UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

DIAGNÓSTICO SITUACIONAL DEL DATA CENTER BAJO CUMPLIMIENTO NORMATIVO Y DE ESTÁNDAR EN EL HOSPITAL II ESSALUD DE HUARAZ; 2017.

TESIS PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

BACH. TONGO EVANGELISTA, YONEN YONEL

ASESOR:

ING. JAMANCA RAMIREZ MARCO ANTONIO

HUARAZ – PERÚ

2017

JURADO EVALUADOR DE TESIS Y ASESOR

DR. VICTOR ANGEL ANCAJIMA MIÑAN

Presidente

DR. JUAN RAÚL CADILLO LEÓN

Secretario

MGTR. ERICK GIOVANNY FLORES CHACÓN

Miembro

ING. MARCO ANTONIO JAMANCA RAMIREZ

Asesor

DEDICATORIA

A mi querido padre; Marino Simeón, quien siempre está presente en mi corazón, a mi madre Delia Evangelista por su apoyo incondicional; además a mi hermana por su apoyo, buenos consejos para seguir adelante en mis estudios y lograr ser un profesional con mucho éxito.

Yonen Yonel Tongo Evangelista

AGRADECIMIENTOS

A nuestro Dios Padre, a su hijo señor Jesucristo por brindarme sus bendiciones cada día en la realización de mis estudios, metas y siempre confió en ellos.

A los docentes de esta casa superior de estudios que me brindaron sus enseñanzas con dedicación y me formaron profesionalmente.

A mis amigos y compañeros, que supieron brindarme su apoyo incondicional y con quienes he llegado a compartir y aprender.

A todas las personas que de una manera u otra hicieron posible la realización de la presente investigación.

Yonen Yonel Tongo Evangelista

RESUMEN

Esta Tesis ha sido desarrollado bajo la línea de investigación: Implementación de las tecnologías de información y comunicación para mejorar continua de la calidad en las organizaciones del Perú, de la escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote, con el objetivo de determinar el diagnostico situacional del Data Center bajo normativas y estadales de Hospital II EsSalud Huaraz. La investigación tuvo un diseño no experimental de tipo descriptivo. La población en estudio fue un centro de datos de la organización; el instrumento metodológico que se utilizó para determinar el diagnostico de estas variables fue un CheckList; Con lo que una vez se aplicó el instrumento de recolección de datos se obtuvieron los siguientes resultados: En lo que respecta las cuatro dimensiones en la tabla Nro 32 se puede interpretar que el 40.7% del total de ítems no cumplen con los controles que establecen los estándares y normativa; mientras que el 59.3% de los ítems si se cumplen; Estos resultados coincidió con lo propuesto en el hipótesis general planteada en la investigación donde se planteó que el diagnostico situacional del data center determinara las mejoras y continuidad del servicio que brindan el data center de la EsSalud red asistencial de Ancash – Huaraz; por lo que esta hipótesis quedan demostradas y aceptadas. Finalmente, La investigación queda debidamente justificada en la necesidad de contar con el diagnostico situacional del Data Center lo cual determinara su continuidad y/o mejoras de los servicios que brinda el data center.

Palabras Clave: Data Center, Diagnostico Situacional, Metodología, Estándar, Normas, Controles.

ABSTRACT

This thesis has been developed under the line of research: Implementation of information and communication technologies for continuous improvement of quality in the organizations of Peru, of the Professional School of Systems Engineering of the Universidad Católica los Ángeles de Chimbote, with the objective of determining the situational diagnosis of the Data Center under normative and state of Hospital II EsSalud Huaraz. The research had a non-experimental design of descriptive type. The study population was a data center of the organization; the methodological tool that was used to determine the diagnosis of these variables was a CheckList; As a result of the data collection instrument, the following results were obtained: With regard to the four dimensions in Table Nro 32 it can be interpreted that 40.7% of the total items do not comply with the controls established by the standards and regulations; while 59.3% of the items are met; These results coincided with what was proposed in the general hypothesis raised in the research where it was proposed that the situational diagnosis of the data center determine the improvements and continuity of the service provided by the EsSalud data center of Ancash - Huaraz; so this hypothesis is demonstrated and accepted. Finally, the investigation is duly justified in the need to have the situational diagnosis of the Data Center which will determine its continuity and / or improvements of the services provided by the data center.

Keywords: Data Center, Situational Diagnosis, Methodology, Standard, Norms, Controls.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

I. INTRODUCCIÓN

Un Centro de Datos o Data Center es el lugar donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También llamado Centro de Cómputo, cumple varias funciones siendo la principal el administrar y gestionar servicios informáticos.

La intención de este estudio es proporcionar información general sobre el estado situacional del data center de la EsSalud, factores que se deben tener en cuenta para un centro de datos, basándose en la normativa TIA-942 quien ofrece recomendaciones acerca de la instalación de hardware necesario para crear una infraestructura en un entorno operativa, siendo necesario para garantizar la continuidad del servicio y la protección física de los equipos informáticos o de comunicaciones; el mismo que ayudará a futuras generaciones como un material de consulta y aprendizaje

Las normas ejercen muchas presiones sobre los centros de datos, desde el punto de vista del cumplimiento de normativas, como del efectivo desarrollo de operaciones, lo cual es indispensable la incorporación del servicio para cubrir eficientemente las necesidades actuales de la institución. La normativa TIA-942 determina los pasos en el proceso de diseño que se describen y se aplican al diseño de un nuevo centro de datos o la ampliación de un centro de datos existente.

La problemática actual de la organización EsSalud Huaraz, está en el centro de datos, contando con servidores instalados en un espacio pequeño e inadecuado, instalaciones de más de 4 años de antigüedad, muchos de ellos sin contrato de soporte y mantenimiento así como también computadoras personales funcionando como servidores, esta situación es particularmente alarmante por cuanto pone en serio riesgo la operatividad dela organización. (1)

En la actualidad el centro de datos del EsSalud de Huaraz está expuesta a múltiples amenazas, a raíz de que su implementación fue limitado, ajeno a normas y estándares y no escalable; En un proyecto de implementación de un Data Center como punto crítico y la cual determinara su seguridad es eliminar los puntos de fallas y aumentar la confiabilidad de las informaciones de la institución o empresa, por lo tanto es importante que los data centers estén preparados para resistir tanto catástrofes

naturales como cualquier incidente y/o amenazas físicas que abarcan desde incendios de grandes proporciones hasta un simple vaciamiento de agua en el Data Center. Calor, humo y gases corrosivos deben ser evitados, pues dañan hardware y datos.

En base a la problemática descrita en el párrafo anterior, se planteó el siguiente enunciado del problema: ¿Cuál es el diagnostico situacional del Data Center bajo normativa y estándares en el EsSalud-Red asistencial Ancash en el año 2017?

En esta investigación se propuso lograr cumplir con el siguiente objetivo general: Determinar el diagnóstico situacional del data center bajo cumplimiento normativo y de estándares en la EsSalud red asistencial Áncash – Huaraz en el año 2017.

Para lograr cumplir dicho objetivo general se propuso los siguientes objetivos específicos:

1. Realizar un estudio detallado de la infraestructura del data center del EsSalud.
2. Identificar los controles de las normativas y estándares universales para el diseño de un data center.
3. Elaborar y aplicar el instrumento de medición al data center para determinar el estado situacional bajo normativa y estándares.
4. Describir el estado situacional del data center por sus dimensiones.

El presente estudio de investigación cobra importancia debido a la necesidad de contar con el diagnostico situacional del data center lo cual determinara su continuidad y/o mejoras de los servicios que brinda el data center, la rápida evolución de las TIC y la necesidad de estar conectados en todo momento han obligado a las empresas a requerir un alto nivel de fiabilidad y sobre todo la seguridad de los servicios del data center, de tal forma que se proteja la información corporativa y esté disponible sin interrupciones o degradación del acceso.

El presente trabajo se desarrolló en el departamento de Ancash, Ciudad de Huaraz, Organización EsSalud Red Asistencial Ancash-Huaraz, que abarca en el área de informática Centro de Datos (Data Center), buscando lograr determinar el estado situacional del mismo.

II. REVISIÓN DE LA LITERATURA.

2.1 Antecedentes

2.1.1 Antecedentes a nivel Internacional

ADC Telecommunications (2) usa, 2005 en su informe técnico "Cómo diseñar un centro de datos óptimo" concluye que un centro de datos óptimo es un sistema bien diseñado, cuyas piezas trabajan juntas para garantizar un acceso fiable a los recursos del centro y brindan la flexibilidad necesaria para satisfacer las necesidades desconocidas que puedan surgir en el futuro. Descuidar cualquier aspecto del diseño puede dejar al centro de datos vulnerable a fallas muy costosas u obsolescencia prematura. Este informe técnico ha tratado varias consideraciones de diseño clave y brindado recomendaciones.

Ing. German Patricio Villamarín Coronel (3) Ecuador, 2010 en su proyecto de grado magister "Análisis de los requerimientos funcionales y de operación para la implementación del data center de la universidad nacional de Loja" concluye que Actualmente la Universidad cuenta con un espacio en donde se ubican rack y servidores ubicados en el último piso del Edificio de la Administración Central, el cual no cuenta con acceso restringido, un DMZ, seguridad es, ventilación, piso falso, por lo que este proyecto servirá de base para la implementación de un Data Center seguro y que cumpla con las normas TIA-942, ANSI/TIA/EIA 568-B Y ANSI/TIA/EIA-607 entre las más importantes.

Ricardo Napoleon Guagalango Vega, Patricio Esteban Moscoso Montalvo (4) Ecuador, 2011 en su tesis pre-grado "Evaluación técnica de la seguridad informática del data center de la escuela politécnica del ejército" concluye La Seguridad Informática permite proteger la infraestructura computacional incluyendo la información contenida, por ello debe ser tratado con la mayor responsabilidad en todas las áreas del Data Center, siendo uno de los factores de éxito principales la comunicación en la organización, porque el recurso humano organizado con Normas y Políticas establecidas más las herramientas computacionales

colaboran en la prevención de amenazas y disminución de Riesgos en Seguridad.

Jordi Arjona Aroca (5) España, 2015**,** en su tesis doctoral "PROBLEMAS ESTRUCTURALES Y EFICIENCIA ENERGÉTICA EN CENTROS DE DATOS" concluye que la computación en nube está vivo y probablemente no más de un niño todavía. Sin embargo, incluso en esta temprana edad ya somos capaces de ver muchas de las ventajas, sin duda no todos, que el cloud computing puede ofrecernos. A pesar de todas estas ventajas, no debemos olvidarnos de sus inconvenientes y este fue uno de los objetivos de esta tesis. El objetivo principal de esta tesis era hacer frente a dos de los principales problemas de los centros de datos, los costes estructurales y el consumo de energía, que se introdujeron en la Parte I. La reducción de los costos asociados a estas dos cuestiones no sólo es un objetivo económico, sino también, con mayor claridad en el caso del consumo de energía, un problema ambiental. La energía se genera a un costo y, por tiempo indefinido el aumento de nuestro consumo de energía tendrá un efecto perjudicial en nuestro mundo. Es nuestro deber, como investigadores, que se preocupan por la sostenibilidad y asegurar que los tiempos futuros serán mejores.

María Aguirre Patiño, Rut España Peláez, Iván Solís Granda, Alfonso Aranda Segovia (6) Ecuador**,** en su proyecto "Diseño y Simulación de un Data Center Cloud Computing que cumpla con la norma PCI-DSS" que como objetivo es de Diseñar y simular un Data Center que provea servicios de Cloud Computing al mercado local cumpliendo con el estándar de la norma PCI-DSS y concluye que las 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.

Yaselga Yaselga, Edwin Homero (7) Quito, 2013 en su tesis pre-grado "Diseño del Centro de Datos para Petroecuador en el edificio matriz en base al Estándar TIA-942-2" concluye que el diseño del Centro de Datos para la Empresa Pública PETROECUADOR, no solo está enfocado en lograr una administración centralizada de todos sus equipos informáticos, sino también en proporcionar escalabilidad en cuanto a su infraestructura física y tecnológica. De acuerdo a las diferentes distribuciones de equipos de red y servidores, encontrados en los racks del cuarto de cómputo, se procedió a realizar una redistribución de estos equipos en base a sus niveles de potencia, con el objetivo de disminuir los niveles de temperatura ocasionados por la aglomeración de equipos en ciertos racks.

Diana Carolina Córdova Flores (8) Ecuador 2012**,** en su tesis pregrado "data center 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" como objetivo general se plantea Diseñar un Centro de Datos (Data Center) aplicando estándares internacionales 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. Y concluye que Un centro de datos o Data Center es un lugar acondicionado para albergar un buen número de servidores y equipos de comunicaciones acomodados en racks, con temperatura y humedad constante y altos niveles de seguridad.

Wilson Fernando, Freile Sandoval (9) Quito, 2008, en su tesis pre-grado "diseño y construcción de un módulo de monitoreo y control del suministro de energía eléctrica a un data center a través de la internet", concluye que La automatización de distintos tipos de dispositivos es una herramienta muy importante para el departamento técnico de cualquier empresa, el presente proyecto constituye un prototipo de un sistema alternativo, para dar solución de los problemas que surgen por el abastecimiento de energía eléctrica, en lugares donde se requiere un suministro de energía constante.

2.1.2 Antecedentes a nivel Nacional

Jocelyne Estelita Nogueira Solís (10) Lima, 2013 en su tesis pre-grado "Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER" con el objetivo diseñar un procedimiento de auditoría física y medio ambiental para centros de datos (Data Center) basado en la clasificación y estándar internacional TIER, con la finalidad de verificar las condiciones de seguridad de información con las que cuentan dichas instalaciones, concluyendo que los procedimientos han podido ser correctamente aplicados en la auditoría a un Data Center real, permitiendo obtener los resultados adecuados que demuestren la efectividad o deficiencia de los controles que se hayan implantado y que perjudican la seguridad y continuidad de operación.

Liliana Raquel Castillo Devo (11) Lima, 2008, en su tesis pre-grado "Diseño De Infraestructura De Telecomunicaciones Para Un Data Center" concluye que 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.

Luis Alfredo López Córdova (12) Lima, 2008, en su proyecto de tesis "Diseño de red power over Ethernet con categoría 6ª para aplicación en data center" concluye que el principal problema es que no hay conocimiento integral de los demás profesionales como Arquitectos, ingenieros electrónicos, ingenieros Civiles y sanitarios que interviene de alguna manera en los proyecto de redes, no toman en consideración los requerimientos básicos de una res física, es de suma urgencia que los profesionales de redes empiecen a firmar los planos para que en las obras no se encuentren dificultades como ducterias de menos diámetro a la especificada para el recorrido de los cables.

2.2 Bases Teóricas

2.2.1. Organización EsSalud Red Asistencial de Ancash - Huaraz

Antecedentes

El 12 de agosto de 1936 se promulga la Ley N.º 8433 que crea la Caja Nacional del Seguro Social Obrero, marcando prácticamente el inicio de la Seguridad Social en el Perú. Anteriormente conocido como el Instituto Peruano de Seguridad Social (IPSS).

El Seguro Social de Salud, EsSalud, es un organismo público descentralizado, con personería jurídica de derecho público interno, adscrito al Sector Trabajo y Promoción Social. Tiene por finalidad dar cobertura a los asegurados y sus derechohabientes, a través del otorgamiento de prestaciones de prevención, promoción, recuperación, rehabilitación, prestaciones económicas, y prestaciones sociales que corresponden al régimen contributivo de la Seguridad Social en Salud, así como otros seguros de riesgos humanos.

Información del rublo

EsSalud empresas del rubro de Seguro Social de Salud.

Visión:

Ser una institución que lidere el proceso de universalización de la seguridad social, en el marco de la política de inclusión social del Estado.

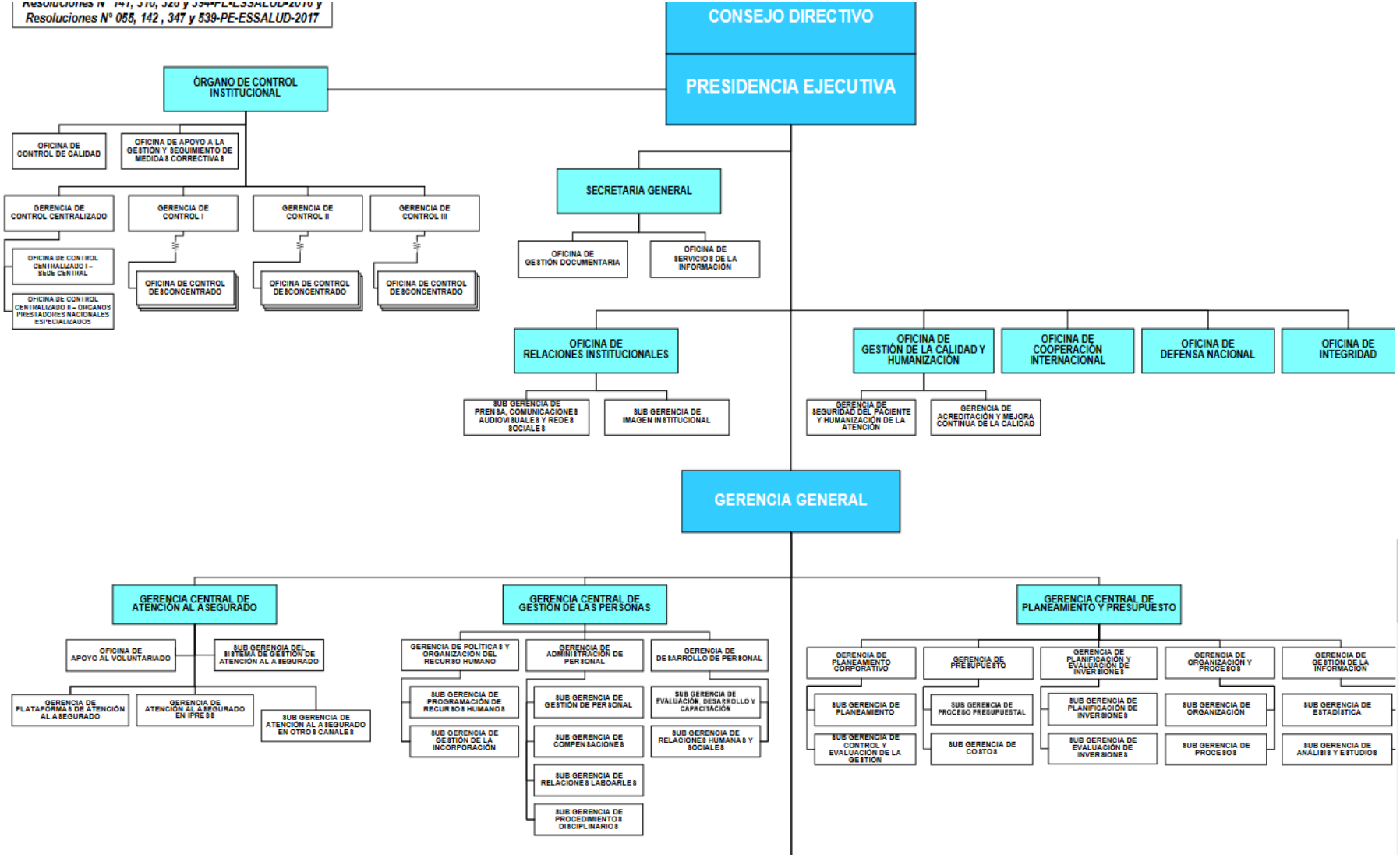
Misión:

Somos una institución de seguridad social de salud que persigue el bienestar de los asegurados y su acceso oportuno a prestaciones de salud, económicas y sociales, integrales y de calidad, mediante una gestión transparente y eficiente.

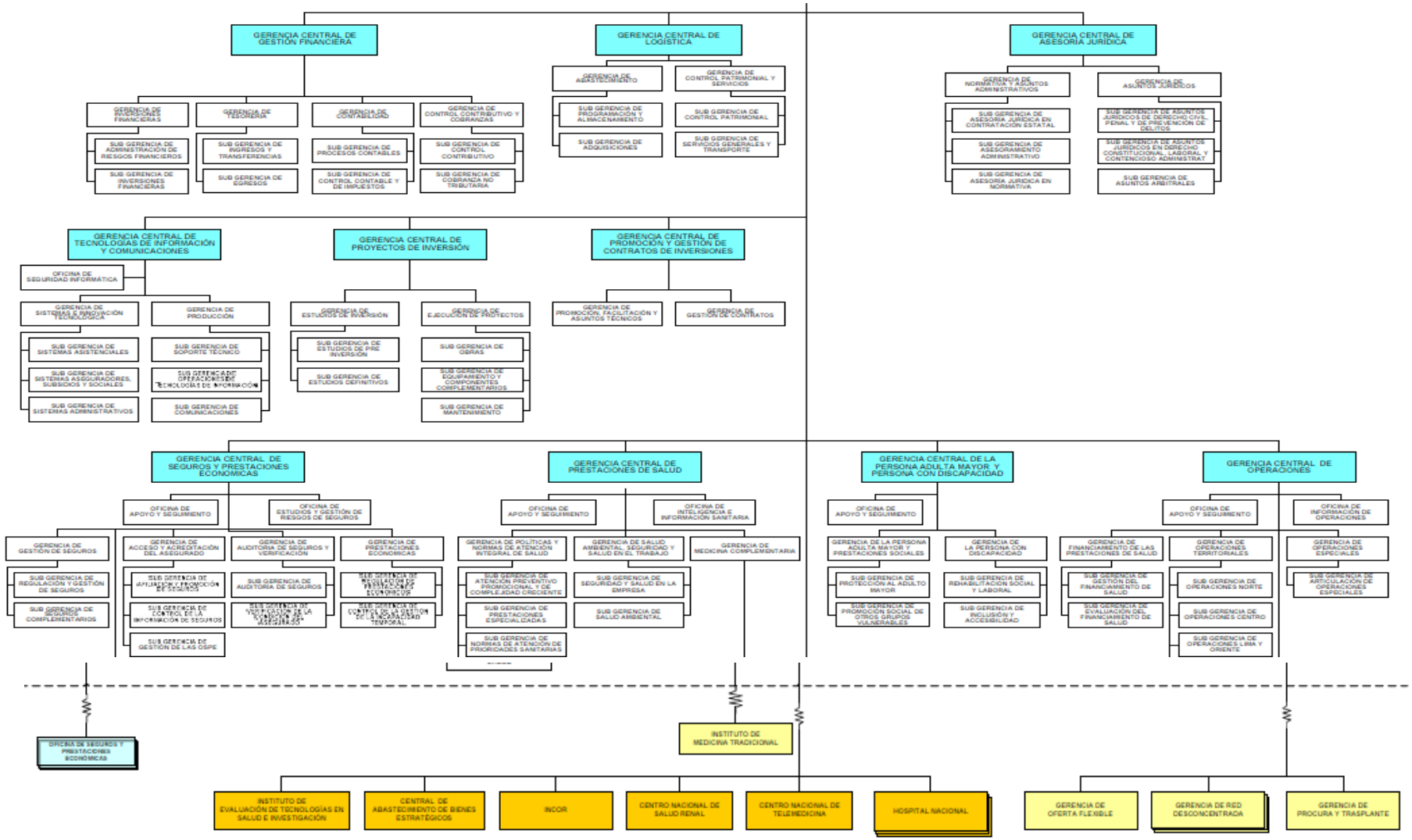
Ubicación:

Campamento Vichay s/n –Independencia - Huaraz
CENTRAL (043) 422940.

Ilustración Nro 01: Organigrama estructural del EsSalud



Fuente: Resolución N° 656-PE-ESSALUD-2014



Fuente: Resolución N° 656-PE-ESSALUD-2014

Centros Asistenciales:

- Hospital II Huaraz
- Centro Medico Carhuaz
- Posta Medica Yungay
- Posta Medica Piscobamba
- Centro Medico Caraz
- Centro Medico Huari

2.2.3.2. INFRAESTRUCTURA DATA CENTER

La implementación del data center del hospital II Huaraz no está bajo ningún normativa, una implementación de forma empírica y provisional, con una instalación de cableado estructurado de 5 años de antigüedad, servidores sin raspados de seguridad.

Servicios:

- Internet Speedy Telefónica
- Servidor de sistema de gestión General
  Plataforma Linux

  Módulos:

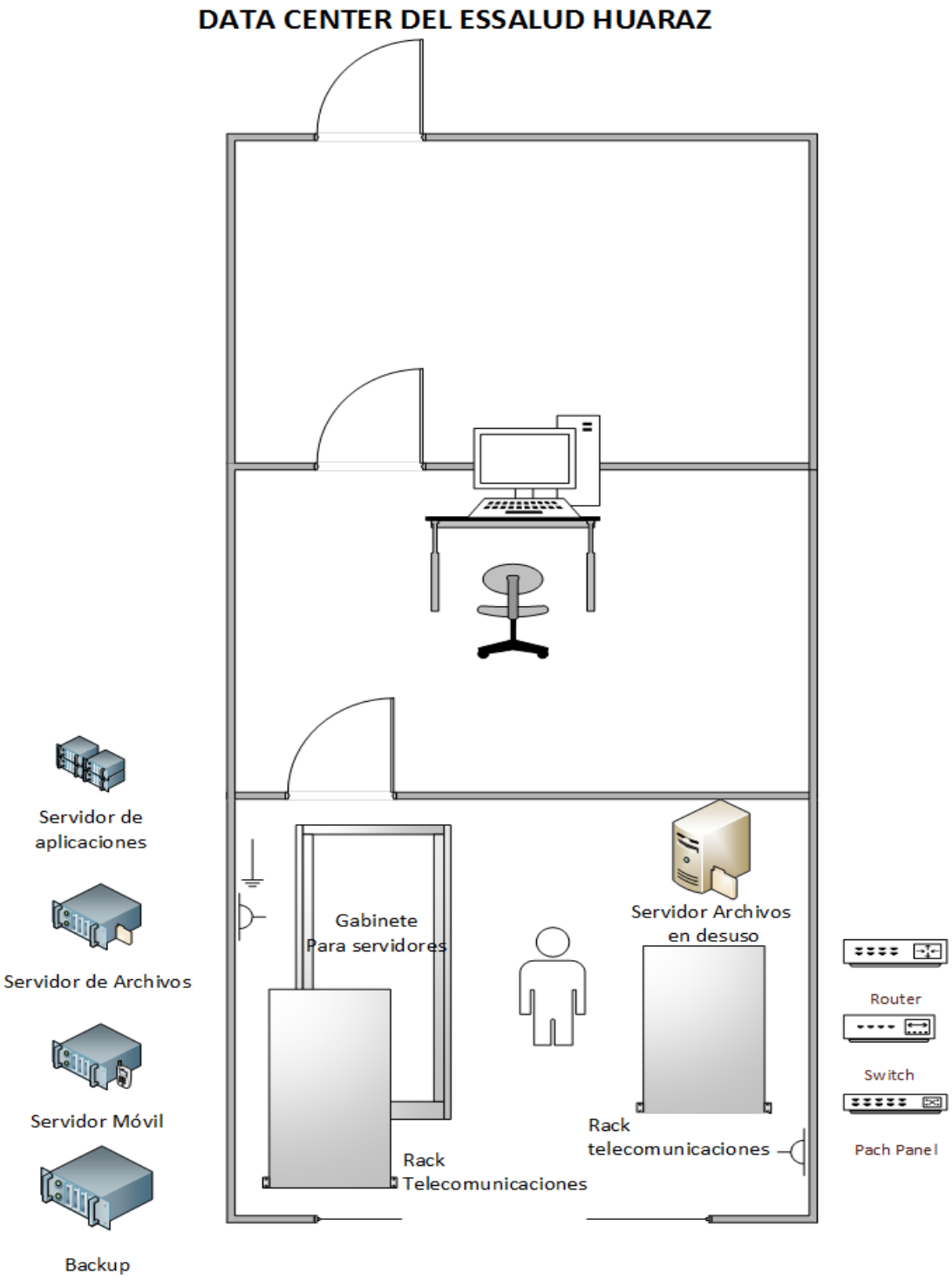
  - Admisión
  - Historia Clínica
  - Farmacia
  - Hospitalización
  - Emergencia
  - Centro Quirúrgico
  - Central de Depósitos
  - Estadísticas
  - Facturación
  - Seguridad
  - Utilitarios
  - Otros Módulos
- Servidos de comunicaciones central de telefonía
  T-Conecta central telefónica Asterisk
- Servidor de Aplicaciones.
- Servidor de Backus

Usuarios finales de los servicios:

Hospital II Huaraz: 150	CM Caraz: 25
CM Carhuaz: 20	CM Huari: 20
PM Yungay: 7	PM Piscobamba: 6

Ascendiendo a un total de 228 usuarios que cuentan con los servicios que brindan el centro de datos de la red asistencial Huaraz.

Ilustración Nro 02: Infraestructura actual del data center



Fuente: Elaboración Propia

Galería de imágenes del Data center EsSalud de Huaraz

Ilustración Nro 06: Rotulado del cableado

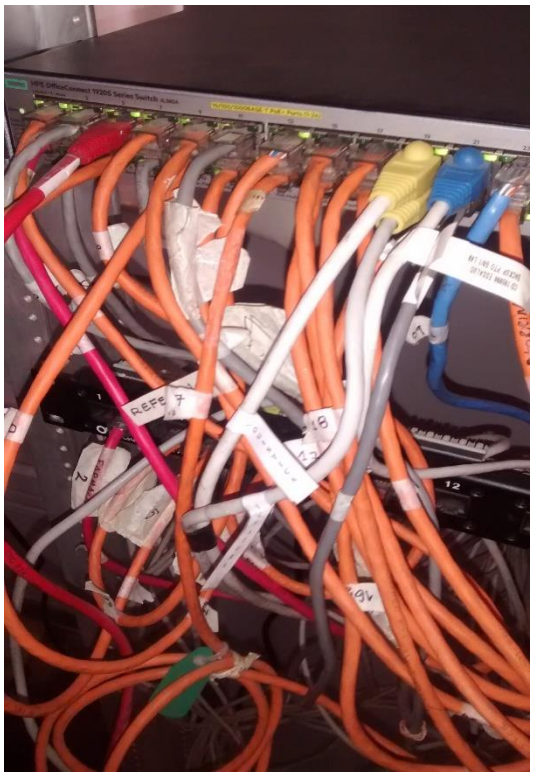
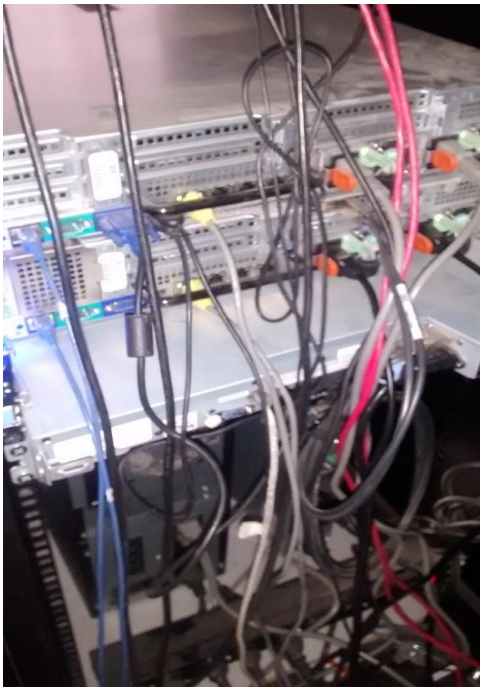


Ilustración Nro 04: Servidor en desuso

Ilustración Nro 03: organización de cables

Ilustración Nro 05: Tendido de cables por el piso



Fuente: Data center del EsSalud

2.2.2 Las Tecnologías de Información y Comunicación

Definición:

Son aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y alas tecnologías afines aplicadas a la toma de decisiones (13).

Conjunto de conocimiento y aplicaciones prácticas que permiten la "adquisición, producción, almacenamiento, tratamiento, transmisión registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Las TIC incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual" (14).

En los últimos años se ha dado un paso hacia delante y se van incluidos aquellas tecnologías que tienen como fin difundir o comunicar esta información y compartir conocimiento, así, ahora se habla de Tecnologías de la Información y de las Comunicaciones. Este resultado ampliado conocido como TICS es la denominación genérica que abarca las Tecnologías de la Información, las actividades de equipos y servicios de comunicaciones y las personas. El creciente uso de este acrónimo es Una medida del acelerado fenómeno de convergencia entre información y comunicaciones.

Las TIC, como herramienta que son, permiten realizar básicamente tres funciones.

- Obtener m información en mucho menos tiempo e incluso obtener información que no sería posible obtener de otra manera.
- Procesar información de una manera más creativa, completa rápida y confiable.
- Comunicarnos con más personas más efectivas y eficientemente.

Áreas de aplicación de las TIC

Las TIC se aplican en las siguientes áreas de una empresa.

- **Administrativa:** Contable, financiera procedimientos, ERP.
- **Procesos productivos:** CAD, CAM, entrega de productos.
- **Relaciones externas:** Mercado y CRM, proveedores SChM, aliados confidencialidad.
- **Control y evaluación gerencial:** Sistemas de información y MIS, gestión de calidad, formación del equipo humano.

Beneficios de las TIC

Desde el punto de vista empresarial, las TIC pueden aportar beneficios estratégicos que son críticos para las organizaciones, Las TIC pueden:

- Establecer barreras de entrada.
- Afectan los costes de cambio.
- Permiten la diferenciación de productos y servicios.
- Limitan el acceso a los canales de distribución.
- Aseguran una política de precios competitivos.
- Reducen los costes de los proveedores y facilitan su tarea.
- Usan la información como un producto en sí mismo.
- Crean una relación más estrecha entre proveedores y clientes.

Por lo que respecta a Internet y al World Wide Web, su expansión supone una gran ventaja para las organizaciones virtuales, que desean usar esta tecnología. La conectividad y la estandarización, entre otras, son características que hacen de este medio un instrumento poderoso a la hora de crear organizaciones virtuales, desde un punto de vista funcional aportan: (15).

- Rentabilidad: al reducir los costes de la instalación de un sistema en red, al tratarse de una tecnología de fácil acceso.
- Estandarización: que permite a estructuras virtuales usar hardware y software heterogéneos, para comunicar e intercambiar datos de forma homogénea.

- Uso amigable: porque, como tecnología poderosamente intuitiva, minimiza la necesidad de formación.
- Potencial multimedia: ya que el multimedia se vuelve un soporte de las interfaces interactivas, que refuerzan la eficiencia del intercambio de información.
- Capacidad de actualización: ya que Internet facilita adaptar los contenidos o ajustar los sistemas a unas infraestructuras determinadas.
- Aspectos de seguridad: garantiza cada vez mejor la solvencia de las transacciones y el intercambio de información confidencial, aunque este siga siendo, quizás uno de los puntos débiles más destacables de este medio.
- Eficiencia del sistema: al garantizar el intercambio de información en tiempo real, y reforzar el trabajo interactivo en grupo, mediante el uso de herramientas de trabajo en grupo conocidas como "GroupWare".
- Almacenamiento de informaciones competidas: al permitir el acceso a información relevante sin que exista dependencia del lugar físico donde se guarda dicha información, lo que resulta esencial e imprescindible para el trabajo virtual.

Principales TIC utilizadas en las organizaciones

Las principales tecnologías de la información y comunicaciones que utiliza una empresa son: Internet, comercio electrónico, telecomunicaciones básicas, aplicación de las TIC en la industria.

a) Internet

Es un medio de comunicación global, que permite el intercambio de información entre los usuarios conectados a la red y que conecta a unos 8 millones de servidores encargados de servicios de información y de todas las operaciones de comunicación y de retransmisión; llega hasta unos 250 millones de usuarios en más de 100 países. Internet ofrece una oportunidad única, especial y decisiva a organizaciones de cualquier tamaño (16).

b) Comercio Electrónico

El comercio electrónico incluye actividades muy diversas coma el intercambio de bienes y servicios, el suministro online de contenido digital, la transferencia electrónica de fondos, las compras públicas, los servicios postventa actividades de promoción y publicidad de productos y servicios, campañas de Imagen de las organizaciones, marketing en general, facilitación de los contactos entre los agentes de comercio, seguimiento e investigaci6n de mercados, concursos electrónicos y soporte para la compartici6n de negocios.

c) **Telecomunicaciones Básicas**

Las telecomunicaciones básicas incluyen todos los servicios de telecomunicaciones, tanto públicos como privados, que suponen la transmisión de extremo a extremo de la información facilitada por los clientes.

La prestación de los servicios de telecomunicaciones básicas se realiza mediante el suministro transfronterizo y el establecimiento de empresas extranjeras o de una presencia comercial, incluida la posibilidad de ser propietario y explotar la infraestructura independiente de redes de telecomunicaciones. Ejemplos de servicios de telecomunicaciones básicas:

1. Servicios de teléfono.
2. Servicios de transmisión de datos con conmutación de paquetes.
3. Servicios de transmisión de datos con conmutación de circuitos.
4. Servicios de télex.
5. Servicios de telégrafo.
6. Servicios de facsímil.
7. Servicios de circuitos privados arrendados.
8. Otros servicios:
    - Servicios analógicos/digitales de telefonía móvil/celular.
    - Servicios móviles de transmisión de datos.
    - Servicios de radio búsqueda.
    - Servicios de comunicación personal.

- Servicios móviles por satélite (incluidos, por ejemplo, telefonía, datos, radio búsqueda y/o servicios de comunicación personal).
- Servicios fijos por satélite.
- Servicios de terminales de muy pequeña abertura.
- Servicios de estación terrestre de acceso.
- Servicios de teleconferencia.
- Servicios de transmisión de vídeo.
- Servicios de radiotelefonía con concentración de enlaces.

d) Aplicaciones de las TIC en la Industria

En los últimos años se ha producido una rápida expansión y evolución de la tecnología de los sistemas de información para empresas. Sin embargo, el estado de los sistemas informáticos de las organizaciones no ha evolucionado con Sus necesidades. La mayor parte de empresas tienen programas insuficientes, con características tecnológicas atrasadas y no hacen sino automatizar algunas de las funciones bicas de la organización. Los cambios producidos por el boom de las nuevas tecnologías van obligado amuchas empresas a tomar decisiones para adaptarse a estos cambios.

Existen diversas soluciones que se podrán aplicar en función de las necesidades concretas de cada caso: redes locales, trabajo colaborativo, ingeniería (CAD, CAM), gestión y producción (ERP), clientes y comunicación (CRM), etc.

e) **Gestión de innovación**

La Innovación Tecnológica constituye una estrategia clave dirigida al desarrollo de nuevos procesos y productos, mediante la generación, transferencia incorporación y adaptación de tecnologías. La Innovación es producto de la creatividad y del empleo eficaz de las herramientas de ciencia y tecnología, sin embargo, también requiere Una organización y gestión de los Sistemas de Innovación en la Empresa.

Habrá que tener en cuenta los criterios consideraciones para realizar una correcta planificación estratégica de la Innovación, cómo gestionar el conocimiento y que metodología seguir para realizar una vigilancia tecnológica que permita a la Empresa mantenerse al día en cuanto a las últimas tecnologías.

2.2.3 Data Center

2.2.3.1 Concepto

Conocido también como un centro de datos o centro de procesamiento de datos, se define como un área donde se alojan los equipos que procesan datos con una infraestructura eficiente para que asegure el funcionamiento óptimo de estos, de esta forma garantiza que la información se encuentre segura y disponible.

El estándar TIA 942 concebido como una guía para los diseñadores e instaladores de centro de datos, provee los lineamientos tomando en cuenta cuatro sub sistemas, telecomunicaciones, arquitectura, sistema eléctrico y sistema mecánico.

TIER denominación del nivel de fiabilidad de un centro de datos, indicando por uno de los cuatro niveles de fiabilidad llamados TIER, en función de su redundancia, a mayor número de TIER, mayor disponibilidad y por tanto mayores costes de construcción.

TIER	% Disponibilidad	% de parada	Tiempo de parada por año
Tier I	99.671%	0.329%	28.82 horas
Tier II	99.741%	0.251%	22.68 horas
Tier III	99.982%	0.018%	1.57 horas
Tier IV	99.995%	0.005%	52.56 minutos

Tabla Nro 01: Niveles de TIER (17)

2.2.3.2 Clasificación

2.2.3.2.1 Por el tipo de servicio

Data center de internet: Construido por empresas para proveer a sus clientes tanto servicios de internet como servicios de datos (housing y hosting) quien abarca gran parte del mercado de las telecomunicaciones.

Data center corporativo: Son construidos para proveer servicio de datos a una sola empresa, quien permite la interconexión entre los diferentes servidores internos de una organización hacia la WLAN e internet.

2.2.3.2.2 Por los niveles de redundancia

Está determinada por el Uptime Institute (18) y depende de la disponibilidad y redundancia que posee una data center, se definen por 4 niveles de TIER:

TIER I: Infraestructura básica

Usados en empresas pequeñas, no posee redundancia en ningún de sus componentes por lo que es susceptible a interrupciones de los servicios en el caso de existir alguna falla en sus elementos.

TIER II: Infraestructura con dispositivos redundantes

Posee elementos redundantes, usualmente en aspectos eléctricos y de refrigeración, que lo hace menos susceptible a interrupciones en comparación al nivel I, tiene una sola ruta de distribución eléctrica, el piso y el uso de UPS es un requerimiento para su alimentación.

TIER III: Infraestructura concurrente mantenible

Además de contar con redundancia en sus componentes, posee dos rutas de alimentación eléctrica y de enfriamiento de las cuales una está activa, todos los equipos de telecomunicaciones deben tener fuentes de alimentación redundantes esto permite realizar mantenimiento sin interrupciones de los servicios. Se establece el control de acceso mediante uso de lector de tarjeta o la identificación biométrica con el tiempo estimado de fallas de 105 minutos al año.

TIER IV: Infraestructura tolerante a fallos

Data center con sistemas independientes con múltiples componentes redundantes y rutas de distribución que están activas siempre. Tiene resguardo contra desastres naturales como sismos, huracanes o inundaciones. Funcionamiento de alarmas de incendios, extinción de incendios o las características de apagado de emergencia puede causar una interrupción de aproximadamente 52.56 minutos anuales.

Ilustración Nro 07: Mapa de Certificaciones registrados por Uptime Institute

Uptime Institute Tier Certification Map

Country: Peru

Company	Data Center Name	Data Center Location	Tier Certification
GMD S.A.	GMD Cloud Data Center, Phase 1	Lima, Peru	• Tier III Certification of Constructed Facility • Tier III Certification of Design Documents
BBVA Continental Lima	Peru CPD	Lima, Peru	• Tier III Certification of Constructed Facility • Tier III Certification of Design Documents
Telefónica del Perú	Data Center Monterrico	Lima, Peru	• Tier III Certification of Design Documents

Fuente: Uptime Institute

En la imagen anterior se muestra los países en las cuales los datas center han sido certificados, se puede notar que en Europa existe más certificaciones a diferencia de latino américa concretamente en el Perú 4 centros de datos tienen la certificación TIER III.

2.2.4. Estándares ANSI/TIA/EIA-942 Infraestructura De Telecomunicaciones Para Data Centers.

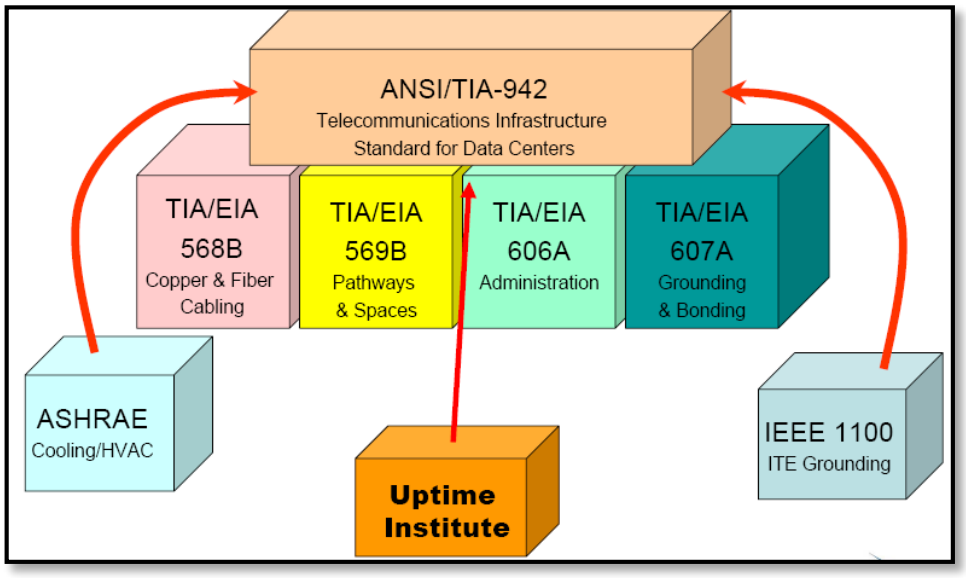
2.2.4.1. Descripción

ANSI/TIA/EIA-942 desarrollado por la Asociación de la Industria de Telecomunicaciones (TIA), tiene como alcance definir una guía de diseño para Infraestructuras TI (Tecnologías de la Información) que garantice: seguridad operacional, continuidad del servicio, disponibilidad y solidez.

El estándar especifica los requerimientos mínimos para la infraestructura de telecomunicaciones de Data Centers y cuartos de cómputo incluyendo Data Centers

empresariales de único inquilino y Data Centers de "hosting" de Internet multi-inquilinos, además está basado en el *Uptime Institute* y contiene algunas recomendaciones Eléctricas, Mecánicas, Telecomunicaciones y Arquitectónicas.

Ilustración Nro 08: Bloques de construcción de un Data center



Fuente: Peñaloza Figueroa M. Standard TIA-942 (19)

Propósito de la Norma

El propósito de esta norma es proporcionar requisitos y directrices para el diseño y la instalación de un centro de datos o sala de ordenadores. Está diseñado para ser utilizado por los diseñadores que necesitan un conocimiento global del diseño del centro de datos, incluyendo la planificación de las instalaciones, el sistema de cableado, y el diseño de la red. La norma permitirá el diseño de centros de datos para ser considerado temprano en el proceso de desarrollo de la construcción, lo que contribuye a las consideraciones arquitectónicas, al proporcionar información que corta a través de los esfuerzos de diseño multidisciplinar; promover la cooperación en las fases de diseño y construcción. La planificación adecuada durante la construcción o renovación es significativamente menos costosa y menos perjudicial que después de la instalación está en funcionamiento. Los centros de datos en particular, pueden beneficiarse de la infraestructura que se planifica con antelación para apoyar el crecimiento y los cambios en los sistemas informáticos que los centros de datos están diseñados para soportar. (20)

Definición de términos

Las definiciones genéricas en este apartado se han formulado para ser utilizado por toda la familia de estándares de infraestructura de telecomunicaciones. Los requisitos específicos se encuentran en las cláusulas normativas de la presente norma. A los efectos de esta norma, se aplican las siguientes definiciones. (20)

Piso de acceso: Un sistema que consiste en paneles de piso completamente desmontables e intercambiables que se apoya sobre pedestales o largueros (o ambos) ajustables para permitir el acceso a la zona de debajo.

Proveedor de acceso: El operador de cualquier instalación que se utiliza para transmitir señales de telecomunicaciones hacia y desde un local del cliente.

Administración: El método para el etiquetado, identificación, documentación y el uso necesario para implementar movimientos, adiciones y cambios en la infraestructura de telecomunicaciones.

Columna vertebral:

1) Una instalación (por ejemplo, vía, por cable o conductores) entre cualquiera de los siguientes espacios: salas de telecomunicaciones, salas comunes de telecomunicaciones, terminales de baja y sirve, instalaciones de entrada, salas de equipos y salas de equipos comunes.

2) en un centro de datos, una instalación (por ejemplo, vía, por cable o conductores) entre cualquiera de los siguientes espacios: salas de ingreso o espacios, las principales áreas de distribución, áreas de distribución horizontal, salas de telecomunicaciones.

Unión: La unión permanente de las piezas metálicas para formar una trayectoria eléctricamente conductora que asegure la continuidad eléctrica y la capacidad para conducir con seguridad cualquier corriente probable que se impongan.

Gabinete: Los recipientes que pueden incluir dispositivos de conexión, terminaciones, aparatos, cableado y equipos.

Gabinete (telecomunicaciones): Un recinto con una tapa abatible utilizado para la terminación de los cables de telecomunicaciones, cables y dispositivos de conexión.

Cable: Un conjunto de uno o más conductores aislados o fibras ópticas, dentro de una funda envolvente.

Cableado: Una combinación de todos los cables, los puentes, cables y hardware de conexión.

Cableado centralizado: Una configuración de cableado del área de trabajo a una conexión cruzada centralizada utilizando tirón a través de cables, una interconexión o empalme en la sala de telecomunicaciones.

Canal: El camino de transmisión de extremo a extremo entre dos puntos en los que se conecta un equipo específico de la aplicación.

Sala de equipos comunes (telecomunicaciones): Un espacio cerrado para aparatos e interconexiones de red troncal para más de un inquilino en un edificio o campus.

S**ala de ordenadores**: Un espacio arquitectónico cuya función principal es dar cabida a los datos de los equipos de procesamiento.

Conducto:

(1) Una pista de rodadura de sección transversal circular.

(2) Una estructura que contiene uno o más conductos.

Hardware de conexión: Un dispositivo que proporciona terminaciones de cables mecánicos.

Punto de consolidación: Un lugar para la interconexión entre cables horizontales que se extienden desde la construcción de vías y cables horizontales que se extienden en vías de muebles.

Cruzar conectar: Una instalación que permite la terminación de los elementos del cable y su interconexión o conexión cruzada.

Conexión cruzada: Un esquema de conexión entre el cableado corre, subsistemas y equipos que utilizan cables de conexión o jumpers que se adhieren a la conexión de hardware en cada extremo.

Centro de datos: un edificio o parte de un edificio cuya función principal es para

albergar una sala de ordenadores y sus áreas de apoyo.

Punto de demarcación: Un punto donde el control o la propiedad cambios operativos.

Interferencia electromagnética: Radiada o conducida energía electromagnética que tiene un efecto indeseable sobre el equipo o señal transmisiones electrónicas.

Habitación o espacio de entrada (de telecomunicaciones): Un espacio en el que se unen las instalaciones de red troncal de telecomunicaciones de construcción inter o intra lleva a cabo.

Cable de equipo; cable: Un conjunto de cable o cable utilizado para conectar equipos de telecomunicaciones para el cableado horizontal o columna vertebral.

Equipos área de distribución: el espacio de la sala de ordenadores ocupado por los bastidores del equipo o armarios.

Sala de equipos (de telecomunicaciones): Un espacio centralizado de ambiente controlado para equipos de telecomunicaciones que normalmente alberga un principal o intermedia de conexión cruzada.

Suelo: Una conexión conductora, intencional o accidental, entre un circuito eléctrico (por ejemplo, las telecomunicaciones) o el equipo y la tierra, oa algún cuerpo conductor que sirva en lugar de la tierra.

Toma de tierra: El acto de la creación de una planta.

Conductor de tierra: Un conductor utilizado para conectar el electrodo de puesta a tierra a la barra de tierra principal del edificio.

Cableado horizontal:

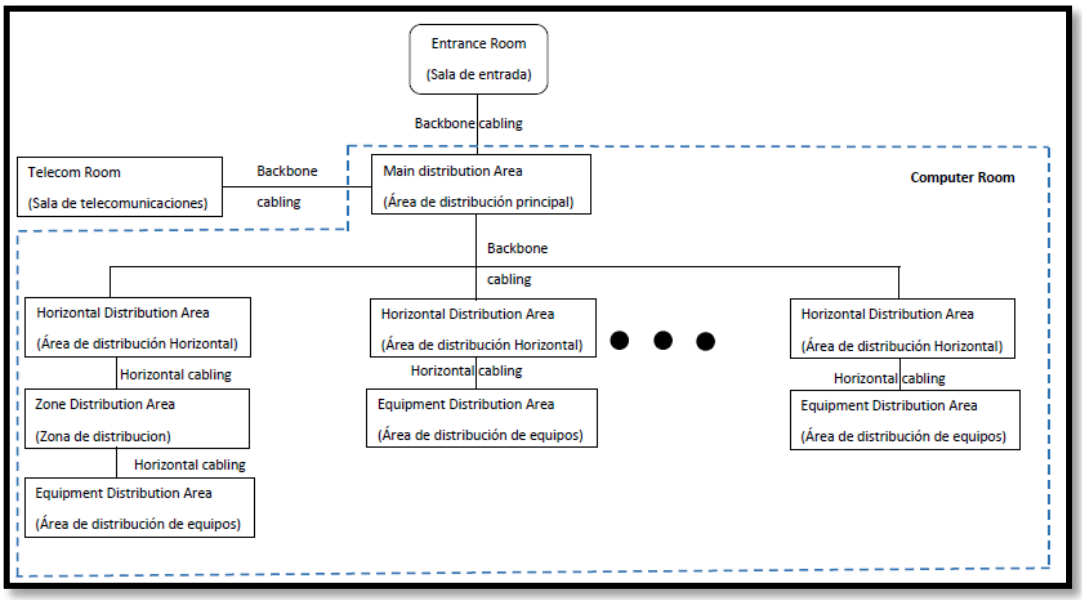
1) El cableado entre e incluyendo la toma / conector de telecomunicaciones y la conexión cruzada horizontal.
2) El cableado entre e incluyendo la salida del sistema de automatización del edificio o de la primera terminación mecánica de la conexión horizontal.

2.2.4.2 Áreas Funcionales De Un Data Center

La distribución de los equipos se alinea a las recomendaciones establecidas en la norma ANSI/TIA 942, distribuidas en áreas con el fin de separar las funciones de cada uno de los espacios que conforman un Data Center y de esta forma facilitar los posibles cambios que podrían suscitarse en cuanto a la ubicación de los equipos ahorrando tiempo y estudio o de reorganización de las áreas del centro de datos.

En la siguiente imagen se observa la forma en la que se encuentra relacionadas las áreas de un data center:

Ilustración Nro 09: Áreas Funcionales de un Centro de Datos



Fuente: Estandar ANSI/TIA/EIA 942 2012 (21)

a. Sala de entrada (Entrance Room)

Esta es la ubicación para el equipo proveedor de acceso y puntos de demarcación, así como la interfaz con los sistemas de cableado campus. La Entrada de la sala puede estar ubicado dentro o fuera de la sala de ordenadores, la parte del centro de datos que alberga el equipo de procesamiento de datos. La norma recomienda ubicar la sala de entrada exterior de la sala de informática para una mejor seguridad. Cuando se encuentra dentro de la sala de ordenadores, la Entrada de la sala debe consolidarse con

la MDA. Es posible que las distancias de cableado del proveedor pueden requerir múltiples habitaciones de entrada para los centros de datos más grandes. (22)

- Equipos portadores y de demarcación

b. Área de distribución principal (MDA)

Similar a un MDF, el MDA es una zona céntrica que alberga la conexión cruzada principal, así como routers centrales y conmutadores para infraestructuras LAN y SAN. La MDA puede incluir una conexión cruzada horizontal (HC) para un área de distribución de equipos cercanos. La norma requiere al menos un MDA y especifica la instalación de bastidores separados para fibra, UTP y cable coaxial en esta ubicación. (22)

- Routers
- Switches de backbone LAN/SAN
- PBX
- Muxes m13

c. Áreas de distribución horizontal (HDA)

Similar a un TR, la HDA sirve como punto de distribución para el cableado horizontal y casas conexiones cruzadas y equipos activos de distribución de cable en el área de distribución de equipos. Al igual que la MDA, la norma específica la instalación de bastidores separados para fibra, UTP y cable coaxial en esta ubicación. También recomienda ubicar los interruptores y paneles de conexión para reducir al mínimo las longitudes de cordón de parcheo y facilitar la gestión de cables. La HDA se limita a 2.000 conexiones, y el número de HDAS es dependiente de la cantidad de cableado y el tamaño total del centro de datos. (22)

- LAN
- SAN
- Switches KVM

d. Área Distribución Equipamientos (EDA)

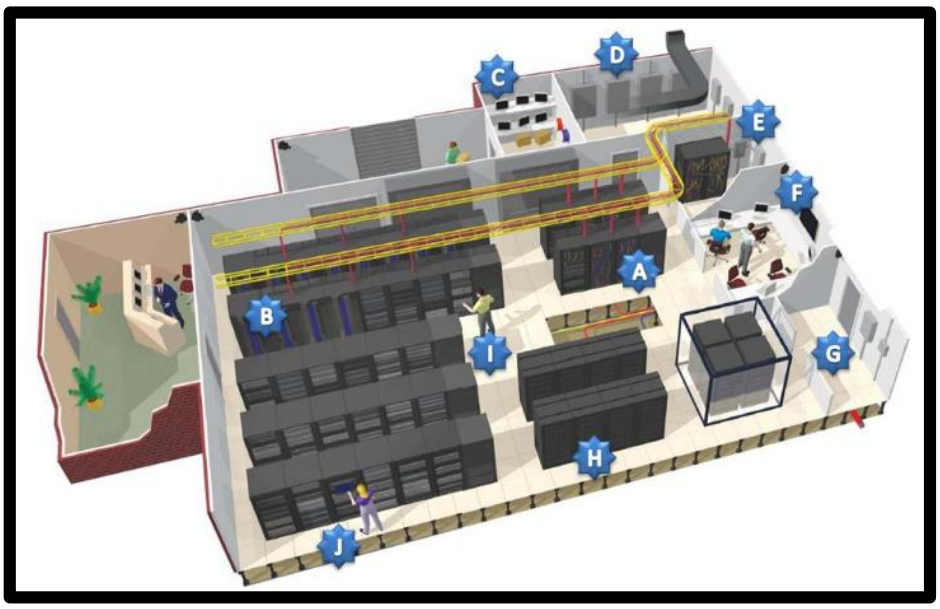
Cables horizontales son normalmente terminan con paneles de conexión en la EDA, la ubicación de armarios y bastidores de equipos. La norma específica la instalación de bastidores y gabinetes en un patrón alternativo para crear pasillos "calientes" y "fríos", una configuración que se disipa eficazmente el calor de la electrónica (ver Consideraciones ambientales para una discusión sobre el enfriamiento y pasillo caliente / pasillo frío de configuración). (22)

- Racks
- Gabinetes

e. Zona de Distribución (ZDA)

El ZDA es un punto de interconexión opcional en el cableado horizontal entre el HDA y EDA. El ZDA puede actuar como un punto de consolidación para la flexibilidad de reconfiguración o para equipo vivienda independiente como mainframes y servidores que no pueden aceptar paneles de conexión. Sólo una ZDA se permite dentro de un cableado horizontal ejecutar, con un máximo de 288 conexiones. El ZDA no puede contener-conexiones cruzadas o equipos activos. (22)

Ilustración Nro 010: Distribución de áreas de un centro de datos



Fuente: http://www.itadviser.com.mx/index-10.html

Distribución de las áreas según la imagen 10:

A: Área de Distribución Principal (MDA)

B: Área de Distribución Horizontal (HDA)

C: Cuarto de almacenamiento

D: Cuarto de Máquinas Eléctricas/Mecánicas

E: Cuarto de Telecomunicaciones

F: Centro de Operaciones y Soporte

G: Cuarto de Entrada de Servicios

H: Área de Distribución de Equipos (EDA)

I: Cuarto de Computadores

J: Área de Distribución Local (ZDA)

2.2.4.3 Subsistemas De Un Data Center

Para el diseño e implementación de un Data Center se deben tomar en cuenta varios aspectos que no simplemente tienes que ver con el número de equipos o el tamaño que este debe tener, por estas razones es conveniente segmentar en diferentes áreas para poderlas analizar y estudiar de forma más conveniente de modo que sea entendible y brinde una visión clara de lo que se pretende realizar.

Ilustración Nro 011: Ingeniería Única vs Componentes estandarizados

Fuente: Standardization and Modularity in Data Center Physical Infrastructure

Los subsistemas de un centro de datos según las especificaciones de la Norma TIA-942 para el diseño de un data center son:

2.2.4.3.1. Telecomunicaciones

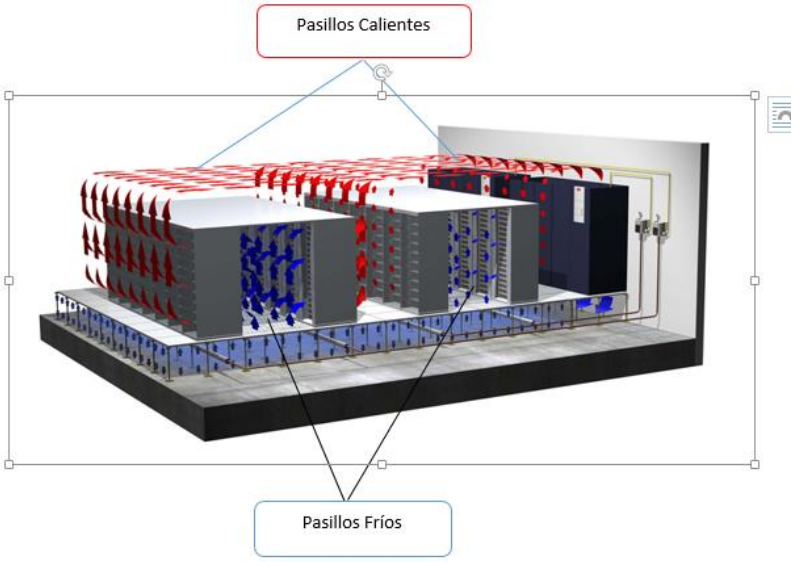
Subsistema donde se encuentra todas las áreas funcionales, así como las partes conformadas por el cable estructurado del centro de datos, cada una de estas áreas cumple con funciones ya definidas que aseguran una funcionabilidad óptima de toda la infraestructura.

a. Rack y Gabinete

Son conocidos como gabinetes, sirven para brindar alojamiento a los equipos de conectividad, están conformados por rieles, paneles laterales y frontales, debidamente protegidos.

- Controlar el cableado tanto horizontal como vertical.
- Limitar el pase establecido como el caso de radios de curvatura (Fibra óptica).
- Organizados uno al frente de otro dando paso a la creación de áreas calientes y áreas frías.
- Contar con ventiladores en la parte superior como inferior.

Ilustración Nro 012: Pasillos Fríos y Calientes de un Data Center



Fuente: http://www.socored.es/data-center-climatizacion.php

Pasillos Calientes: Se forman detrás de los racks y gabinetes, en este pasillo no se deberán ubicar placas perforadas porque se deberá evitar la mezcla del aire caliente

con el aire frio, debajo de este espacio deberá ser instalado el cableado de telecomunicaciones según las recomendaciones del estándar.

Pasillos Fríos: Ubicados al frente a los gabinetes contara con placas perforadas logrando que el aire frio llegue a los equipos de conectividad, este aire una vez que ha pasado por los diferentes dispositivos será expulsado por la parte trasera hacia el pasillo caliente, en este sitio a su vez se instalar los cables de energía eléctrica bajo el piso falso.

Consideraciones que se deben tener según TIA-942:

Los racks que son compatibles con el piso de acceso serán atornillados a la losa de cemento o a un canal de metal asegurado a la losa, mediante varillas roscadas que se penetran a través de las baldosas.

Se debe dejar un mínimo de 1 m de espacio delantero para la instalación de los equipos o un espacio delantero de 1,2 m para acomodar equipos más profundos, un mínimo de 0,6 m de espacio posterior para facilitar el acceso de servicio en la parte de atrás de gabinetes y racks.

Los gabinetes serán seleccionados para proporcionar una ventilación adecuada para los equipos que alojará, para lo cual usará: ventiladores para la circulación del aire y el flujo de aire natural entre pasillos calientes y fríos que entra a través de las aberturas de ventilación en la parte delantera y las puertas traseras de los gabinetes.

La altura máxima de gabinetes y racks será de 2,4 m; de preferencia no deben ser más altos de 2,1 m para un acceso más fácil de los equipos instalados en la parte superior.

Los gabinetes deben tener una profundidad suficiente para acomodar el equipo previsto, incluido el cableado en la parte delantera y/o trasera, cables de alimentación, equipos de gestión de cables y enchufes.

La configuración habitual de tomas de corriente en los gabinetes indica que por los menos debe existir una regleta de 20 A, 220 V.

El cuarto de entrada, el área de distribución principal y las áreas de distribución horizontal, deben utilizar racks de 480 mm para patch panels y equipos; además se

instalarán administradores verticales de cable entre cada par de gabinetes y en ambos extremos de cada fila de gabinetes; no deberán ser inferiores a 83 mm de ancho.

Los proveedores de servicios pueden instalar sus propios equipos en el cuarto de entrada, ya sean en gabinetes de 585 mm o gabinetes propietarios.

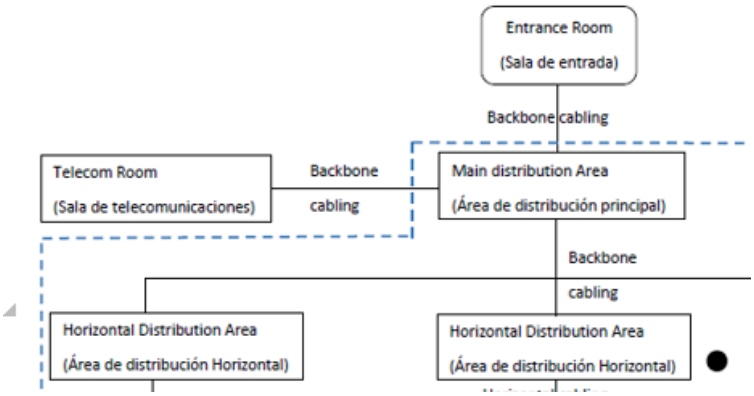
Cuando se instalan racks individuales, los administradores verticales de cable deben tener por lo menos 150 mm de ancho. Cuando se instala una fila de dos o más gabinetes, se debe considerar la posibilidad de poner administradores verticales de cable de 250 mm de ancho entre gabinetes y administradores verticales de cable de 150 mm de ancho en ambos extremos de la fila. Los administradores de cable deben extenderse desde la parte superior de los racks hasta el piso.

b. Backbone

Es un sistema primario de conectividad el cual permite la conexión de las áreas de distribución tanto principal (MDA) como horizontal (HDA) con las instalaciones de entrada de servicios.

En el Backbone pueden ser instalados cables de fibra óptica o de cobre. Es importante considerar la elección de un cable que soporte a nuevas tecnologías y servicios futuros y no solamente atender la demanda actual de la red. (23)

Ilustración Nro 013: Cableado Backbone



Fuente: ANSI/TIA/EIA-942

Cables de Cobre:

La norma indica para el uso de cables de cobre, la Categoría 6 o superior. Debe soportar tasas de transmisión de 1Gbps/10Gbps para distancias de hasta 100 metros.

Para soporte a tasas de 10Gbps o superiores es recomendado la utilización de cableado blindado (F/UTP), pues las interferencias electromagnéticas, que son puntos de entrada para errores y pérdidas de bits en altas velocidades de transmisión son eliminadas con el blindaje.

La nueva categoría de cableado en cobre, denominada Categoría 6A, tiene un mejor desempeño para transmisiones a 10Gbps en 100 metros.

Características	Categoría			
	6		6A	
	U/UTP	F/UTP	U/UTP	F/UTP
Banda (Mhz)	250	250	500	500
Distancia máxima para el Backbone (m)	100	100	100	100
Velocidad de Transmisión Garantizada para 100 metros	1 Gbps 10Gbps(*)	1 Gbps 10Gbps(*)	10Gbps	10Gbps
Peso (Kg/Km)	42	53	60	57
Diámetro nominal (mm)	6,2	7,5	8,8	8,1

Tabla Nro 02: Diferencias entre las tecnologías para cableado de cobre (23)

El uso de cables Categoría 5e no es recomendado para un Data Center pues es una tecnología antigua y su tasa de transmisión es más limitada.

Cable Fibra:

Pueden ser monomodo o multimodo. Para la utilización de fibras multimodo, la norma ANSI/TIA 942 indica el uso de cables con fibras optimizadas a laser tipo MM 50µm OM3 (ISO/IEC 11.801), pues este tipo de fibra tiene características de atenuación y desempeño superiores que las fibras convencionales soportando enlaces de hasta 550 metros con tasas de transmisión de 10Gb.

Características	OM2 MM(50.0)	OM1 MM(62.5)	OM3 MM(50.0)
Distancia máxima para el Backbone 10Gbps (m)*	82	33	550
Distancia máxima para el Backbone 1Gbps (m)*	550	275	1040

Tabla Nro 03: Comportamiento de las fibras frente a las tareas de transmisión de 1 y 10gbps (23)

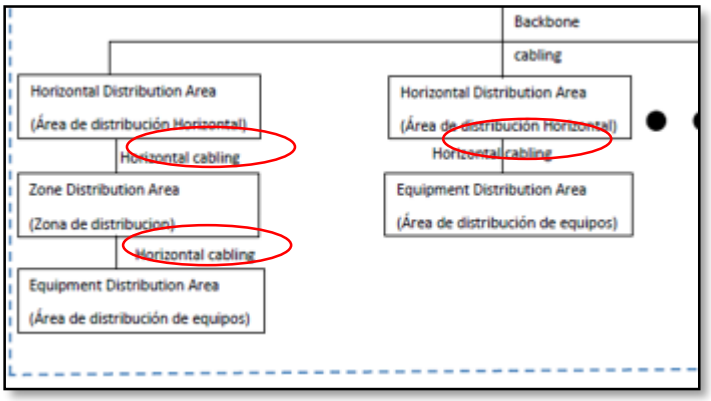
Para la elección del cableado en el Data Center se debe tomar en cuenta:

- La flexibilidad con respecto a los servicios soportados.
- Requisitos de vida útil del cableado.
- Instalación / tamaño del sitio y número de personal.
- La capacidad del canal en el sistema de cableado.
- Recomendaciones del fabricante o especificaciones de los equipos.

c. Cableado Horizontal (24)

La distribución horizontal es la parte del cableado de telecomunicaciones que conecta las áreas de trabajo con los distribuidores o repartidores horizontales, ubicados en el Armario o Sala de Telecomunicaciones.

Ilustración Nro 14: Cableado Horizontal en un Centro de Datos



La distribución horizontal incluye:

- Cables de distribución horizontal
- Conectores de telecomunicaciones en las áreas de trabajo (dónde son terminados los cables de distribución horizontal)
- Terminaciones mecánicas de los cables horizontales
- Cordones de interconexión ("Patch-cords") en el Armario o Sala de Telecomunicaciones.
- Puede incluir también "Puntos de Consolidación"
- La distancia máxima para el cable de distribución horizontal es de 90 m, medida en el recorrido del cable, desde el conector de telecomunicaciones en el área de trabajo hasta el panel de interconexión en el armario de telecomunicaciones.
- Los cordones de interconexión ("patch-cords") utilizados en las áreas de trabajo y en el armario de telecomunicaciones no deben ser más largos que 10 m en conjunto (completando una distancia de 100 m de "punta a punta". Se recomienda que los cordones de interconexión en cada extremo no superen los 5 m
- Los cables reconocidos para la distribución horizontal son:
- UTP o STP de 100 y cuatro pares
- Fibra óptica multimodo de 50/125 μm
- Fibra óptica multimodo de 62.5/125 μm

Tipo de Tecnología	Enlace Completo	Distancia Horizontal
Fibra Óptica	300 metros	-
Cobre	100 metros	90 metros

Tabla Nro 04: Distancias máximas permitidas (23)

d. Patch Panel

Son elementos que se encargan de recibir todas las conexiones provenientes de los diferentes equipos de conectividad, sirviendo a la vez como organizadores del cableado estructurado y protegiendo a los puertos de los equipos de fallos producidos por la mala conexión que pudiese darse.

- Apoyar la gestión de capa física,

- LEDs (diodos emisores de luz) para cada puerto.
- Tiene sensores para la gestión individual de los puertos.
- Proporciona el monitoreo on-line de la conectividad.
- Detección de rotura del patch cord.
- Se suministra descargado sin los keystone jacks.
- Tiene etiquetas individuales para identificar los puertos.
- No necesita alimentación CA (corriente alterna).

e. Patch Cord

Son cables que se utilizan para la conexión de dispositivos en redes o comunicaciones electrónicas, sus extremos terminan con conectores RJ-45 que contienen internamente cables más pequeños, estos patch cord están estructurados mediante cables UTP la categoría dependerá del uso que se le vaya a dar al cable.

La longitud típica de estos cables según lo especifica la norma para su uso en los Data Center es de 5 m, cabe mencionarse que los patch cord son generalmente pequeños ya que su uso es para trabajar dentro de los racks.

e. Componentes Redundantes

Los dispositivos redundantes dependen de tipo de TIER a implementar, en el diseño de un Data Center Tier II, se debe contar con los siguientes dispositivos redundantes: UPS, y generadores eléctricos según lo establece la Norma ANSI/EIA-942.

2.2.4.3.2. Arquitectura

En la parte arquitectónica la norma establece varios parámetros para de esta forma dar una utilización adecuada a cada una de las áreas, además de una optimización del espacio en el cual se establecerá el Centro de Datos.

a. Selección del Sitio

La decisión de donde estará ubicado el Data Center depende de varios factores los cuales se encuentran relacionados con aspectos de seguridad que cuente este espacio, condiciones climáticas para mantener estables los dispositivos de conectividad.

El tamaño no se especifica dentro del estándar ANSI/EIA-942, sin embargo, para su diseño se deben de tomar en consideración:

- Dispositivos de telecomunicaciones (servidores de red, centrales telefónicas, elementos de comunicaciones para voz, datos y video, etc.)
- Espacio mínimo recomendado es de 13.5m2, varia en base al número de quipos.

b. Tipo de Construcción

El Data Center deberá ser un lugar cerrado para evitar o reducir el polvo que podría producirse en el ambiente, por lo cual se recomienda el sellado de todos los espacios como pisos, paredes y techos; se recomienda también debido a que se cuenta con un espacio cerrado el uso de colores claros en sus paredes para lograr una adecuada reflexión de la luz evitando que el área se torne obscura.

c. Techos y Pisos

En el diseño del Data Center se debe tener en consideración características para el techo como para el piso, por ejemplo, la norma establece que la altura mínima para el Centro de Datos es de 2,6 m desde el piso a cualquier tipo de obstrucción tales como cámaras, aspersores o lámparas, existiendo un mínimo de 0.46 m de altura libre para la ubicación de los aspersores de agua.

El Data Center debe contar con un piso falso que brinde consistencia y soporte para el montaje de toda la infraestructura y en donde la carga mínima a soportar es de 7.2 kPa, este piso se construye con materiales antiestáticos, se hace uso de placas perforadas para brindar ventilación a los equipos, estas placas solo se colocarán en los lugares donde sea necesario flujo de aire frío para los equipos y se encontrarán separadas de los sistemas de aire acondicionado al menos 2 m de distancia.

La altura que tendrá el piso falso depende del tamaño del sitio, las densidades de calor que circulan en este espacio y el sistema de aire acondicionado con el que se cuenta. Para un nivel II la norma establece una altura de 450 mm y para el caso de las bandejas

como medio de enrutamiento del cableado estas se ubicarán a una distancia de 150 mm por debajo de los paneles que conforman el piso falso.

d. Sala de Generadores y UPS

Un Data Center debe contar con un sistema de generación de energía independiente, aunque de ser necesario o debido al espacio físico con el que se cuente la norma establece que se puede hacer uso del generador del edificio.

También es necesario el uso de estabilizadores de energía para garantizar el correcto funcionamiento de los equipos, estas UPS deberán ser localizadas dentro del Centro de Datos en un espacio que no cause daños a la infraestructura y que mantenga una distancia de aproximadamente 1m entre los gabinetes de los equipos.

e. Controles de Acceso

Es necesario dotar al Centro de Datos de la seguridad acorde a su importancia ya que de ella dependerá que personal no autorizado o capacitado ingrese a realizar maniobras en los equipos, lo que pudiese ocasionar fallas en el sistema; por lo cual se recomienda instalar puertas de seguridad en el acceso a este espacio, contando además con sistemas de video vigilancia (esto último no lo especifica la norma para un Tier II) que brindarían mayor seguridad o mediante la utilización de accesos biométricos para guardar un listados del personal que tuvo acceso a esta área.

La puerta de acceso hacia el Data Center debe estar protegida contra robo, se recomienda que sea estructurada con planchas de acero, refuerzos en su parte interna, cerraduras electromagnéticas, resistencia al calor de por lo menos 1000 ˚F por hora, bisagras de alta resistencia al peso y a la fricción que puede darse; esta puerta deberá contar con un tamaño aproximado de 1.20m x 2.20m, con una ventana de seguridad (mirilla) de 0.30m x 0.30m aproximados, adicionalmente se puede agregar una barra cierra puerta y una barra antipático.

2.2.4.3.3. Eléctrica

Este es uno de los aspectos fundamentales a ser tomados en consideración en el diseño de toda infraestructura sea o no de telecomunicaciones, puesto que depende de este subsistema el correcto funcionamiento de los equipos de conectividad.

Su diseño requiere de un correcto estudio por parte de personal capacitado para que no existan daños que podrían terminar con la vida útil de los equipos que en algunos casos son demasiado costosos y pueden generar pérdidas significativas a la empresa, por esta razón es conveniente tomar en cuenta las recomendaciones de la norma como son: Cantidad de accesos, puntos únicos de falla, redundancia de UPS, sistemas de puesta a tierra, generadores, sistemas de monitoreo entre otros, evitando perjuicios que pueden dejar inoperable al Centro de Datos.

a. Entrada de Servicios

La cantidad de accesos depende del nivel de Tier a implementar, para el diseño que se lleva acabo se toma en consideración que se trata de un Data Center Tier II, lo cual indica que contará con una sola línea de distribución eléctrica según los requerimientos especificados en la norma.

Este cuarto generalmente se encuentra ubicado en el subterráneo o sótano del edificio, el mismo que debe estar localizado en un área seca, distante de espacios que puedan generar fugas de aguas, así como también en este sitio no se podrá ubicar dispositivos ajenos a la entrada de servicios.

b. Luminarias

El espacio en el cual se instalará el Data Center debe estar provisto por una correcta iluminación que ayude a garantizar visibilidad con el mayor ahorro de energía posible, el estándar establece que el Data Center debe contar con una iluminación mínima de 500 lux horizontalmente y 200 lux verticalmente, estas condiciones tomando como referencia 1 m por encima del piso falso.

c. Redundancias de UPS

Las UPS entran en funcionamiento cuando se ha producido algún fallo en el sistema eléctrico (alzas o bajas de voltaje) protegiendo a que la operatividad de los equipos se mantenga sin alteraciones, están conformadas por estabilizadores de tensión y baterías internas que dan respaldo a los equipos en interrupciones eléctricas hasta que el generador se encuentre funcionando o hasta que retorne el suministro eléctrico. Las UPS deben contar con una capacidad suficiente para brindar soporte a los equipos, esta capacidad depende del número de dispositivos que conformen el Data Center.

En un Tier II debe existir redundancia en este tipo de elementos por lo que se necesitará de dos sistemas de UPS independientes, que estén activas simultáneamente, cada uno de estos módulos será provisto por un medio de aislamiento individual que no afecte a la operación de cada uno de ellos o de su redundancia.

d. Generadores

Es recomendable que se cuente con un generador adicional para brindar soporte al Data Center en situaciones en la cuales por fallas podrían perder la conexión con el proveedor de servicio eléctrico, cabe mencionarse que se puede hacer uso del generador con el cual cuente el edificio, estos generadores deberán ser alimentados por biocombustibles ya sea diésel o gas y deberán proveer de energía a las UPS para mantenerlas activas en caso de existir alguna falla.

e. Puesta a Tierra

Este sistema garantiza una vía directa de descarga hacia la tierra, evitando que los equipos sean afectados por daños ocasionados debido a las variaciones de voltaje maximizando el tiempo de vida útil de los equipos que conforman la red; el sistema de puesta a tierra varía en base al número de dispositivos que deba proteger, pudiendo ser tan simple como una varilla metálica enterrada en el suelo de un edificio, como también un sistema estructurado que cumpla con recomendaciones para dar protección a cuartos de telecomunicaciones, salas de equipos o centros de datos.

Cabe mencionarse que los sistemas de conexión a tierra deberán ser verificables visualmente, puesto que el uso incorrecto de los elementos podría aumentar la degradación con el vínculo eléctrico que se generan al existir diferencias de potencial entre los componentes estructurales del Data Center lo que ocasionaría riesgos potenciales en la seguridad.

La puesta a tierra de un Data Center busca proporcionar una trayectoria de baja impedancia que brinde protección a los dispositivos contra sobre-corriente, así como también evite que potenciales altamente peligrosos de las estructuras metálicas alcancen al ser humano, entre estas recomendaciones podemos mencionar:

- El neutro y el conductor para la puesta a tierra solo se podrá conectar en un único punto denominado de referencia cero, el cual se encuentra ubicado

generalmente en la acometida de energía del edificio o la salida de un sistema derivado.

- El tipo de electrodo a utilizarse dependerá de las características del suelo.
- Se debe evitar utilizar las estructuras de los edificios que no hayan sido diseñadas para este tipo de funciones.
- Los electrodos pueden ser ubicados en diferentes configuraciones como delta, estrella, círculo, línea o con mallas.
- La impedancia para el electrodo a tierra no podrá superar el valor de 2 Ohms dentro de la banda de 0 a 1800 Hz, este valor puede cambiar si se utiliza circuitos derivados.
- El sistema se encuentra compuesto por una barra de tierra principal, una barra aislada y un conductor aislado para cada circuito derivado.

2.2.4.3.2. Mecánica

Este subsistema está estrechamente relacionado con la parte funcional del Centro de Datos, tiene como objetivos principales velar por los sistemas de temperatura o climatización, control de espacio, presión, niveles de cañerías y drenajes, sistemas para detección de incendios, detecciones de líquidos, y condensadores, rociadores o *sprinklers*, control para HVAC (*Heating, Ventilation, and Air Conditioning*), sistema de detección por aspiración entre otros.

a. Sistemas de Climatización

Los sistemas de aire acondicionado deben ser diseñados y proyectados para una operación continua de 7dias/24 horas/ 365 días del año, en el caso de un Tier II la norma específica que no es necesario que estos dispositivos cuenten con un sistema para el control de humedad por lo que solamente es necesario conocer exactamente la capacidad que debe tener este sistema de climatización, la misma que se puede determinar haciendo uso de la siguiente ecuación.

$$C=230*V + (\#PyE + 476)$$

Donde:

C = Capacidad del sistema de aire acondicionado.

230 = Factor Latinoamericano calculado a una temperatura máxima de 40 °C con unidades de BTU/hm^3

V = Volumen del área en el cual se instalará el aire acondicionado.

PyE = Representa el número de personas que se encontrarán en el lugar más el número de equipos que emitan calor y estén instalados en este sitio.

476 = Factor que representa las ganancias y las pérdidas que aportan las personas y los equipos eléctricos su unidad de medida está dada en BTU/h.

b. Sistemas para detección de incendios

Estos sistemas se los utiliza como medidas para proteger a los equipos y el espacio de alguna eventualidad de incendio que podría darse ocasionando daños en los equipos electrónicos.

El estándar recomienda que se instale un sistema detector de humo para brindar un mejor nivel de protección al Centro de Datos. Este sistema debe ser mucho más sensible que los sistemas tradicionales siguiendo las recomendaciones de la norma NFPA 75 la cual describe los lineamientos para la protección de los equipos de tecnologías de la Información.

2.2.4.4. Otras Definiciones

a. Rutas de Cableado

El cableado no será encaminado a través de espacios públicos a menos que esté encerrado en rutas seguras; cajas de paso, o cajas de empalme, las mismas que deberán ser cerradas con llave y monitoreadas.

La entrada del cableado de telecomunicaciones del Data Center no debe ser colocada en un cuarto de equipos comunes (CER).

Para reducir al mínimo el acoplamiento longitudinal entre los cables de energía y los cables de cobre de par trenzado, se deben respetarse las distancias de separación proporcionadas

Cantidad de circuitos	Tipo de circuito eléctrico	Distancia de separación (mm)
1 - 15	110/240V a 20A 1 fase blindada o sin blindaje	30 mm
16 - 30	110/240V a 20A 1 fase blindada	50 mm

31 - 60	110/240V a 20A 1 fase blindada	100 mm
61 - 90	110/240V a 20A 1 fase blindada	150 mm
91 +	110/240V a 20A 1 fase blindada	300 mm
1 +	415V a 100A 3 fases alimentador blindado	300 mm

Tabla Nro 05: Separación de Cables de par trenzado de cobre y cable de energía según TIA-942

Si los cables se energía son sin protección, las distancias de separación de la tabla se duplicarán.

Si se utilizan bandejas de cacles aéreos, la distancia de separación normal mínima es de 300 mm entre la parte superior de una bandeja y la parte inferior de la bandeja.

La fibra y el cableado de cobre de las bandejas de cable y de otras vías de uso común, deben estar separados de manera que mejore la administración, operación y la minimización del daño de los cables de fibra.

b. Rutas de entrada de telecomunicaciones

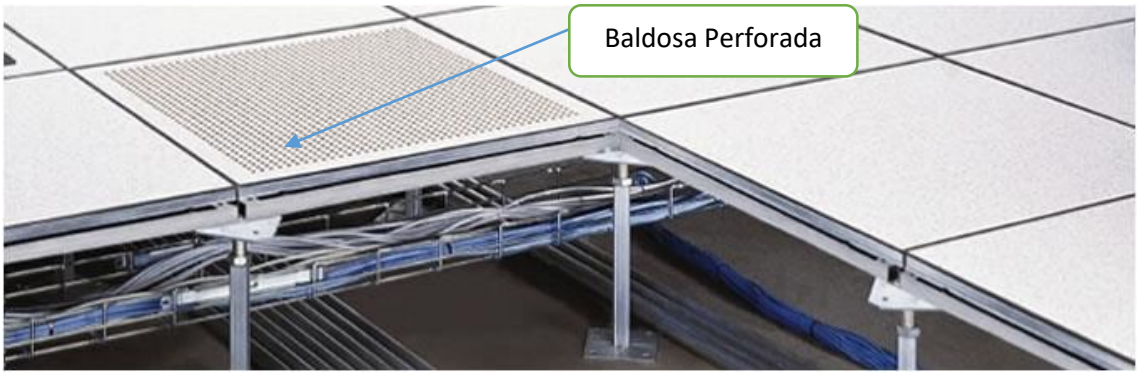
Deben ser subterráneas y a cada proveedor de servicios se le debe asignar por lo menos un tubo conduit de 100 mm de diámetro en cada punto de entrada. Los tubos conduit usados para los cables de fibra óptica de entrada deberán tener tres ductos interiores, dos tubos de 38 mm de diámetro y un tubo de 25 mm de diámetro, o tres tubos de 33 mm de diámetro (triducto).

c. Sistema de acceso por piso

También conocidos como sistemas de piso elevado, diseñado para hacer cableados desde abajo.

El cableado de telecomunicaciones en el piso de acceso estará en bandejas de cable que no bloquean el flujo de aire, éstas deben tener una profundidad máxima de 150 mm.

Ilustración Nro 15: Colocación de bandejas de cable en el piso



Fuente: http://www.corporativo-sic.com.mx/infraestructura/piso.php

d. Bandejas aéreas de cable

Pueden ser instaladas en varias capas para proporcionar capacidad adicional. Las instalaciones típicas incluyen dos o tres capas de soportes de cables, uno para los cables de alimentación y una o dos de cableado de telecomunicaciones.

Estas bandejas de cable aéreo se han complementado con un sistema de conductos o una bandeja de cables de conexión de fibra; el mismo que se puede asegurar a las mismas barras colgantes utilizadas para apoyar las bandejas de cable.

En los pasillos y otros espacios comunes en los Data Centers de Internet, las bandejas aéreas de cable, deben tener fondos sólidos o ser colocados por lo menos 2,7 m por encima del piso terminado.

La profundidad máxima recomendada de cualquiera de las bandejas de cable es de 150 mm; deben estar suspendidas del techo y conectadas a la infraestructura de conexión a tierra.

Los accesorios de iluminación y los aspersores se deben colocar entre las bandejas de cable, no directamente sobre las bandejas de cables.

e. Redundancia

Los Data Centers que están equipados con diversas instalaciones de telecomunicaciones deben ser capaces de continuar su función bajo condiciones

catastróficas, puesto que de otra manera se interrumpirían los servicios de telecomunicaciones del mismo.

ANSI/EIA/TIA-942 define distintos grados de disponibilidad basados en recomendaciones del Uptime Institute, estableciendo cuatro niveles (tiers) en función de la redundancia necesaria para alcanzar niveles de disponibilidad de hasta el 99,995%.

Lo cierto es que, para aumentar la redundancia y los niveles de confiabilidad, los puntos únicos de falla deben ser eliminados tanto en el Data Center como en la infraestructura que le da soporte.

- ✓ **Configuraciones de redundancia**

  Se usan "N", "N+1", "N+2", "2N", "2(n+1)" para designar a las distintas configuraciones de redundancia de los sitemas de alimentación ininterrumpida.

  Existen cinco:

  "N" Requisito base: Es la configuración más simple donde el sistema cumple los requisitos básicos y no proporciona redundancia.

  Redundancia "N+1": Es aquella que proporciona una unidad adicional, un módulo, una ruta, o un sistema, además de lo estrictamente necesario para satisfacer el requisito básico.

  El fracaso o el mantenimiento de cualquier unidad, módulo, o de la ruta no va a interrumpir las operaciones.

  Redundancia "N+2": Proporciona dos unidades adicionales, módulos, rutas, o sistemas, además de lo estrictamente necesario para satisfacer el requisito básico. El fracaso o el mantenimiento de cualquiera de las dos unidades individuales, los módulos, o los caminos no interrumpen las operaciones.

  Ésta es una de las configuraciones más habituales; requiere que las UPSs estén sincronizadas y habitualmente que sean del mismo fabricante.

  Redundancia "2N": Proporciona dos unidades completas, módulos, rutas, o sistemas; para cada uno requiere de un sistema base. El fracaso o el

mantenimiento de una unidad entera, módulo, ruta, o del sistema no interrumpirán las operaciones.

Tiene muchas posibles implementaciones en las que es posible eliminar los posibles puntos de fallo, con el consiguiente incremento en costes al redundar cuadros eléctricos, equipos de transferencia, etc.

Redundancia "2(N+1)": Ofrece dos unidades completas de redundancia (N+1), módulos, rutas o sistemas. Incluso en caso de fallo o mantenimiento de una unidad, módulo, ruta, o sistema, cierta redundancia se proporcionará y las operaciones no se interrumpirán.

- ✓ **Niveles de Tiers**

Tiers I:

- Negocios pequeños y tiendas (Empresas que venden soluciones informáticas).
- Infraestructura de TI solo para procesos internos.
- Compañías que hacen uso de la Web como una herramienta de mercadeo.
- Compañías que basan su negocio en Internet pero que no requieren calidad en sus servicios.

Tiers II:

- Negocios pequeños (Empresas que venden telefonía IP)
- Uso de TI limitado a las horas normales de trabajo
- Compañías de software que no ofrecen servicios "online" o "real-time"
- Compañías que basan su negocio en Internet pero que no requieren calidad en sus servicios.

Tiers III:

- Compañías que dan soporte 24/7 como centros de servicio e información

- Negocios donde los recursos de TI dan soporte a procesos automatizados.
- Compañías que manejan múltiples zonas horarias.

Tiers IV:

- Compañías con presencia en el mercado internacional.
- Servicios 24x365 en un mercado altamente competitivo.
- Compañías basadas en el comercio electrónico.
- Acceso a procesos y transacciones Online.
- Entidades financieras.

Características	**TIER I**	**TIER II**	**TIER III**	**TIER IV**
Vías de distribución	Solo 1	Solo 1	1 Activa 1 Pasiva	2 Activas
Componentes redundantes	N	N + 1	N + 1	2(N + 1) o S +
Altura del piso falso (cm)	30	45	75-90	75-90
Resistencia del piso kg/m^2	415	490	1250	1250+
Meses para implementar	1-3	3 a 6	15 a 20	15 a 30
Tiempo de inactividad de TI	28,8 h	22,0 h	1,6 h	0,4 h
Disponibilidad del sitio	99,671%	99,749%	99,982%	99,995%

Tabla Nro 06: Características de los Tiers

Características	**TIER I**	**TIER II Componentes redundantes**	**TIER III Mantener Concurrentemente**	**TIER IV Tolerante a fallos**
Centro de Operaciones	No requerido	No requerido	Requerido	Requerido
Servicios redundantes para acceso de proveedores	No requerido	No requerido	Requerido	Requerido
Vías de Backbone redundantes	No	No	Si	Si
Cableado horizontal redundante	No	No	No	Opcional
Fuente de poder redundante en routers y switches	No	Si	Si	Si

Tabla Nro 07: Niveles de un Data center

Característica	**TIER I**	**TIER II**	**TIER III**	**TIER IV**
Tipo de Construcción	Arrendada	Arrendada	Autónomo	Autónomo
Personal	Ninguno	1 turno	1 + turno	24 para siempre
Refrigeración ininterrumpida de Clase A	No	No	Posiblemente	Si

Resistencia del piso lbs/ft^2	85	100	150	150+
Voltaje de utilidad (Típico)	208, 480	208, 480	12-15kv^2	12-15 kV^2
Puntos únicos de fallo	Uno o más puntos de falla para sistemas de distribución de equipos en servicios eléctricos o sistemas mecánicos	Uno o más puntos de falla para sistemas de distribución de equipos en servicios eléctricos o sistemas mecánicos	Pocos+ errores humanos	Casi nulos excepto fuego y EPO

Tabla Nro 08: Atributos típicos de los Tiers

f. Sistemas críticos

En esta norma se especifica cuáles son los sistemas críticos que debe tener cada Tiers respecto a: Telecomunicaciones, Arquitectura y Estructura, Parte Eléctrica y Mecánica.

- ✓ **Requisitos del sistema de telecomunicaciones**

Tier I:

- *C*ableado, racks, gabinetes & rutas satisfacen requerimientos del TIA-942.
- Tiene 1 ruta de entrada desde el proveedor del acceso a la instalación.
- Ruta única para todo el cableado.
- Etiquetado recomendado: ANSI/TIA/EIA-606-A.

Tier II:

- Todos los requerimientos del Tier 1.
- Tiene 2 rutas de entrada desde el carrier (proveedor de acceso) a las instalaciones.
- Routers y switches tienen fuentes de alimentación y procesadores redundantes.
- Aborda vulnerabilidad de la entrada de servicio al edificio.

Tier III:

- Todos los requerimientos del Tier 2.
- Ser servido por al menos 2 carriers (proveedores de acceso).

- Un cuarto de entrada secundario con una separación mínima de 20 m del principal.
- Pathways del backbone redundantes.
- Múltiples routers y switches para redundancia.
- Aborda vulnerabilidad de un único proveedor de acceso (carrier).

Tier IV:

- Todos los requerimientos del Tier 3.
- Cableado de backbone redundante.
- El cableado de backbone debe estar en conductos (ser canalizado).
- Área de distribución secundaria opcional.
- Cableado horizontal redundante opcional.
- Aborda cualquier vulnerabilidad de la infraestructura del cableado.
- Áreas aisladas.

Subsistema de Telecomunicaciones	Tier I	Tier II	Tier III	Tier IV
Entrada de Proveedores de acceso diversificadas con mínimo 20m de separación	No	Si	Si	Si
Cuarto de entrada secundario	No	No	Si	Si
Área de istribución secundaria	No	No	No	Opcional
Routers y switches con fuente de alimentación redundante	No	Si	Si	Si

Tabla Nro 09: Características de los subsistemas de telecomunicaciones de los Tiers

✓ **Requisitos del Sistema Arquitectónico y Estructural**

Tier I:

No tiene protección de eventos físicos, naturales o intencionales.

Tier II:

- Protección mínima a eventos críticos.
- Puertas de seguridad.

Tier III:

- Acceso controlado por los sistemas de identificación y autenticación.
- Muros exteriores sin ventanas en los cuartos de cómputo.
- Protección contra radiación electromagnética.
- Seguridad perimetral con sistema de microondas de detección de intrusos y CCTV.

Tier IV:

- Protección contra desastres naturales como inundaciones, es decir control sobre todos los aspectos de sus instalaciones.
- Edificio separado.
- Requerimientos antisísmicos según la zona.

✓ **Requisitos del Sistema Eléctrico**

Tier I:

- Prevé el uso de un grupo electrógeno (gmg) como forma de respaldo ante un corte del suministro de la energía eléctrica pública.
- Piso falso, UPS y generador (opcionales) sin redundancia.
- Tiene una ruta de distribución.
- UPS simple o paralelos por capacidad, deben contar con bypass.
- PDUs y cuadros de distribución utilizados para distribución de la carga.
- Sistemas de tierra con requerimientos mínimos.
- El monitoreo de los sistemas es opcional.

Subsistema Arquitectónico	Tier 1	Tier 2	Tier 3	Tier 4
Proximidad a áreas de inundación registradas por las autoridades	NA	No permitido dentro de áreas	No debe haber historias de inundación durante los últimos 100 años y de 50 años a menos de 91 metros	No debe haber historias de inundación durante los últimos 100 años a menos de 91 metros
Proximidades a autopistas	NA	N A	No menos de 91 metros	No menos de 0.8 Km
Proximidad a aeropuertos	NA	N A	No menos de 1.6 Kms y no más de 48 Kms	No menos de 8 Kms y no más de 48 Kms
Aéreas de parqueo de visitantes y empleados separados	NA	N A	Si, físicamente separadas por una barrera o pared	18.3 mts de separación con barreras físicas

Edificio con diferentes dueños	NA	Permitido si no hay riesgos en los	Permitido si todos los ocupantes son compañías de TC	Permitido si todos los ocupantes son compañías de data
Debe cumplir con NFPA 75	NA	Si	Si	Si

Tabla Nro 10: Características de subsistemas arquitectura de los tiers

Tier II:

- Posee redundancia N+1 a nivel de los componentes principales de respaldo de energía (UPS y gmg) y en el sistema de aire acondicionado.
- PDUs redundantes, preferiblemente alimentados de sistemas UPS separados.
- Los gabinetes y bastidores deben tener circuitos eléctricos dedicados de 20A/120V.
- El sistema de puesta a tierra del edificio debe ser diseñado y probado para proporcionar una impedancia a tierra de menos de 5 ohmios.
- Debe ser proporcionado un Emergency Power Off System (EPO).

Tier III:

- Redundancia N+1 en los componentes de respaldo de energía, transformadores de la subestación, posee dos rutas de distribución de energía; una ruta estará activa y la otra será de respaldo.
- Todos los equipos deben admitir doble entrada de alimentación y a los que no admitan se les alimentará a través de una llave estática de transferencia de 2 entradas y 1 salida.
- Doble batería de arranque con cargadores individuales en los gmg.
- Autonomía en combustible de 72 h para los gmg.
- Doble banco de baterías para las UPS.
- Doble entrada de alimentación eléctrica.
- Poseerá sistema de tierra y sistema de protección contra rayos.
- Sistema de Control y Monitoreo para monitorear la mayoría de los equipos eléctricos.

Tier IV:

- Redundancia 2(N+1) en los componentes de respaldo de energía y varias rutas activas de distribución de energía.
- Cableados de energía en canalizaciones distintas por lugares separados.
- Todos los equipos deben admitir doble entrada de alimentación.
- La entrada de alimentación eléctrica debe ser distinta para cada transformador, así como exclusiva.
- Los UPS deben contar con bypass manual para mantenimiento o falla.
- El Data Center debe contar con una entrada de servicios dedicada y aislada de otras facilidades no críticas.
- El edificio debe tener al menos dos alimentadores de subestaciones de servicios públicos diferentes para redundancia.

Subsistema Eléctrico	**Tier 1**	**Tier 2**	**Tier 3**	**Tier 4**
Permite hacer mantenimientos sin shut down	No	No	Si	Si
Número de rutas de alimentación	1	1	Uno activo uno pasivo	Dos activos
Acometida de proveedor externo de energía	Alimentación sencilla	Alimentación sencilla	Alimentación dual	Alimentación dual
Redundancia en generador	N	N	N+1	2N
Cables de alimentación de equipos de cómputo y comunicaciones	Uno	Dos	Dos	Dos
Autonomía de combustible	8 horas	24 horas	72 horas	96 horas
Redundancia en UPS	N	N+1	N+1	2N
Topología de UPS	Módulo sencillo	Paralelo redundante o distribuido redundante	Paralelo redundante o distribuido redundante	Paralelo redundante o distribuido
Boton de apagado de emergencia (EPO)	Si	Si	Si	Si

Tabla Nro 11: Características de subsistemas eléctricos de los Tiers

- ✓ **Requisitos del Sistema Mecánico**

Tier I:

- Una o varias unidades de aire acondicionado sin redundancia.
- Tuberías con una sola ruta

Tier II:

- Incluye un aire acondicionado con la capacidad de refrigeración, para mantener la temperatura crítica y la humedad.
- Los sistemas de aire acondicionado deben cumplir 7 x 24 x 365 y deben contar con redundancia N+1.
- Todos los equipos de aire acondicionado deben accionarse por el sistema generador de reserva.
- Todos los sistemas de control de la temperatura deben ser alimentados a través de circuitos dedicados redundantes de la UPS.
- Un sistema de reserva a diesel debe ser instalado para proporcionar energía al sistema de suministro de alimentación ininterrumpida y equipos mecánicos.

Tier III:

- Múltiples unidades de aire acondicionado.
- La redundancia puede obtenerse de las dos fuentes de suministro de energía a cada unidad de aire acondicionado, o dividir los equipos de aire acondicionado entre varias fuentes de alimentación.
- Tuberías y bombas duales.
- Todos los acondicionadores de aire del cuarto de cómputo deben estar respaldados por un generador de poder.
- Equipo de refrigeración con redundancia N+1, N+2, 2N, o 2 (N+1) puede ser dedicado para el Data Center.

Sub Sistema Mecanico	**Tier I**	**Tier II**	**Tier III**	**Tier IV**
Redundancia de unidades de aire acondicionado	No tiene unidades redundantes	Una unidad redundante por área crítica	Cantidad de unidades AC suficientes para mantener el área crítica durante la pérdida de una fuente de potencia	Cantidad de unidades AC suficiente para mantener el área crítica durante la pérdida de una fuente de potencia eléctrica
Alimentación eléctrica para equipos de aire	Camino sencillo	Camino sencillo	Múltiples caminos	Múltiples caminos
Tuberías para refrigerantes	Camino sencillo	Camino sencillo	Camino doble	Camino doble

Sistema de extinción automática con supresión por agua o agente	Si	Si	Si	Si

Tabla Nro 12: Características de subsistemas mecánicos de los Tiers

Tier IV:

- Soporta fallas en un tablero de alimentación.
- El sistema de climatización incluye varias unidades de aire acondicionado con la capacidad de refrigeración, para mantener la temperatura crítica y la humedad relativa a las condiciones de diseño, con suficientes unidades redundantes.
- El sistema de tuberías o sistemas de doble vía no causará la interrupción del sistema de aire acondicionado.

2.2.5. Normas ISO

Son documentos que especifican requisitos, especificaciones, directrices o características que pueden ser empleados en organizaciones para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con su objetivo. Hasta el momento ISO (International Organization for Standardization), ha publicado alrededor de 21780 normas internacionales. (25)

2.2.5.1. Norma ISO 27002

Esta Norma Internacional proporciona una lista de objetivos de control comúnmente aceptados, controles de mejores prácticas que se utilizarán como guía de implementación al seleccionar e implementar controles para lograr la seguridad de la información.

En la actualidad la norma ISO/IEC 27002:2005 cuenta con 11 dominios, 39 Objetivos de control y 133 Controles:

Sección 5: Políticas de seguridad de la información

Sección 6: Organización de la seguridad de la información

Sección 7: Seguridad de los recursos humanos

Sección 8: Gestión de Activos

Sección 9: Control de Acceso

Sección 10: Criptografía

Sección 11: Seguridad física y ambiental

Sección 12: Seguridad operacional

Sección 13: Seguridad de las comunicaciones

Sección 14: Adquisición, desarrollo y mantenimiento de sistema

Sección 15: Relaciones con proveedores

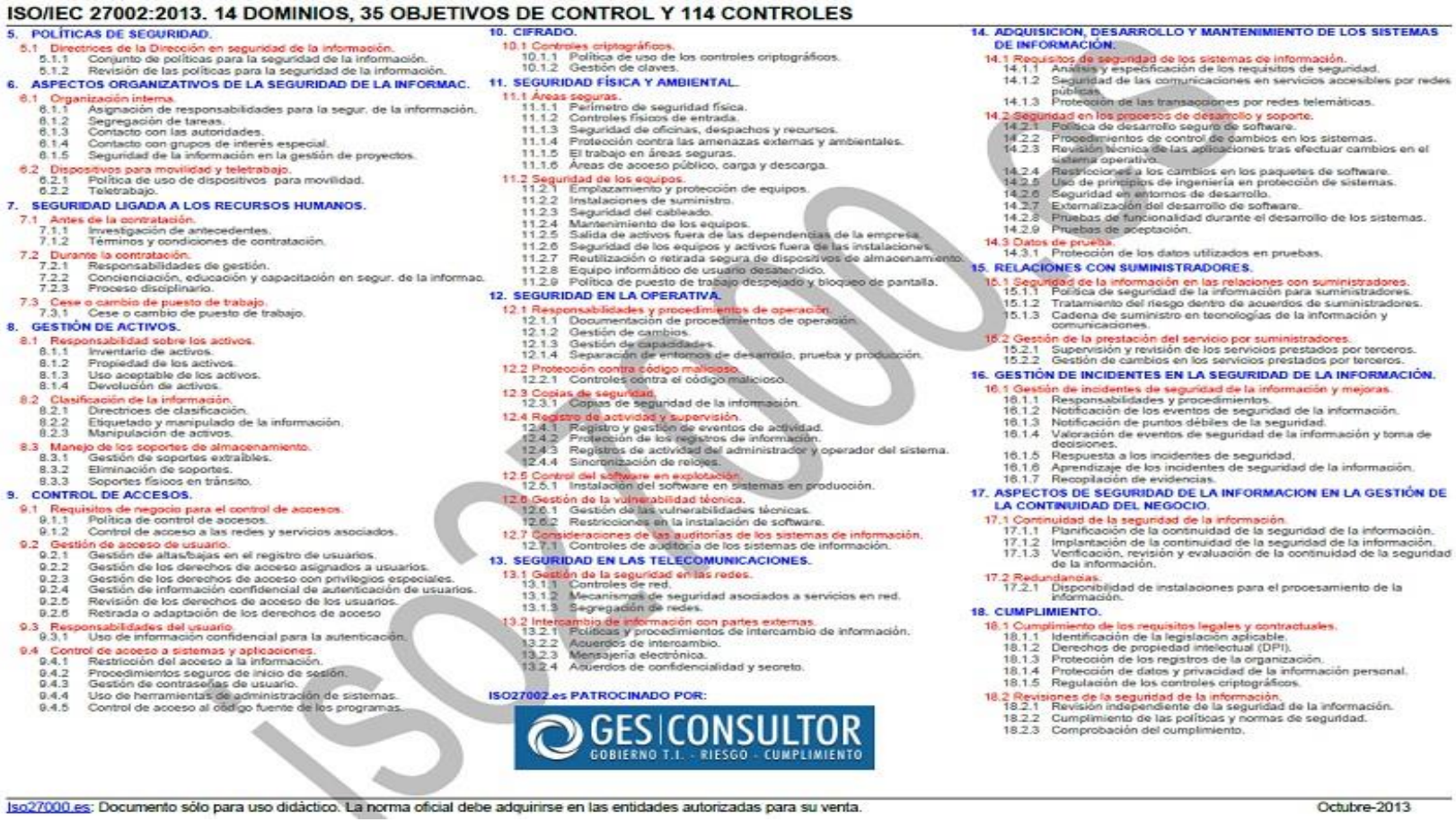
Sección 16: Gestión de incidentes de seguridad de la información

Sección 17: Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

Sección 18: Cumplimiento

Para el desarrollo del proyecto de investigación y elaboración del instrumento de medición, se tomara en cuenta controles que vas estrechamente relacionados con un centro de datos, por la naturaleza del proyecto (Diagnostico Situacional).

Ilustración Nro 16: Controles ISO 27002



ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Octubre-2013

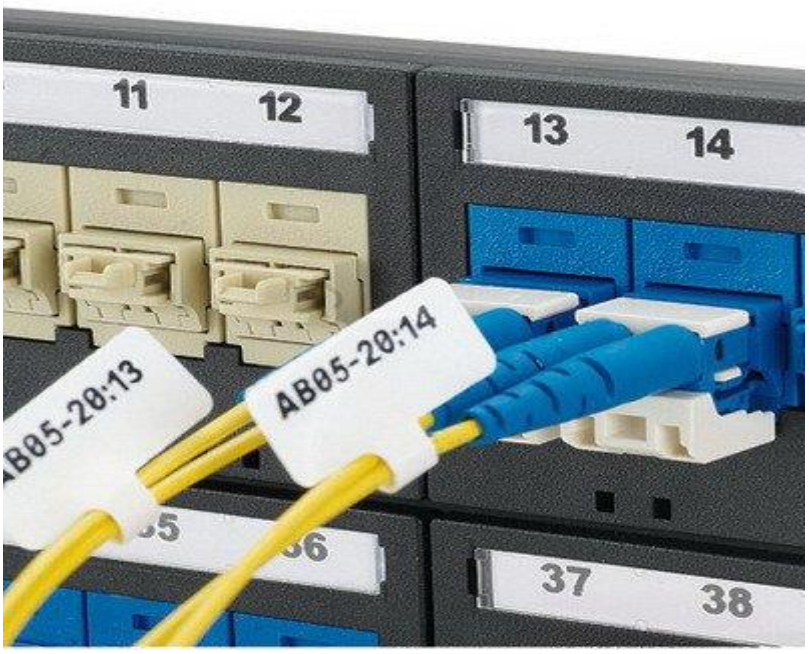
Fuente: ISO 27000.es

2.2.6. Norma ANSI/TIA/EIA 606

La norma ANSI/TIA/EIA 606 es vital para el buen funcionamiento de su cableado estructurado ya que habla sobre la identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con la finalidad de que se puedan identificar cada uno de los servicios que en algún momento se tengan que habilitar o deshabilitar. Esto es muy importante, ya que en la documentación que se debe entregar al usuario final, la norma dice que se tendrá que especificar la forma en que está distribuida la red, por dónde viaja, qué puntos conecta y los medios que utiliza (tipos de cables y derivaciones) (26).

Se define la manera como rotular todos los componentes de un sistema de cableado estructurado, el cual provee un esquema de administración uniforme, es decir que rige para todos los aspectos del cableado estructurado. La norma 606 es indispensable para el correcto funcionamiento del cableado estructurado ya, que habla sobre la identificación de cada uno de los subsistemas basado en etiquetas, códigos y colores, con finalidad de que se puedan identificar con facilidad cada uno de los cables y su servicio.

Ilustración Nro 17: etiquetado y Rotulado de componentes del cableado



Fuente: https://www.cesco.com

Al momento de realizar las etiquetas hay que tomar en cuenta que estas deben tener un tamaño, color y contraste apropiado para asegurar su Lectura, y el material con las que sean realizadas debe garantizar que tengan un tiempo de vida igual o superior al componente etiquetado.

Los componentes a ser etiquetados son:

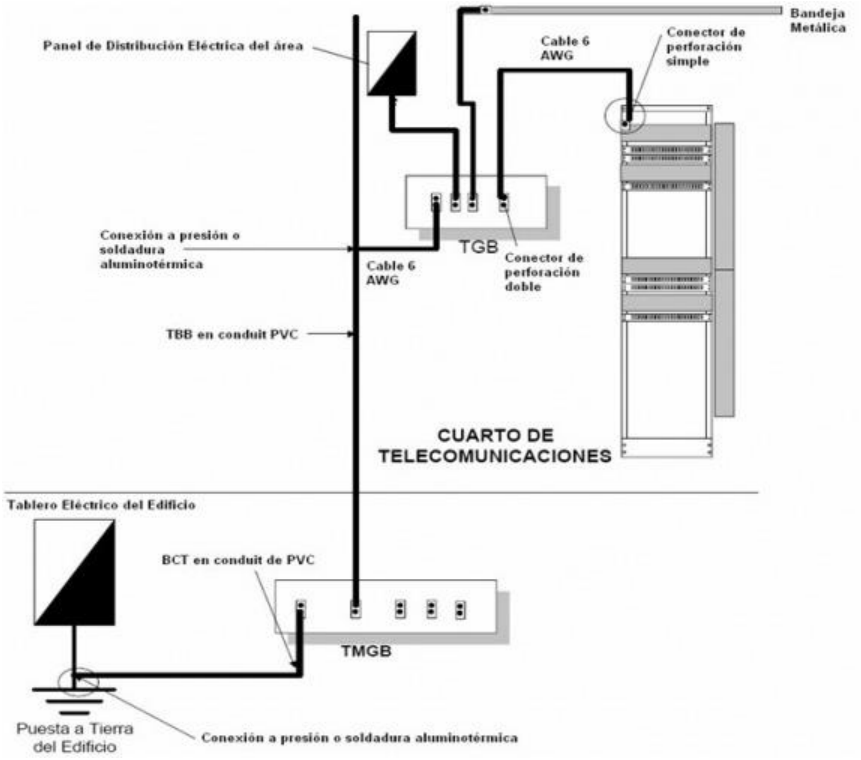
- Espacios de telecomunicaciones.
- Cables
- Hardware
- Puestas a Tierra

2.2.7 ANSI/TIA/EIA 607

Requerimientos para telecomunicaciones de puesta a tierra y puenteado de edificios comerciales. ANSI/TIA/EIA-607 discute el esquema básico y los e infraestructura de las telecomunicaciones mediante el empleo de un sistema de puesta a tierra adecuadamente configurado e instalado. EIA/TIA 607 define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y proteger los elementos del sistema estructurado.11 ANSI/TIA/EIA -607 Tierras y aterramientos para los sistemas de telecomunicaciones de edificios comerciales. Con mejoras en las estructuras de computadoras.

El estándar que describe el sistema de puesta a tierra para las redes de telecomunicaciones es ANSI/TIA/EIA-607. El propósito principal es crear un camino adecuado y con capacidad suficiente para dirigir las corrientes eléctricas y voltajes pasajeros hacia la tierra. Estas trayectorias a tierra son más cortas de menor impedancia que las del edificio.

Ilustración Nro 18: Distribución y topología de conexión Puesta a Tierra



Fuente: ANSI/TIA/EIA 607

A continuación, se explicarán términos básicos para entender un sistema de puesta a tierra en general:

Puesta a tierra (grounding): Es la conexión entre un equipo o circuito eléctrico y la tierra

Conexión equipotencial a tierra (bonding): Es la conexión permanente de partes metálicas para formar una trayectoria conductora eléctrica que asegura la continuidad eléctrica y la capacidad de conducir de manera segura cualquier corriente que le sea impuesta.

Conductor de enlace equipotencial para telecomunicaciones (BCT): Es un conductor de cobre aislado que interconecta el sistema de puesta a tierra de telecomunicaciones al sistema de puesta a tierra del edificio. Por lo tanto une el TMGB con la puesta a tierra del sistema de alimentación. Debe ser dimensionado al menos de la misma sección que el conductor principal de enlace de telecomunicaciones (TBB). No debe llevarse en conductos metálicos.

Barra de tierra principal de telecomunicaciones (TMGB): Es una barra que sirve como una extensión dedicada del sistema de electrodos de tierra (pozo a tierra) del edificio para la infraestructura de telecomunicaciones. Todas las puestas a tierra de telecomunicaciones se originan en él, es decir que sirve como conexión central de todos los TBB del edificio.

Consideraciones del diseño:

- Usualmente se instala una por edificio.
- Generalmente está ubicada en el cuarto de entrada de servicios
- En el cuarto de equipos, en cualquiera de los casos se tiene que tratar de que el BCT sea lo más corto y recto posible.
- Montada en la parte superior del tablero o caja.
- Aislada del soporte mediante aisladores poliméricos (50 mm. mínimo)
- Hecha de cobre y sus dimensiones mínimas 6 mm. de espesor y 100 mm. de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá.

Barra de tierra para telecomunicaciones (TGB): Es la barra de tierra ubicada en el cuarto de telecomunicaciones o de equipos que sirve de punto central de conexión de tierra de los equipos de la sala.

Consideraciones del diseño:

- Cada equipo o gabinete ubicado en dicha sala debe tener su TGB montada en la parte superior trasera.
- El conductor que une el TGB con el TBB debe ser cable 6 AWG. Además, se debe procurar que este tramo sea lo más recto y corto posible.

- Hecha de cobre y sus dimensiones mínimas 6 mm. de espesor y 50 mm. de ancho. Su longitud puede variar, de acuerdo a la cantidad de cables que deban conectarse a ella y de las futuras conexiones que tendrá.
- Aislada mediante aisladores poliméricos (h=50 mm mínimo)

Conductor central de enlace equipotencial de Telecomunicaciones (TBB): Es un conductor aislado de cobre utilizado para conectar todos los TGB's al TMGB. Su principal función es la de reducir o ecualizar todas las diferencias de potencial de todos los sistemas de telecomunicaciones enlazados a él.
Consideraciones del diseño:

- Se extiende a través del edificio utilizando la ruta del cableado vertical.
- Se permite varios TBB's dependiendo del tamaño del edificio.
- Cuando dos o más TBB's se usen en un edificio de varios pisos, éstos deberán ser unidos a través de un TBBIBC en el último piso y cada tres pisos.
- Su calibre debe ser mínimo 6 AWG y máximo 3/0 AWG, por lo tanto se deberá usar un conductor de cobre aislado cuya sección acepte estas medidas.
- El estándar ha establecido una tabla para diseñar este conductor de acuerdo a su distancia:

2.2.8. Análisis De Riesgo

Existen riesgos asociados al uso de las tecnologías de información, ya sea daños causados por desastres naturales, errores y fallos no intencionados y por ataques intencionados debido a intrusos con fin de sustraer datos de la empresa para beneficios propios. Por lo tanto, la organización debe realizar el análisis de riesgos, porque en definitiva en la actualidad el valor de la información es enorme. Por eso se vuelve imprescindible poder contar con una estrategia y herramientas que nos permitan evaluar y reconocer todos los riesgos asociados con el uso de las TI, con el objetivo de poder minimizar esos riesgos.

En este sentido, lo primero que debemos tener en cuenta para realizar un análisis serio de la situación es conocer los riesgos típicos que suelen presentar las TI, es decir cuáles son las amenazas más frecuentes.

2.2.8.1. Metodología De Gestión De Riesgo

Definición de riesgo:

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema. (27)

Análisis de riesgos:
Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.
Gestión de riesgos:
Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

EL Análisis y gestión de riesgos en su contexto
Las tareas de análisis y gestión de riesgos no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad.
El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección (27).

2.2.8.2. MAGERIT
Implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información (28).

Análisis y gestión de riesgos

Seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles (28).

El objetivo a proteger es la misión de la organización, teniendo en cuenta las diferentes dimensiones de seguridad:

Disponibilidad: Disposición de los servicios a ser usados cuando sea necesario, la carencia de disponibilidad supone una interrupción del servicio.

Integridad: Mantenimiento de las características de completitud y corrección de los datos. Evitar que la información pueda aparecer manipulada.

Confidencialidad: Que la información llegue solamente a personas autorizadas.

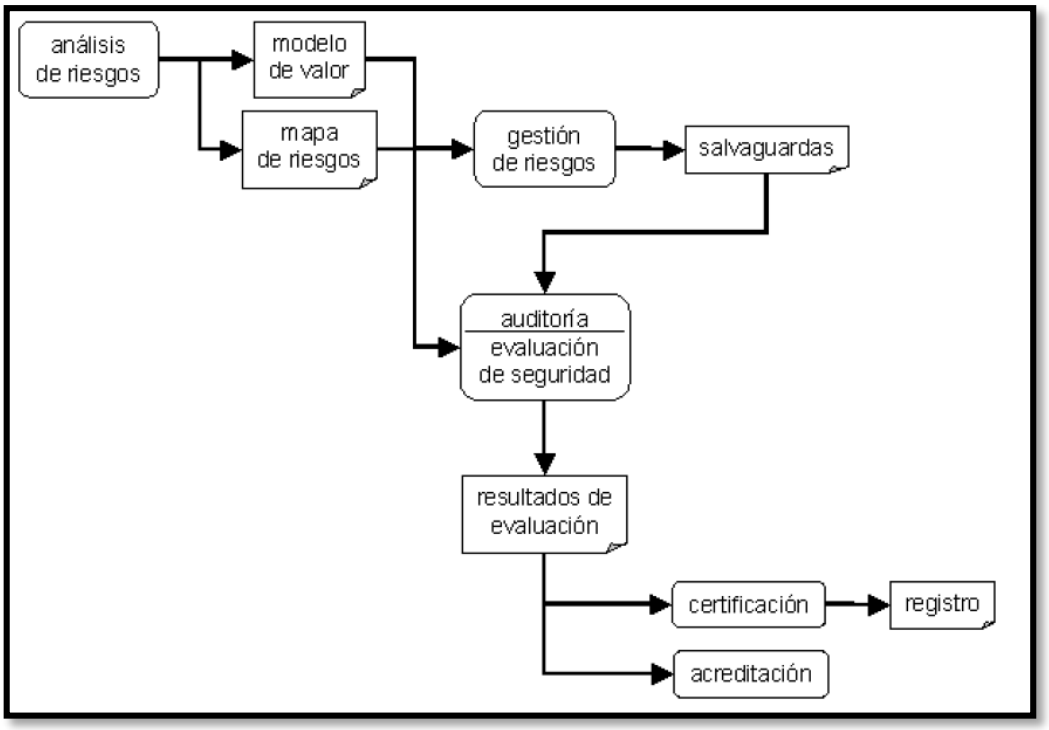
Objetivos:

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicación (TIC)
- ✓ Ayuda a describir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Evaluación, certificación, auditoría y acreditación

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. El análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado. El análisis de riesgos es un paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema: (28)

Ilustración Nro 19: Contexto de certificación y acreditación de sistemas de información



Fuente: Magerit v3 (28)

Método de Análisis de Riesgo

El análisis de riesgo es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

1. Determinar los Activos: relevantes para la organización, su interrelación y su valor, en el sentido de que perjuicio (coste) supondría su degradación.

- ✓ Datos
- ✓ Servicios
- ✓ Aplicaciones informáticas
- ✓ Equipos informáticos
- ✓ Soportes de información
- ✓ Equipamiento auxiliar
- ✓ Redes de comunicaciones
- ✓ Instalaciones
- ✓ Personas

2. Determinar las amenazas: a la que están expuestas los activos determinados.

- ✓ Origen Natural
- ✓ Del entorno (de origen industrial)

- ✓ Defectos de las aplicaciones
- ✓ Causadas por las personas de forma accidental
- ✓ Causadas por las personas de forma deliberada

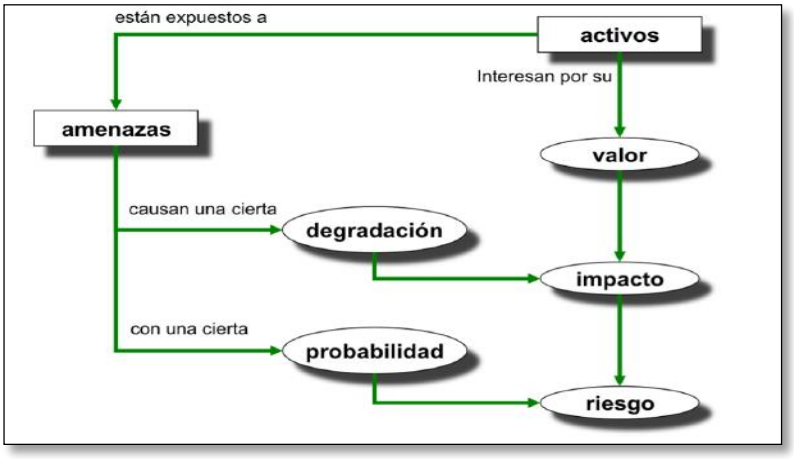
3. Determinar Salvaguardas: dispuestas y cuan eficientes son frente al riesgo.

- ✓ Tipo de activos a proteger
- ✓ Dimensión o dimensiones de seguridad que requiere protección
- ✓ Amenazas de las que necesitamos protegernos
- ✓ Si existe salvaguardas alternativas

4. Estimar el impacto: Definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el Riesgo: Definido como el impacto ponderado con la tasa de ocurrencia.

Ilustración Nro 20: Elementos del análisis de riesgo potencial



Fuente: Magerit v3 (28)

Lista de activos del centro de Datos

ACTIVO	CATEGORÍA
Centro de datos	Infraestructura
Computador de escritorio	Infraestructura
Computador portátil	Infraestructura
Servidor de aplicación	Infraestructura
Servidor de archivos	Infraestructura
Switch	Infraestructura
Router	Infraestructura
Modem	Infraestructura
Firewall	Infraestructura
Medios Extraíbles	Infraestructura

Red de Cableado	Infraestructura
Discos de Backup	Infraestructura
Servidor Proxi	Infraestructura
Servidor DHCP	Infraestructura
Central Telefónica	Infraestructura
Red Telefónica	Infraestructura
Fuentes de alimentación	Equipamiento Auxiliar
Sistema de alimentación ininterrumpida	Equipamiento Auxiliar
Equipos de Climatización	Equipamiento Auxiliar
Sistema contra Incendio	Equipamiento Auxiliar

Lista de amenazas del data center

AMENAZAS	CATEGORÍA
Acceso no autorizado al centro de datos	Cumplimiento
Incumplimiento en el mantenimiento/ chequeo del sistema de información	Cumplimiento
Uso no autorizado de equipo informático	Cumplimiento
Uso de software sin licencia	Cumplimiento
Manipulación con hardware	Fraude interno/externo
Hurto de documentos	Fraude interno/externo
Acceso forzado al centro de datos	Fraude interno/externo
Falla suministro eléctrico	Interrupción y fallas del sistema
Falla de equipo informático	Interrupción y fallas del sistema
Errores de hardware	Interrupción y fallas del sistema
Errores de administración	Interrupción y fallas del sistema
Errores de actualización y mantenimiento	Interrupción y fallas del sistema
Amenazas de equipos por temperatura y humedad	Física
Humo e incendios	Física
Filtración de líquidos	Física
Terremotos, inundaciones, tormentas, avalancha	Física

Lista de vulnerabilidades del data center

VULNERABILIDADES
Falta de protección física en puertas
Acceso no protegido a las instalaciones informáticas
Sistemas contra incendios insuficientes
Diseño deficiente de edificios
Construcción deficiente de edificios
Materiales inflamables empleados en la construcción
Falta de protección física en las ventanas

Paredes que se pueden asaltar físicamente
Paredes interiores que no sellan la sala por completo tanto en el techo como en suelo
Instalación situada sobre una línea de error
Falta de revisiones de hardware
Sistema sin proteger físicamente
Falta de procedimientos
Falta de planes de continuidad
Falta de políticas de uso

III. SISTEMA DE HIPÓTESIS

3.1. Hipótesis Principal

El diagnostico situacional de data center determina las mejoras y continuidad del servicio que brindan el Data Center de la EsSalud Ancash- Huaraz.

3.2. Hipótesis específicas.

- El centro de datos tiene un nivel de fiabilidad muy bajo, siendo necesario una reestructuración del mismo.

IV. METODOLOGIA

4.1. Diseño de la investigación

Según Hernández R. (29), el diseño señala al investigador lo que debe hacer para alcanzar sus objetivos de estudio, contestar las interrogantes que se planteado y analizar la certeza de la hipótesis formuladas en un contexto en particular.

La investigación utilizada para el desarrollo de este trabajo es de diseño no experimental, investigación cuantitativa y de nivel descriptivo:

- Diseño no experimental; por que la variable de estudio no se manipula y son observadas tal y como se presentan en la realidad.
- Investigación cuantitativa; Para determinar el estado situacional del Data Center se aplica un checklist objetiva; controles las cuales serán cuantificadas, por contener como únicas respuestas (si o no).
- Nivel descriptivo; En un estudio descriptivo se selecciona una serie de cuestiones, conceptos o variables y se mide cada una de ellas con el propósito de describirlas.

  Se Utilizó de tipo descriptiva, porque se tuvo que realizar visitas a la organización y aplicar un checklist con el fin de recolectar información para determinar el estado actual del data center.

4.2. Población y Muestra

La población a la que se aplicara los instrumentos de medición para esta investigación es aplicar un checklist al Centro de Datos, por ser mínima la población se realizara el estudio con la totalidad de la población.

4.3 Técnicas e Instrumentos

4.3.1 Técnicas

Para determinar el diagnostico situacional del data center del EsSalud de Huaraz se utilizará la técnica de Observación.

- **La Observación**

  Se define como una técnica de recolección de datos que permite acumular y sistematizar información sobre un hecho o fenómeno social que tiene relación

con el problema que motiva la investigación. En la aplicación de esta técnica, el investigador registra lo observado, mas no interroga a los individuos involucrados en el hecho o fenómeno social; es decir, no hace preguntas, orales o escrita, que le permitan obtener los datos necesarios para el estudio del problema. (30)

4.3.2 Instrumentos

El instrumento será aplicado al Data center del EsSalud de Huaraz.

- **Checklist**

  La lista de chequeo, como herramienta metodológica está compuesta por una serie de ítems, factores, propiedades, aspectos, componentes, criterios, dimensiones o comportamientos, necesarios de tomarse en cuenta, para realizar una tarea, controlar y evaluar detalladamente el desarrollo de un proyecto, evento, producto o actividad. Dichos componentes se organizan de manera coherente para permitir que se evalúe de manera efectiva, la presencia o ausencia de los elementos individuales enumerados o por porcentaje de cumplimiento u ocurrencia. (31)

4.4. Procedimiento de recolección de datos

Se inició con la identificación de las diferentes fuentes de información, técnicas y la elaboración del instrumento para la recolección de datos, luego se procedió obtener la autorización para llevar a cabo la aplicación del instrumento, identificando el lugar y tiempo que tomara la aplicación, finalmente se procedió a aplicar el checklist lo cual ayudara a determinar el diagnostico situacional del data center del EsSalud de Huaraz.

4.5. Definición operacional de Variables en estudio

Tabla Nro 13: Matriz de Operacionalización de variables

Variables	Definición Conceptual	Dimensión	Indicadores	Definición Operacional
Interviniente: Normativa y estándares de diseño de un data center	Normativa que establece una guía de recomendaciones y directrices para implementar un Data Center aprobado en el 2005 por ANSI	Establece Recomendaciones en cuanto a: Telecomunicaciones, arquitectura, sistema eléctrico, sistema mecánico y seguridad Informática.	-Genera herramienta de recolección de datos. -Controles de medición y clasificación de Data Center.	Si No
Dependiente: Diagnostico Situacional del data center	-Diagnostico que produce conocimientos para la acción y toma de decisiones adecuadas para asegurar la continuidad del servicio de un data center. -Resultado al aplicar los controles establecidos por la normativa TIA-942	Necesidad de contar con un diagnostico situacional lo cual determinara la continuidad o restructuración de los servicios.	-Estado situacional Reporte de resultados. -Propuesta de mejora para Data center. -Conocimiento de controles a tener en cuenta para el diseño de un data center.	Tier I - Regular Tier II - Bueno Tier III – Muy bueno Tier IV - Excelente

Fuente: Elaboración Propia

4.6 Plan de Análisis

-Procedimientos de recolección de datos, para determinar el diagnostico situacional del data center del EsSalud de Huaraz, se efectuó la visita del caso a la organización y al área de informática con la finalidad de realizar la aplicación del checklist que cuenta con 81 items.

-Plan de Análisis de Datos, se determina las especificaciones de infraestructura del data center; para poder determinar el diagnostico situacional es ideal identificar de cómo están implementadas y si cumplen con los controles y recomendaciones que establecen los estándares y normas.

V. RESULTADOS

5.1 Resultados

5.1.1. Resultados por dimensiones

5.1.1.1 Arquitectura

Tabla Nro 14: Ubicación del data center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**3**	**60**
No	**2**	**40**
Total	**5**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro. 14 se puede observar que el 60% del total de los ítems cumplen con los controles que establecen los estándares y normativas.

Tabla Nro 15: Acceso al data Center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**1**	**33.3**
No	**2**	**66.7**
Total	**3**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 15 se puede observar que el 66.7% del total de ítems no cumplen con los controles que establecen los estándares y normativas.

Tabla Nro 16: Tamaño del Data Center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**1**	**25**
No	**3**	**75**
Total	**4**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 16 se puede observar que el 75% del total de ítems no cumplen con los controles que establecen los estándares y normativas.

Tabla Nro 17: Altura del Techo

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**2**	**50**
No	**2**	**50**
Total	**4**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 17 se puede observar que el 50% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 18: Iluminación del data center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**3**	**75**
No	**1**	**25**
Total	**4**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 18 se puede observar que el 25% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 19: Puertas de acceso del data center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**4**	**66.7**
No	**2**	**33.3**
Total	**6**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 19 se puede observar que el 33.3% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 20: Carga sobre el Suelo

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**2**	**100**
No	**0**	**0**
Total	**2**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 20 se puede observar que el 0% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 21: Señalización y consideraciones Sísmicas

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**1**	**33.3**
No	**2**	**66.7**
Total	**3**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 21 se puede observar que el 66.7% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 22: Diseño Ambiental

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**1**	**11.1**
No	**8**	**88.9**
Total	**9**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 22 se puede observar que el 88.9% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 23: Consolidado del sistema de Arquitectura

Alternativas	n	%
Si	**18**	**45**
No	**22**	**55**
Total	**40**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 23 se puede observar que el 55% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

5.1.1.2 Sistema Eléctrico

Tabla Nro 24: Diseño Eléctrico - Fuente de Poder

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**4**	**57.1**
No	**3**	**42.9**
Total	**7**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 24 se puede observar que el 42.9% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 25: Conexión Puesta a Tierra del Data Center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**2**	**66.7**
No	**1**	**33.3**
Total	**3**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 25 se puede observar que el 33.3% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 26: Consolidado del sistema eléctrico

Alternativas	n	%
Si	**6**	**60**
No	**4**	**40**
Total	**10**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 26 se puede observar que el 40% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

5.1.1.2 Sistema de Telecomunicaciones

Tabla Nro 27: Sistema de Telecomunicaciones

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**10**	**100**
No	**0**	**0**
Total	**10**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 27 se puede observar que el 0% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 28: Cableado Data Center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**4**	**66.7**
No	**2**	**33.3**
Total	**6**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 28 se puede observar que el 33.3% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Tabla Nro 29: Consolidado del sistema de Telecomunicaciones

Alternativas	n	%
Si	**14**	**87.5**
No	**2**	**12.5**
Total	**16**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 29 se puede observar que el 12.5% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

5.1.1.2 Sistema Mecánico

Tabla Nro 30: Sistema Mecánico del data center

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**3**	**60**
No	**2**	**40**
Total	**5**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 30 se puede observar que el 40% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

5.1.1.2 Sistema Seguridad Informática

Tabla Nro 31: Seguridad Informática

Distribución de resultados; respecto al análisis del diagnóstico situacional del data center del EsSalud Huaraz; 2017;

Alternativas	n	%
Si	**7**	**70**
No	**3**	**30**
Total	**10**	**100%**

Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 31 se puede observar que el 30% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

5.1.2. Resultado General

Tabla Nro 32: Consolidado General

Alternativas	n	%
Si	**48**	**59.3**
No	**33**	**40.7**
Total	**81**	**100%**

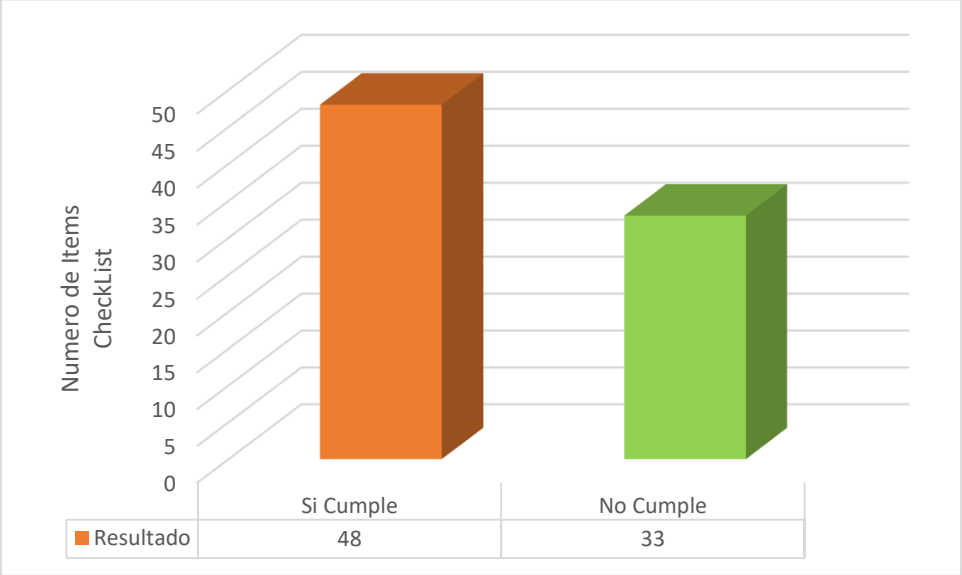
Fuente: Aplicación del checklist para determinar el diagnostico situacional del data center.

Aplicado por: Tongo Y.; 2017

En la Tabla Nro 32 se puede observar que el 40.7% del total de ítems no cumplen con los controles que establecen los estándares y normativa.

Ilustración Nro 21: Resultados consolidados del CheckList

Resultado consolidado del checklist aplicado para determinar el diagnostico situacional del Data Center del EsSalud de Huaraz; 2017.



5.2 Análisis de resultado

La presente investigación tuvo como objetivo general: determinar el diagnostico situacional de data center bajo estándares y normativa del EsSalud Red Asistencial de Ancash – Huaraz, 2017; a fin de determinar la continuidad del servicio o reestructuración del data center para garantizar la fiabilidad de la información; en

consecuencia, se ha tenido que realizar la aplicación del instrumento que permita conocer el estado situacional del data center. En consecuencia, luego de la interpretación de los resultados se realizó los siguientes análisis de resultados.

1. En lo que respecta a la dimensión: Arquitectura en la tabla Nro 23 se puede interpretar que el 55% del total de ítems no cumplen con los controles que establecen los estándares y normativas; mientas que el 45% de los ítems si cumplen.

   Estos resultados nos muestran que el Data Center del EsSalud de Huaraz reúne las condiciones de una infraestructura Básica con un nivel de fiabilidad baja, considerando que más del 50% de controles no se cumplen, se concluye una alta necesidad prioritaria y urgente de una reestructuración del data center.

2. En lo que respecta a la dimensión: Eléctrico en la tabla Nro 26 se puede interpretar que el 40% del total de ítems no cumplen con los controles que establecen los estándares y normativas; mientas que el 60% de los ítems si cumplen.

   Estos resultados nos muestran que el Data Center del EsSalud de Huaraz reúne las condiciones de una infraestructura Básica con un nivel de fiabilidad Media, considerando que del 40% de controles no se cumplen, se concluye una necesidad prioritaria de una reestructuración del data center.
3. En lo que respecta a la dimensión: Telecomunicaciones en la tabla Nro 29 se puede interpretar que el 12.5% del total de ítems no cumplen con los controles que establecen los estándares y normativas; mientas que el 87.5% de los ítems si cumplen.

   Estos resultados nos muestran que el Data Center del EsSalud de Huaraz reúne las condiciones de una infraestructura Básica con un nivel de fiabilidad Alta, considerando que tan solo el 12.5% de controles no se cumplen, se concluye que se priorice mejorar las deficiencias para optimizar y conseguir un servicio muy fiable.
4. En lo que respecta a la dimensión: Mecánico en la tabla Nro 30 se puede interpretar que el 40% del total de ítems no cumplen con los controles que

establecen los estándares y normativas; mientas que el 60% de los ítems si cumplen.

Estos resultados nos muestran que el Data Center del EsSalud de Huaraz reúne las condiciones de una infraestructura Básica con un nivel de fiabilidad Media, considerando que del 40% de controles no se cumplen, se concluye una necesidad prioritaria de una reestructuración del data center en el sistema Mecánico.

5. En lo que respecta a la dimensión: Seguridad Informática en la tabla Nro 31 se puede interpretar que el 30% del total de ítems no cumplen con los controles que establecen los estándares y normativas; mientas que el 70% de los ítems si cumplen.

   Estos resultados nos muestran que el Data Center del EsSalud de Huaraz reúne las condiciones de una infraestructura Básica con un nivel de fiabilidad Alta, considerando que del 30% de controles no se cumplen, se concluye que se priorice mejorar las deficiencias para optimizar y conseguir un servicio muy fiable.

En lo que respecta la dimensión general: Data Center en la tabla Nro 32 se puede interpretar que el 40.7% del total de ítems no cumplen con los controles que establecen los estándares y normativa; mientras que el 59.3% de los ítems si se cumplen.

El resultado nos muestra la deficiencia de los subsistemas implementados en el data center, siendo necesario la reestructuración del mismo, considerando que se brinda un servicio con un nivel de fiabilidad baja, no siempre se cumplen en su totalidad de controles ya que las características de las instalaciones de un edificio y las exigencias de la organización 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 normativas.

5.3 Propuesta de mejora

A consecuencia del análisis de los resultados obtenidos y explicados anteriormente, se planteó como propuesta de mejorar la fiabilidad del servicio del data center lo siguiente:

Diseñar e Implementar el Data Center para la EsSalud Red Asistencial de Ancash – Huaraz en base al estándar TIA-942; 2017.

Para el diseño considerar las directrices y recomendaciones que nos ofrecen el estándar ANSI/TIA/EIA 942; El centro de datos de la EsSalud por la información crítica que gestiona, el estándar establece que el nivel mínimo es TIER II instraestructura con dispositivos redundantes.

Requerimientos mínimos para TIER II por subsistemas:

Telecomunicaciones:

- Todos los requerimientos del Tier 1.
- Tiene 2 rutas de entrada desde el carrier (proveedor de acceso) a las instalaciones.
- Routers y switches tienen fuentes de alimentación y procesadores redundantes.
- Aborda vulnerabilidad de la entrada de servicio al edificio.

Arquitectónico:

Tier II:

- Protección mínima a eventos críticos.
- Puertas de seguridad.

Eléctrico:

Tier II:

- Posee redundancia N+1 a nivel de los componentes principales de respaldo de energía (UPS y gmg) y en el sistema de aire acondicionado.

• PDUs redundantes, preferiblemente alimentados de sistemas UPS separados.

• Los gabinetes y bastidores deben tener circuitos eléctricos dedicados de 20A/120V.

• El sistema de puesta a tierra del edificio debe ser diseñado y probado para proporcionar una impedancia a tierra de menos de 5 ohmios.

• Debe ser proporcionado un Emergency Power Off System (EPO).

Mecanico

Tier II:

• Incluye un aire acondicionado con la capacidad de refrigeración, para mantener la temperatura crítica y la humedad.

• Los sistemas de aire acondicionado deben cumplir 7 x 24 x 365 y deben contar con redundancia N+1.

• Todos los equipos de aire acondicionado deben accionarse por el sistema generador de reserva.

• Todos los sistemas de control de la temperatura deben ser alimentados a través de circuitos dedicados redundantes de la UPS.

• Un sistema de reserva a diesel debe ser instalado para proporcionar energía al sistema de suministro de alimentación ininterrumpida y equipos mecánicos.

VI. CONCLUSIONES

1. De acuerdo a los resultados, interpretados y analizados se logró describir el estado situacional del data center y quedando demostrado que el nivel de fiabilidad es baja, en consecuencia se sugiere la reestructuración o diseño de un Data Center bajo estándar TIA-942 para el EsSalud de Huaraz.

2. El diagnostico situacional del Data Center busca proporcionar al EsSalud Red Asistencial de Ancash – Huaraz, información sobre su estado actual del Data center lo cual ayudara a determinar la reestructuración del data center, volviéndolo competitivo dentro del mercado de las telecomunicaciones, puesto que se sugiere cumplir con normas internacionales para su diseño.

3. La interpretación de resultados coincidió con lo propuesto en la hipótesis general planteada en la investigación donde se planteó que el diagnostico situacional del data center determinara las mejoras y continuidad del servicio que brindan el data center de la EsSalud red asistencial de Ancash – Huaraz.

4. Con la descripción del diagnóstico situacional de Data center se logró identificar controles tanto de estandarización y normalización que se deben de tener en cuenta al planificar el diseño de un Data Center, lo cual ayudara a futuras investigaciones e implementación de un data center.

VII. RECOMENDACIONES

1. El presente proyecto de investigación propone el diseño del Data Center para el EsSalud de Huaraz, Mejorando su infraestructura de telecomunicaciones y posibilitando mejorar su nivel de fiabilidad y redundancia.
2. Al administrar e incorporar recursos del Data Center se lo debe realizar en forma ordenada respetando los lineamientos descritos por los estándares en sus diferentes subsistemas, de no llegar a la reestructuración, se deben de buscar solución que más se acerque a las recomendaciones de las diferentes normativas.
3. Es conveniente un registro adecuado del personal que ingresa al *Data Center* mediante el control de acceso, si bien la norma ANSI/TIA 942 no recomienda el uso de cámaras, se recomienda al menos la colocación de una videocámara para lograr un mayor control en la seguridad.
4. Se sugiere la incorporación de medidas de seguridad contra manazas naturales como Señalización y alumbrado de emergencia, protección contra fuegos, sistema de drenaje de agua, todo esto por estar siempre expuesto a múltiples amenazas.
5. Realizar una certificación del Data Center ya que los estándares lo recomiendan.

REFERENCIAS BIBLIOGRÁFICAS

1. Ministerio del Trabajo y Promocion del Empleo, Ministerio de Salud. Reorganización del Seguro Social de Salud-EsSalud Diagnostico y Propuestas. Diagnostico. Lima: Ministerio de Salud, Lima; 2013.

2. ADC Telecommunications. Cómo Diseñar un Centro de Datos Optimo. Informe Tecnico. USA: TE Connectivity, USA; 2005.

3. Coronel IGPV. Análisis de los requerimientos funcionales y de operacion para la implementacion del data center de la universidad nacional de Loja. Tesis. Cuenca: Universidad de Cuenca, Ecuador; 2010.

4. Ricardo Napoleon Guagalango Vega PEMM. Evaluación técnica de la seguridad informática del data center de la escuela politécnica del ejército. Tesis. Sangolqui: Universidad de las Fuerzas Armadas-ESPE, Ecuador; 2011.

5. Aroca JA. Problemas Estructurales y eficiencia energética en centros de datos. Tesis Doctoral. Madrid: Universidad Carlos III de madrid, España; 2015.

6. María Aguirre Patiño REPISGAAS. Diseño y Simulación de un Data Center Cloud Computing que cumpla con la norma PCI-DSS. Proyecto. Guayaquil: Escuela superior Politecnica del Litoral, Ecuador; 2011.

7. Yaselga Yaselga EH. Diseño del Centro de Datos para Petroecuador en el edificio matriz en base al Estándar TIA-942-2. Tesis. Quito: Escuela Politécnica Nacional, Ecuador; 2013.

8. Flores DCC. Data Center para mejorar la infraestructura de comunicacion de datos en el departamenteo de sistemas informaticos y redes de comunicación de la universidada tecnica de Ambato. Tesis Pre-grado. Ambatto: Universidad Tecnica de Ambato, Ecuador; 2012.

9. Freile Sandoval WF. Diseño y construcción de un módulo de monitoreo y control de suministro de energía eléctrica a un data center a través de la internet. Tesis. Quito: Escuela Politécnica Nacional, Ecuador; 2008.

10. Solís JEN. Procedimientos para la auditoría física y medio ambiental de un Data. Tesis. Lima: Pontificia Universidad la Catolica del Perú, Lima; 2013.

11. Nogueira Solis JE. Procedimientos para la auditoria fisica y medio ambiental de un Data Center basado el la clasificacion y estandad internacional TIER. TESIS. Lima: Pontificia Universidad Catolica del Perú, Ciencias e Ingenieria ; 2013.

12. Lopez Córdova LA. Diseño de red power over Ethernet con categoría 6ª para aplicación en data center. Tesis. Lima - Peru: Universidad Ricardo Parma, Facultad de Ingenieria; 2008.

13. Bologna J, Walsh A. The Accountant´s Handbook of Information. 1st ed. Sons Wa, editor. Mexico; 1997.

14. Garcia , Valcárcel A. Tecnología Educativa. Implicaciones educativas. Madrid: La Madrid; 2003.

15. SCHERTLER W. Virtual Enterprises in Tourism Viena: Springer Computer Science; 1999.

16. Belloch C. RECURSOS TECNOLOGICOS (TIC). Valencia España: Universidad de Valencia, Unidad de Tecnologia Educativa; 2008.

17. NEWS O. Los niveles Tier 3 y Tier 4. [Online].; 2015. Available from: HYPERLINK "https://www.ovh.es/servidores_dedicados/niveles-tier-3-4.xml" https://www.ovh.es/servidores_dedicados/niveles-tier-3-4.xml .

18. Uptime Insttitute. The Global Data Center Authority. [Online].; 2015. Available from: HYPERLINK "https://es.uptimeinstitute.com/about-ui/global-authority" https://es.uptimeinstitute.com/about-ui/global-authority .

19. Peñaloza Figueroa M. Standard TIA-942. Diseño y Cableado de un Centro de Datos. [Online].; 2007 [cited 2015 Diciembre 13. Available from: HYPERLINK "http://docplayer.es/960551-Standard-tia-942-diseno-y-cableado-de-un-centro-de-datos-disenar-en-base-a-estandares-y-mejores-practicas-temario.html"

http://docplayer.es/960551-Standard-tia-942-diseno-y-cableado-de-un-centro-de-datos-disenar-en-base-a-estandares-y-mejores-practicas-temario.html .

20. American National Standards Institute. ANSI/TIA-942 Norma de infraestructura de telecomunicaciones para centro de datos. Primera ed. EEUU; 2005.

21. Telecommunications Industry Association. Telecommunications Infrastructure Standard for Data Centers. Estandar de infraestuctura. Electronic Industries Alliance, Telecomunicciones; 2005.

22. ADC Krone - Telecommunications. TIA-942 Data Centre Standards Overview. Informe tecnico. ADC telecommunications; 2008.

23. Furukawa. Guía de Recomendaciones Para Data Center. [Online]. [cited 2015 Diciembre 12. Available from: HYPERLINK "http://www.furukawa.com.br/arquivos/g/gui/guia/1580_GuiadeRecomendacionesparaDataCenter.PDF" http://www.furukawa.com.br/arquivos/g/gui/guia/1580_GuiadeRecomendacionesparaDataCenter.PDF .

24. Ing. Joskowicz J. Cableado Estructurado. Informe. Montevideo: Universidad de la republica Montevideo, Uruguay; 2013.

25. Internacional Organization Standardization. Standards ISO. [Online]. [cited 2017 08 09. Available from: HYPERLINK "https://www.iso.org/standards.html" https://www.iso.org/standards.html .

26. Wikibook. Mejores prácticas para redes de datos/Infraestructura. [Online].; 2015 [cited 2017 10 1. Available from: HYPERLINK "https://es.wikibooks.org/wiki/Mejores_pr%C3%A1cticas_para_redes_de_datos/Infraestructura" \l "NORMA_606" https://es.wikibooks.org/wiki/Mejores_pr%C3%A1cticas_para_redes_de_datos/Infraestructura#NORMA_606 .

27. Duque Ochoa BR. Metodologias de Gestión de Riesgo. Informe. Colombia: Universidad del Caldas, Ingenieria ; 2012.

28. Consejo Superior de Administración Electrónica de España. Magerit 3.0 Metodologia de Análisis y Gestión de Riesgos de los Sistemas de Información. 30th ed. electronica A, editor. España: Ministerio de Hacienda y Administraciones Públicas ; 2012.

29. Hernandez R FCBP. Metodologia de la Investigacion 4ed. In Metodologia de la Investigacion. 4th ed. Mexico: McGraw - Hill Interamericana; 2006.

30. Paz DCd. Conceptos y Técnicas de Recolección de Datos en la Investigación. Lima: UNMSM, Facultad de Derecho; 2012.

31. PDCA. Check list/Lista de Chequeo: ¿Que es un checklist y como usarlo? [Online].; 2011 [cited 2017 09 27. Available from: HYPERLINK "http://www.pdcahome.com/check-list/" http://www.pdcahome.com/check-list/ .

32. Seguro Social de Salud Peú. EsSalud: 150 mil asegurados de Juliaca se beneficiarán del servicio de Telemedicina. [Online].; 2015 [cited 2015 Noviembre 15. Available from: HYPERLINK "http://www.essalud.gob.pe/essalud-150-mil-asegurados-de-juliaca-se-beneficiaran-del-servicio-de-telemedicina/" http://www.essalud.gob.pe/essalud-150-mil-asegurados-de-juliaca-se-beneficiaran-del-servicio-de-telemedicina/ .

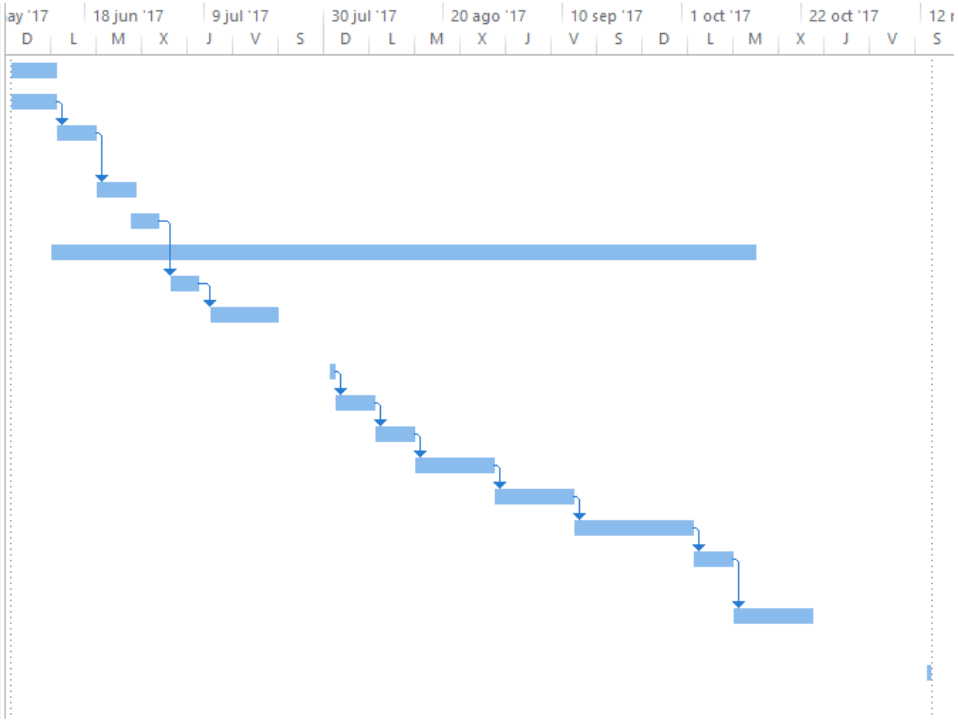
ANEXO

Anexo 01

Cronograma de Actividades

Proyecto de investigación: "Diagnostico situacional del data center bajo cumplimiento normativo y estándares en Hospital II EsSalud de Huaraz;"2017.

Modo de	Nombre de tarea	Duración	Comienzo	Fin
	Redaccion del Titulo	6 días	lun 5/06/17	lun 12/06/17
	Esquema del Proyecto	6 días	lun 5/06/17	lun 12/06/17
	Determinación del problema de estudio	5 días	mar 13/06/17	lun 19/06/17
	Objetivos del proyecto	5 días	mar 20/06/1	lun 26/06/17
	Justificación del Proyecto	5 días	lun 26/06/17	vie 30/06/17
	Revisión de bibliografia	90 días	lun 12/06/17	vie 13/10/17
	Elaboracion de marco teorico	5 días	lun 3/07/17	vie 7/07/17
	Elaboracion de instrumentos de medicion	10 días	lun 10/07/17	vie 21/07/17
	Presentacion del Proyecto	1 día	lun 31/07/17	lun 31/07/17
	Prueba de Instruementos	5 días	mar 1/08/17	lun 7/08/17
	Recoleccion de Datos	5 días	mar 8/08/17	lun 14/08/17
	Procesamiento de datos	10 días	mar 15/08/1	lun 28/08/17
	Análisis de datos	10 días	mar 29/08/1	lun 11/09/17
	Redaccion del informe fiinal	15 días	mar 12/09/1	lun 2/10/17
	Revision y correccion del borrador del informe final	5 días	mar 3/10/17	lun 9/10/17
	Transcripcion y entrega del trabajo final	10 días	mar 10/10/17	lun 23/10/17
	Sustentación del proyecto de investigacion	1 día	lun 13/11/17	lun 13/11/17



ANEXO N° 02

PRESUPUESTO:

PRESUPUESTO DEL PROYECTO	
Nombre del Proyecto:	DIAGNOSTICO SITUACIONAL DEL DATA CENTER BAJO CUMPLIMIENTO NORMATIVO Y DE ESTÁNDARES EN LA ESSALUD – RED ASISTENCIAL ÁNCASH FILIAL HUARAZ EN EL AÑO 2017
Localidad:	Huaraz
Ejecutor:	Bach. Ing. Tongo Evangelista, Yonen Yonel

Recursos: Materiales

DESCRIPCIÓN	CANTIDAD	UNIDAD	P.U. INCLUIDO IGV (0.18)	PRECIO TOTAL
Lapicero Faber-Castell	2	unidad	S/.0.50	S/.1.00
Papel bond Atlas A4 80 gr.	2	millar	S/.30.00	S/.60.00
Folder manila c/ faster	5	unidad	S/.0.80	S/.4.00
Plumón indeleble para pizarra	1	unidad	S/.5.00	S/.5.00
Resaltador Faber-Castell Textliner 48	1	unidad	S/.3.00	S/.3.00
Lápiz 2B	4	unidad	S/.1.00	S/.4.00
Grapas Artesco	1	Caja	S/.3.00	S/.3.00
Perforador Artesco	1	unidad	S/.4.50	S/.4.50
Tarjeta prepago movistar	2	unidad	S/.10.00	S/.20.00
Folder plastificado Artesco	2	unidad	S/.3.00	S/.6.00
Folder manila A4	4	unidad	S/.0.50	S/.2.00
Princo 4X DVD-R 4.7 GB	3	unidad	S/.1.50	S/.4.50
USB Kingston 4.0 GB	1	unidad	S/.5.00	S/.5.00
COSTO TOTAL (incluido IGV)				S/. 122.60

Recursos: Maquinas e impresiones

DESCRIPCIÓN	CANTIDAD	UNIDAD	P.U. INCLUIDO IGV (0.18)	PRECIO TOTAL
Servicio de alquiler PC	1	hora	S/.1.00 x hora	S/.120.00
Servicio de impresión	300	unidad	S/.0.10	S/.30.00
Servicio de fotocopia	120	unidad	S/.0.10	S/.12.00
Servicio de Internet	150	hora	S/.1.00	S/.150.00
Servicio de energía eléctrica	4	mes	S/.20.00	S/.80.00
Servicio de anillado y empastado	4	unidad	S/.2.50	S/.10.00
COSTO TOTAL (incluido IGV)				S/. 402.00

Recursos: Asesoramiento

RUBRO	CANTIDAD	COSTO	PRECIO TOTAL
Inscripción al curso de titulación	1	S/.150.00	S/.200.00
Asesoría tesis	1	S/.450.00 x mes	S/.1.500,00
Asesoría estadística	2	S/.120.00 x mes	S/.480.00
COSTO TOTAL			S/. 2 180,00

Recursos: Movilidad

TRANSPORTE	VECES	COSTO	PRECIO TOTAL
Servicio de Taxi	4	S/.3.50	S/.14.00
Servicio de Taxi colectivo	16	S/.0.80	S/.12.80
COSTO TOTAL			S/.26.80

TOTAL PRESUPUESTO	S/.2. 730,80

FINANCIAMIENTO

FINANCIAMIENTO	Recursos Propios

ANEXO N° 3

CHECKLIST

DIAGNÓSTICO SITUACIONAL DEL DATA CENTER

Proyecto: DIAGNOSTICO SITUACIONAL DEL DATA CENTER BAJO CUMPLIMIENTO NORMATIVO Y DE ESTÁNDAR EN EL HOSPITAL II ESSALUD HUARAZ EN EL AÑO 2017

Responsable: Bach. Yonen Yonel Tongo Evangelista **Fecha:** ……../……. /2017

***INTRUCCIONES PARA EL LLENADO DEL CHECK-LIST**

Marque con una "X" en las columnas "SI" o "NO", si dispone del elemento o cumple con lo especificado en la columna de "Requerimientos Técnicos".

Requerimientos Técnicos		Si	No	Observaciones
ubicación	La sala está Ubicada en un lugar libre de componentes que evitan la expansión de la misma tales como: ascensores, paredes exteriores, u otro edificio fijo			
	Cuenta con Accesibilidad para el suministro de equipos de gran tamaño.			
	La sala se encuentra lejos de fuentes de interferencia electromagnética.			
	Tiene ventanas exteriores.			
	Dispone de planos del edificio			
Acceso	La Puertas de acceso solo proporcionan entrada a personal Autorizado.			
	EL acceso cumple con los Requerimientos de la Autoridad competente.			
DISEÑO ARQUITECTÓNICO				
Tamaño	La sala de informática está dimensionada para satisfacer las necesidades conocidas de equipos específicos incluyendo espacios adecuados			
	Dimensionamiento incluye proyección a futuro, así como las necesidades actuales.			
	Existe un almacén fuera del centro de datos que permite guardar los repuestos, equipo nuevo, insumos, accesorios, y demás fuera de la sala principal.			
	Cuenta con una Zona para desempacar y probar equipos antes de ser Implementados.			
	La altura mínima en la sala de informática es de 2,6 m (8,5 pies) desde el piso terminado a cualquier obstrucción tal como rociadores, accesorios de iluminación, o cámaras.			

Altura de techo	Distancia mínima libre con los aspersores anti incendios de 0.46m (18”)			
	Suelo y Paredes están sellados para minimizar la entrada de polvo.			
	Los acabados deben son de un color claro para mejorar la iluminación ambiente			
Iluminación	Iluminación con un mínimo de 500 lux en el plano horizontal.			
	Iluminación con un mínimo de 200 lux en el plano vertical.			
	Los circuitos de Iluminación están separados.			
	Se cuenta con señalización y alumbrado de emergencia.			
Puertas	Las puertas tienen un mínimo de 1 m de ancho y 2,13 m de alto.			
	Abren hacia Afuera o son corredizas.			
	No tienen umbrales			
	Puertas Con cerraduras.			
	Las puertas son removibles para poder trasladar equipo adentro o afuera de la sala.			
	Existe una puerta de Emergencia			
Suelo	El Suelo tiene capacidad para soportar la carga distribuida y concentrada de acorde al equipo instalado junto con el cableado y medios asociados.			
	El mínimo de carga distribuida que debe soportar es de 7.2KPa (150lbf / ft Sqr)			
Señalización	Se ha desarrollado dentro del plan de seguridad del edificio			
	La señalización adecuada de salida está de acuerdo con la Autoridad Competente.			
	La edificaciones son antisísmicas			
Contaminantes	La habitación está protegido de contaminantes de acuerdo con ANSI / TIA569B. Polvo, estática, ruidos, interferencia.			
HVAC	El Cuarto de equipos tiene un sistema de climatización			
	El sistema de HVAC funciona las 24 horas del día los 356 días del año			
Protección contra incendios	Los sistemas de protección contra incendios y extintores portátiles cumplen con la norma NFPA75			
Infiltración de Agua	Para el riesgo de infiltración de agua se ha proporcionado un medio de evacuación			
	Existe un medio de evacuación o drenaje por cada 100 m^2			

	La habitación del centro de datos está lejos de cualquier tubería, desagüe u otro medio de filtración de agua.			
Parámetros operacionales	La temperatura y la humedad se controlan para proporcionar rangos de funcionamiento continuo			
	Cuenta con sistemas de aire acondicionado			
Baterías	Las Baterías utilizadas para Respaldo poseen ventilación adecuada y contención de derrames.			
DISEÑO ELÉCTRICO				
Poder	Los circuitos de alimentación son Independientes y poseen su propio pen o paneles eléctricos.			
	Posee tomacorrientes dúplex (220V) para conectar herramientas eléctricas, equipos de limpieza de forma independiente a los gabinetes con enchufes múltiples.			
	Se realiza el cambio automático hacia la unidad del generador o cuando ocurre un apagón			
	Cuenta con planos eléctricos del data center certificado por un ingeniero eléctrico.			
	Capacidad de combustible del generador a carga completa			
	Capacidad de UPS mínimo de 8min de no contar con generador			
	Las baterías utilizadas para respaldo poseen ventilación adecuada y contención de derrames.			
Conexión o puesta a tierra	El acceso está a disposición del sistema de puesta a tierra de telecomunicaciones especificado por ANSI / TIA / EIAJSTD607A.			
	La sala de ordenadores tiene una red de conexión común (CBN).			
	La Conexión a Tierra se encuentra conforme al estándar IEEE 1100 para la unión de las telecomunicaciones y equipo de cómputo.			
TELECOMUNICACIONES				
Colocación del equipo	Los equipos están instalados con la ingesta de frio de aire en la parte delantera del armario o un estante			
	Los equipos están instalados con el escape de aire caliente por la parte trasera del armario o un estante.			
Instalación de bastidores	Los bastidores están atornillados directamente al piso o algún soporte sísmico			
Pasillos Fríos y Calientes	Los armarios y bastidores respetan el patrón de ubicación para generar pasillos calientes y fríos.			
Gabinete y rack - altura	La altura máxima de la cabina es de 2,4 m (8Pies)			
	La profundidad del gabinetes o estantes es de 1.1m (43pulgadas)			
	Existe profundidad necesaria para la colocación del cableado, hardware de gestión de cables y enchufes múltiples.			

	El acabado de pintura de los gabinetes y rack son de pintura en polvo u otros resistentes a los arañazos			
	Los gabinetes y Racks están rotulados en la parte frontal y Trasera como lo indica en la norma ANSI/TIA 606			
	Existe Suficiente espacio interno para todos los equipos de Red, Conexiones eléctricas y espacios para redundancia			

CABLEADO DATA CENTER				
Topología	LA topología utilizada es en estrella			
Distancia	La distancia máxima del cableado es de 90m (295 pies) (cable de cobre)			
	LA distancia máxima incluyendo los cables de equipo son de 100m			
	Los cables de datos están separados de cables de alimentación de acuerdo al estándar TIA 942			
	Los cables de datos aéreos están sujetas por una bandeja de cables.			
Identificador de Cable	Los cables y Pach cords están Etiquetados en ambos extremos			
MECANICO				
	Tuberías de agua y desagüe no están asociados con el área del data center			
	Servicio eléctrico independiente al equipo mecánico			
	Posee un mecanismo de detección de humo			
	Cuenta con sistemas de luces de emergencias			
	Los Tomas corrientes que van a la pared cumplen con la distancia correcta del piso 30cm			
SEGURIDAD INFORMATICA				
	Posee una bitácora de ingreso al personal al data center			
	Dispone de un sistema de alarma, control o monitoreo del personal que ingresa al data center			
	Cuenta con políticas documentadas de responsabilidad y obligaciones de las personas que administran el data center			
	Para el Acceso del personal se cuenta con un sistema de autentificación			
	Cuenta con un inventario detallado de todo el equipo en el data center y comunicaciones			
	Elimina las contraseñas del personal que ya no trabaja en la organización			

	Los servicios cuentan con protección actualizada contra virus informático			
	Se cuenta con plan de respaldo al menos diario de todos los datos de los servidores			
	Cuenta con un plan de contingencia en caso de desastres			
	Los respaldos son actualizados constantemente			