o MTP.

9.5.2 Identificación del color

A menos que la codificación de color se use para otro propósito, la protección de tensión del conector y la carcasa del adaptador deben poder identificarse con los siguientes colores:

- fibra de 50/125 µm optimizada para láser de 850 nm - aqua
- fibra 50/125 µm - negro
- fibra de 62.5 / 125 µm - beige
- fibra monomodo - azul
- conectores monomodo de férula de contacto en ángulo - verde

[57] Véase (Standards Reference Guide, 2017)

9.5.3 Salida de telecomunicaciones de FO

- Capacidad para terminar un mínimo de dos fibras en acoplamientos 568 "SC" u otra conexión dúplex
- Medios para asegurar la fibra y mantener un radio de curvatura mínimo de 25 mm (1 pulg.)

9.5.4 Empalmes de Fibra Óptica, Fusión o Mecánica

Pérdida máxima de inserción 0.3 dB

- Pérdida mínima de retorno:
    - multimodo: 20 dB
    - modo único: 26 dB
    - modo único: 55 dB (CATV analógico)

9.5.5 Conector de fibra óptica

- Pérdida máxima de inserción 0,75 dB

9.5.6 Patch Cords

- Deberá ser de doble fibra del mismo tipo que la fibra horizontal y de la columna vertebral
- La polaridad debe ser dúplex con clave

9.6 Estándar ANSI/TIA/569-D.

Rutas y espacios de telecomunicaciones (*Telecommunications Pathways and Spaces*)[58]

Los sistemas de telecomunicaciones tienen un impacto en casi todas las áreas dentro y entre edificios. La complejidad de las telecomunicaciones ha aumentado y ahora incluye voz, datos, video, control de acceso, fuego y seguridad, audio, medio ambiente y otros controles de construcción inteligente sobre los medios que incluyen

[58] Véase (Standards Reference Guide, 2017)

cableado de datos de cobre, fibra óptica y varias formas de transmisión inalámbrica. Este estándar reconoce que los edificios tienen un ciclo de vida prolongado y deben diseñarse para soportar sistemas de telecomunicaciones y medios dinámicamente cambiantes a lo largo de la vida del edificio.

- Este documento estandariza las prácticas específicas de diseño y construcción de vías y espacios con el fin de admitir los medios y equipos de telecomunicaciones dentro de los edificios.
- No estandariza en los medios o equipos.
- Proporciona información útil sobre las alternativas de diseño estándar de la industria disponibles para vías y espacios de telecomunicaciones.
- Depende del diseñador de telecomunicaciones seleccionar adecuadamente entre las alternativas en función de las aplicaciones que se emplean y las diversas limitaciones impuestas.

9.6.1 Arquitectónico y Ambiental

- Ubique la habitación del distribuidor lo más cerca posible del centro del área atendida.
- Si hay varias salas de distribución en el mismo piso, deben estar interconectadas con mínimo un conducto de tamaño comercial 3 o una ruta equivalente.
- Tamaño: el espacio mínimo debe basarse en la cantidad de salidas de equipos (Distribuidor A) servidas directamente. La dimensión mínima es de 3 m (10 pies) de largo por 3 m (10 pies) de ancho. Una sala de distribución que contenga el Distribuidor B debe tener un mínimo de 10 m² (100 pies cuadrados). Una sala de distribución que contenga el Distribuidor C debe tener un tamaño mínimo de 11 m^2 (120 $pies^2$) para construir con un área total de hasta 50,000 m^2 (500,000 $pies^2$). En edificios más grandes, el tamaño de la sala de distribución que contiene el Distribuidor C debe aumentarse en incrementos de 1 m^2 (10 $pies^2$) por cada aumento de 10,000 m^2 (100,000 $pies^2$) en el área de construcción bruta.

- Habrá un mínimo de una habitación de distribuidor por piso.
- Debe haber un mínimo de dos receptáculos de dúplex de CA dedicados, no conmutados, de 120 VCA, cada uno en un circuito derivado dedicado separado de 20 A.
- La temperatura y la humedad se controlarán para cumplir con los requisitos de la Tabla 9.
- Se debe proporcionar un sistema de unión y conexión a tierra según lo especificado por ANSI / TIA-607-C.

9.6.2 Sala de entrada o espacio

La sala de entrada es un espacio en el que tiene lugar la unión de instalaciones de telecomunicaciones inter o intraconstrucción. Es un punto de entrada para el cableado de la planta externa y puede contener cables, protectores y cables de construcción del proveedor de servicios entrantes. Una sala de entrada también puede servir como sala de distribución.

- Se ubicará en un área seca no sujeta a inundación y tan cerca como sea posible del punto de entrada del edificio.
- Tamaño para cumplir con los requisitos presentes y futuros del Distribuidor C.
- Puede ser un área abierta o habitación. Para edificios de más de 2,000 m² (20,000 pies cuadrados), se debe proporcionar una habitación cerrada. En edificios de hasta 10,000 m² (100,000 pies cuadrados), puede ser conveniente utilizar hardware de terminación montado en la pared. Un área de piso más grande puede requerir el uso de marcos independientes para terminar los cables.
- Se debe proporcionar un sistema de unión y conexión a tierra como se especifica en ANSI / TIA-607-C.

9.7 Clasificación *Tier* para centros de datos

Dentro del estándar ANSI/TIA-942 *Telecommunications Infraestructure Standard For Data Centers*, existe un sistema de clasificación que fue inventado por el *Uptime Institute* que fue diseñado para clasificar la fiabilidad de los centros de datos. La clasificación *Tier* (Guillarte, 2013) la cual nos indica el nivel de fiabilidad de un centro de datos asociado a cuatro niveles de disponibilidad definidos, por lo tanto mientras más alto sea al nivel del *Tier* asociado, mayores los costos de implementación asociados a la construcción del centro de datos.

Como podremos observar en la ***Ilustración 23 - Sistema de clasificación Tier***, el sistema de clasificación *Tier* se encuentra basado en la disponibilidad y fiabilidad del centro de datos y es uno de los conceptos que deben de estar siempre presente al momento de diseñar, planificar y construir un centro de datos.

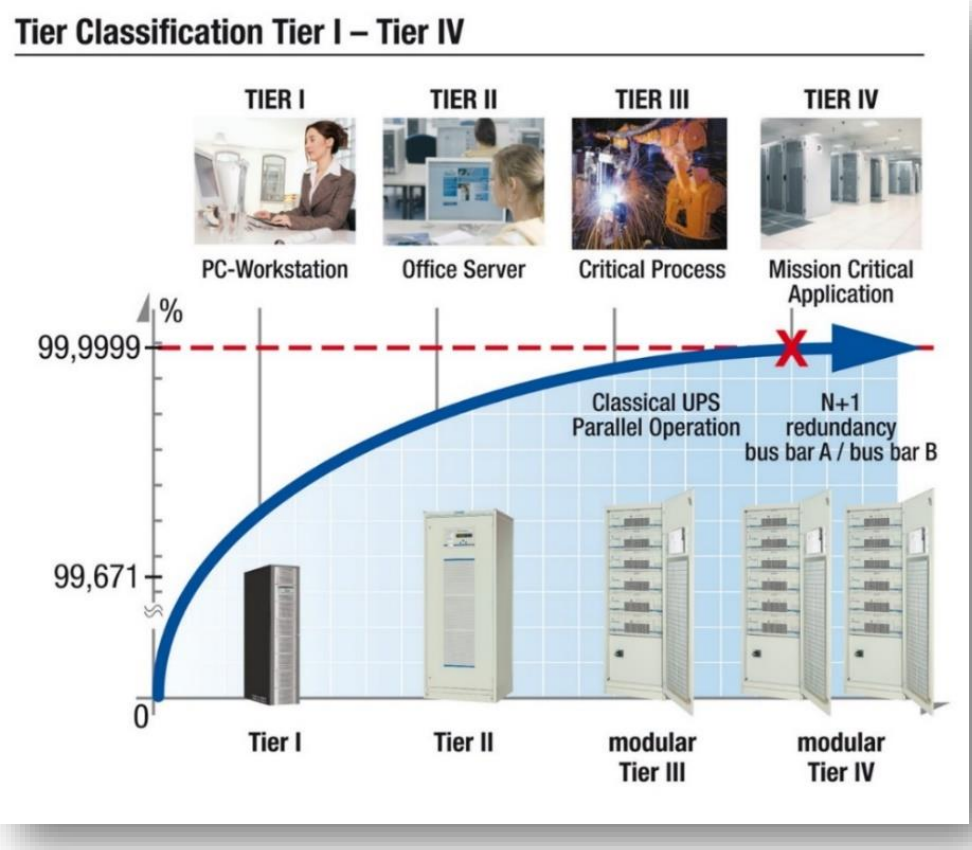

Ilustración 23 - Sistema de clasificación Tier
Fuente: *(Guillarte, 2013)*

De acuerdo a Guillarte (2013), las características principales de clasificación de un *Tier*, se encuentran definidas de la siguiente forma ordenadas de menor a mayor:

9.7.1 *Tier* I: centro de datos básico

- Disponibilidad del 99.671 por ciento.
- El servicio puede interrumpirse por actividades planeadas o no planeadas.
- No hay componentes redundantes en la distribución eléctrica y de refrigeración.
- Puede o no tener suelos elevados, generadores auxiliares o UPS.
- Tiempo medio de implementación, 3 meses.
- La infraestructura del centro de datos deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones.

9.7.2 *Tier* II: centro de datos redundante

- Disponibilidad del 99.741 por ciento
- Menos susceptible a interrupciones por actividades planeadas o no planeadas.
- Componentes redundantes (N+1).
- Tiene suelos elevados, generadores auxiliares o UPS.
- Conectados a una única línea de distribución eléctrica y de refrigeración.
- De 3 a 6 meses para implementar.
- El mantenimiento de esta línea de distribución o de otras partes de la infraestructura requiere una interrupción del servicio al año.

9.7.3 *Tier* III: centro de datos concurrentemente sostenible

- Disponibilidad del 99.982 por ciento.
- Permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas.

- Componentes redundantes (N+1).
- Conectados múltiples líneas de distribución eléctrica y de refrigeración; pero únicamente con una activa.
- De 15 a 20 meses para implementar.
- Hay suficiente capacidad y distribución para poder llevar a cabo tareas de mantenimiento en una línea mientras se da servicio por otras.

9.7.4 *Tier* IV: centro de datos Tolerante a fallos

- Disponibilidad del 99.995 por ciento.
- Permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento no planificado del tipo “peor escenario” sin impacto crítico en la carga.
- Conectados múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes redundantes 2(N+1) significa 2 UPS con redundancia (N+1).
- De 15 a 20 meses para implementar.

10 Glosario de términos

Backbone. – (Núcleo estructural de la red) es el cable que conecta todos los componentes de la red de manera que se pueda producir la comunicación.

Big Data. - El concepto de Big Data pertenece a la lengua inglesa y no forma parte del diccionario que elabora la Real Academia Española (RAE). La noción alude al almacenamiento y la gestión de una cantidad elevada de datos.

BYOD. - *Bring Your Own Device* (BYOD) es una tendencia cada vez más generalizada en la que las empresas permiten a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

CAGR. - La tasa de crecimiento anual, por sus siglas en inglés *CAGR (Compound Annual Growth Rate)* es un concepto con el cual se mide la tasa de rendimiento de una inversión a lo largo del tiempo, por lo general a términos largos

Cloud Computing. - La expresión inglesa *Cloud Computing* es de uso frecuente en nuestra lengua, aunque puede traducirse como Computación en la Nube o informática en la Nube. El concepto refiere a la oferta de diversos servicios y prestaciones digitales a través de la infraestructura de una red.

CRM. - CRM es una sigla de la lengua inglesa que alude a la expresión *Customer Relationship Management* (la cual se puede traducir como “administración de las relaciones con los clientes”).

DoS. - En Internet, un DoS o ataque de denegación de servicio (no confundir con DOS, *Disk Operating System*, con O mayúscula) es un incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar. Habitualmente, la pérdida del servicio supone la indisponibilidad de un

determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red.

DDoS. - *Distributed Denial of Service Attack*. Es un ataque DoS realizado por muchas personas a un servidor de Internet, causando que sus servicios sean inaccesibles por usuarios legítimos

EIA. - (*Electronic Industries Alliance*; Asociación de Industrias Electrónicas) Grupo que especifica los estándares de transmisiones eléctricas, EIA y TIA han desarrollado en conjunto numerosos estándares de comunicación de amplia difusión.

Exabyte. - Un exabyte (EB) es una unidad de almacenamiento de información digital que se utiliza para indicar el tamaño de los datos. Exabyte es equivalente a 1 mil millones de gigabytes (GB)

Housing. - Servicio de alojamiento, conexión, gestión y administración de equipos informáticos.

Hosting. - Se conoce como alojamiento web al servicio de almacenamiento de los datos que son accesibles mediante Internet.

HUD. - Acrónimo del término inglés *Heads-Up Display* (Presentación de Información). Conjunto de iconos, números, mapas, etc. que durante el juego nos dan información sobre el estado de nuestra partida y/o nuestro personaje, como por ejemplo vida restante, ubicación, munición, objetos en uso, etc. También se denomina interfaz o UI (*User Interface*).

HVAC. - Calefacción, ventilación y aire acondicionado. Son las siglas de calefacción, ventilación y aire acondicionado

IPv4. - *Internet Protocol* Versión 4, Protocolo Internet Versión 4.

Latencia. - En el sector de la informática, la latencia refiere a los retardos temporales que se registran en una red. Estos retardos se producen por la demora en la propagación y en la transmisión de los paquetes de datos. Al sumarse todos estos retardos, se obtiene la latencia de la red informática.

Malware. - *Malware* es un acrónimo del inglés de *malicious software*, traducido al español como código malicioso. Los *malwares* son programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.

M2M. - Acrónimo de *machine to machine* (en español, de máquina a máquina), una expresión que designa a la tecnología que permite a dos máquinas remotas —un robot, un automóvil, una máquina industrial...— intercambiar información o comunicación en forma de datos, así como realizar acciones de forma totalmente autónoma, esto es, sin intervención humana. No debe confundirse con el concepto *IoT*. La tecnología M2M puede considerarse un subconjunto del Internet de las Cosas, ya que la primera es la que proporciona a la segunda la conectividad que la hace posible.

PUE. - La eficacia del uso de la energía (PUE, por *Power Usage Effectiveness*) es una medida utilizada para determinar la eficiencia energética de un centro de datos. El PUE se determina al dividir la cantidad de energía que ingresa a un centro de datos entre la potencia utilizada para ejecutar la infraestructura de la computadora dentro de este.

Ransomware. - Los *ransomwares* son unos programas informáticos, elaborados de manera malintencionada, que limitan o bloquean el acceso de los usuarios a diversos sistemas o archivos, a menos que se efectúe un pago por el rescate de éstos.

Switch. – Dispositivo que conecta computadoras.

TIA. - (*Telecommunications Industry Association*; Asociación de la Industria de las Telecomunicaciones) Organización que desarrolla estándares relacionados con las tecnologías de las telecomunicaciones.

UTP. - Un cable es un cordón que está resguardado por alguna clase de recubrimiento y que permite conducir electricidad o distintos tipos de señales. Los cables suelen estar confeccionados con aluminio o cobre. UTP, por otra parte, es una sigla que significa *Unshielded Twisted Pair* (lo que puede traducirse como “Par trenzado no blindado”). El cable UTP, por lo tanto, es una clase de cable que no se encuentra blindado y que suele emplearse en las telecomunicaciones.

VoIP. – (*Voice over IP*: Voz sobre Protocolo Internet) La habilidad para transportar voz telefónica normal sobre una red de datos basada en el protocolo de la Internet, con la misma funcionalidad, confiabilidad y calidad de voz que ofrecen las empresas telefónicas tradicionales

WAN. - WAN es la sigla de *Wide Area Network* (“Red de Área Amplia”). El concepto se utiliza para nombrar a la red de computadoras que se extiende en una gran franja de territorio, ya sea a través de una ciudad, un país o, incluso, a nivel mundial.