ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACION Y VINCULACION

CON LA COLECTIVIDAD

MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS

II PROMOCIÓN

TESIS DE GRADO PRESENTADA PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS.

TEMA: "FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR BASADO EN MARCOS DE REFERENCIA DE TI"

AUTOR: LLERENA, CHRISTIAN ALONSO

DIRECTOR: NAVARRO, JAIRO RENÉ

SANGOLQUI, DICIEMBRE DE 2013

CERTIFICACION DEL DIRECTOR

Certifico que el presente trabajo titulado: "FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR BASADO EN MARCOS DE REFERENCIA DE TI", fue realizado en su totalidad por el Ingeniero Christian Alonso Llerena Villa, bajo mi supervisión.

_____

Ing. Jairo Navarro Bustos

Director de Tesis

DECLARACION

La Tesis de Grado titulada, "FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR BASADO EN MARCOS DE REFERENCIA DE TI", ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas e incorporadas en la bibliografía.

En virtud de esta declaración me responsabilizo del contenido, veracidad y alcance científico de esta tesis.

_____

Ing. Christian Alonso Llerena Villa

AUTORIZACION

Yo, Christian Alonso Llerena Villa, con CI: 1802625465, autorizo a la Universidad de las Fuerzas Armadas - ESPE, la publicación en la Biblioteca virtual, de la Tesis de mi autoría titulada "FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR BASADO EN MARCOS DE REFERENCIA DE TI", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

_____

Ing. Christian Alonso Llerena Villa

AGRADECIMIENTOS

Agradezco a Dios por darme la vida, la perseverancia y el optimismo para seguir adelante en todas las instancias de mi vida, por darme la dicha de tener una familia maravillosa y unos amigos muy valiosos.

Un agradecimiento muy especial al Ing. Jairo Navarro, Director de Tesis, por su incondicional apoyo y aporte profesional, también al Ing. Mario Ron Egas, Coordinador del Programa y al Ing. Luis Escobar, Oponente de la Tesis, quienes con sus recomendaciones han hecho posible la culminación de la presente tesis de grado.

Christian Alonso Llerena Villa

DEDICATORIA

A mi familia.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

En los últimos años el auge de los servicios tecnológicos y procesos automatizados que se realizan en las diferentes entidades públicas del Ecuador ha provocado una innegable necesidad en los departamentos de Tecnología de la Información de las mismas, de mantener disponibles dichos servicios y proteger adecuadamente la información que se almacena y procesa en todos los equipos que se utilizan para este fin. Ante esto se encuentra la creciente demanda de mitigar cualquier riesgo que pueda ocasionar la pérdida o la indisponibilidad de la información, entre estos riesgos se encuentra la evidente posibilidad de que ocurra una falla en la infraestructura física del lugar en el que se encuentran alojados los dispositivos encargados de prestar los servicios de TI. Es así que es de suma importancia realizar la verificación de los componentes de la infraestructura física de los Centros de Datos para evitar o minimizar la posibilidad de que un fallo en alguno de ellos produzca interrupciones en los servicios que brindan las unidades de Tecnología de la Información de las entidades del sector público del Ecuador, por lo que es de vital importancia para el Auditor Informático contar con una Guía, que le permita la revisión de dicha infraestructura de una manera eficiente y con el propósito de generar las debidas recomendaciones que garanticen que el Centro de Datos auditado este en capacidad de garantizar la disponibilidad de los servicios tecnológicos.

Palabras claves:

- Tecnología de la Información
- Centro de Datos
- Disponibilidad
- Guía de Auditoría
- Entidades públicas

CAPÍTULO I

FORMULACIÓN DE UNA GUÍA DE AUDITORIA PARA LA INFRAESTRUCTURA FÍSICA DE LOS CENTROS DE DATOS DE LAS ENTIDADES PÚBLICAS DEL ECUADOR BASADO EN MARCOS DE REFERENCIA DE TI

Mantener operativos los servicios de Tecnologías de la Información (TI), así como preservar, procesar y administrar eficientemente la información que se encuentra en los Centros de Datos o, Data Center, constituye uno de los retos más importantes que deben enfrentar los departamentos de TI, siendo la infraestructura física del Centro de Datos, que incluye el acondicionamiento eléctrico, mecánico, de telecomunicaciones, seguridad y diseño del mismo, un factor de suma importancia que influye en la tarea de garantizar la disponibilidad de la información y la continuidad de las operaciones.

En este contexto, la presente tesis se enmarca en la formulación de una Guía para auditar la infraestructura física de los Centros de Datos de las entidades públicas del Ecuador, la misma que será utilizada por los auditores de la Dirección de Auditoría de Tecnología de la Información de la Contraloría General del Estado y tiene como objetivo evaluar las instalaciones e infraestructura física de los Centros de Datos, con el uso de adaptaciones sugeridas en los marcos de referencia, estándares internacionales y buenas practicas relacionadas a mantener la continuidad de las operaciones de tecnología de la información.

Como paso preliminar, y debido a que cada una de las entidades públicas del Ecuador tiene diferentes objetivos, así como misión y visión distintas, se considera

de suma importancia que el Auditor de Tecnología realice un análisis del impacto que tiene la Tecnología de la Información en la entidad auditada para deducir el nivel de disponibilidad que debe tener su respectivo Centro de Datos. Para esto primeramente se elaborará un cuestionario, que tiene por objeto analizar la criticidad e impacto que representan los servicios de TI dentro de la entidad, el mismo que será desarrollado con las directrices de las principales normas y buenas prácticas de gestión de servicios tecnológicos y de gobierno de tecnología de la información. El resultado de este cuestionario permite determinar el impacto de TI dentro de cualquier entidad y por ende se desprende el nivel de disponibilidad requerido para el Centro de Datos, posteriormente se evaluará la infraestructura física con los parámetros establecidos en los marcos de referencia relacionados y que serán analizados para la formulación de la Guía.

Es así que la Guía constituye una herramienta que permite realizar todo el proceso de auditoría, del cual se obtendrá el respectivo nivel de madurez del Centro de Datos auditado, a partir del cual formularán las debidas conclusiones y recomendaciones que servirán para asegurar que su infraestructura física se encuentre en condiciones óptimas para asegurar la continuidad de las operaciones de la entidad y proteger los valiosos activos que se encuentran hospedados en el mismo.

1.1 Justificación e Importancia

Siendo el centro de datos el lugar que hospeda uno de los más valiosos e irremplazables activos que tiene una organización que es su información, se ha evidenciado la existencia de varias normas que describen los procedimientos para asegurar que el Centro de Datos proteja correctamente el hardware y otros dispositivos que se encuentren en el mismo. Es por tal razón que es de vital

importancia para los departamentos de Tecnología de la Información de cualquier entidad del sector público del Ecuador, mantener una adecuada infraestructura física en el Centro de Datos para asegurar la disponibilidad de los procesos y servicios de TI, y así evitar que cualquier tipo de evento no programado cause pérdidas en los ingresos, incumplimiento de las leyes y regulaciones vigentes, pérdida de imagen y en algunos casos incluso sanciones por no prestar los servicios a los usuarios dentro de los parámetros acordados. En tal virtud, surge la necesidad de verificar que las instalaciones físicas de los Centros de Datos se encuentren correctamente adecuadas para evitar que se produzcan interrupciones en los servicios por el descuido en el mantenimiento o por la mala adecuación de los elementos de tipo eléctrico, arquitectónico, mecánicos y de telecomunicaciones que conforman el mismo.

1.2 Planteamiento del problema

"Durante la última década, la energía y la refrigeración han pasado de ser ideas de último momento a ser las preocupaciones centrales en la construcción y funcionamiento de un Data Center" (Spera, 2012).

Bajo este tipo de apreciaciones se desprende que el descuido en el mantenimiento de la infraestructura física, así como el diseño incorrecto en la adecuación de los elementos que son por parte del centro de datos, comprometen y ponen en alto riesgo la continuidad de las operaciones de TI dentro de las entidades del sector público del Ecuador.

En vista de que las entidades del sector público del Ecuador están destinadas a realizar diversas actividades como petroleras, financieras, administrativas, educación, militares, gobierno; se determina que el nivel de criticidad de las operaciones de cada una de las entidades varía dependiendo de sus objetivos. Con

este antecedente es de suma importancia para la Contraloría General del Estado, que es el Organismo Técnico encargado del control de la utilización de los recursos estatales y la consecución de los objetivos de las instituciones del Estado, realizar auditorías informáticas que ayuden a prevenir que las entidades públicas paralicen o interrumpan sus servicios por fallas en la operación de sus centros de datos, afectando directamente a la disponibilidad de la información, necesaria para el cumplimiento de sus funciones y el logro de sus objetivos.

Para realizar la respectiva evaluación, es menester que el auditor informático cuente con una guía que permita una rápida respuesta a las interrogantes que se presentan al momento de realizar la auditoría, en consecuencia, la guía tiene por objeto ayudar al desarrollo de su trabajo ya que constituye una fuente de consulta y orientación en temas puntuales; y que servirán de referencia y fundamento en la ejecución de la auditoría, por lo que es necesario que este documento incluya la normativa vigente y los fundamentos teóricos tales como normas, estándares y buenas practicas relacionados con el objetivo de la acción de control y que servirán de sustento para realizar las recomendaciones necesarias para establecer un parámetro adecuado en la operación de los Centros de Datos de cualquier entidad pública del Ecuador.

1.3 Formulación del Problema

El centro de datos o *data center* es el sitio principal en donde se encuentra hospedado el hardware que realiza el procesamiento y almacenamiento de la información, la misma que es generada y utilizada en cada una de las entidades públicas del Ecuador para el cumplimiento de sus objetivos, la realización de una auditoría informática a la infraestructura física de los centros de datos sirve para

asegurar que dicha infraestructura proteja correctamente a los dispositivos de hardware, previniendo así las interrupciones en la prestación de servicios tecnológicos.

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar una Guía con los procedimientos para auditar la infraestructura física de los centros de datos de las entidades públicas del Ecuador que permita evaluar su diseño e implementación acorde a los principales marcos de referencia.

1.4.2 Objetivos específicos

- Realizar un análisis de los principales marcos de referencia utilizados a nivel mundial para el diseño y construcción de un Centro de Datos.
- Analizar las Normas de Control Interno expedidas por la Contraloría General del Estado y establecer las relaciones con los estándares relacionados con la infraestructura del Centro de Datos para sustentar la base legal de las acciones de control.
- Determinar el nivel de disponibilidad requerido en el Centro de Datos auditado, en base al impacto de TI dentro de la entidad con el respectivo análisis de riesgos.
- Definir los procedimientos para realizar pruebas específicas del estado del acondicionamiento físico de los Centros de Datos.

- Establecer los niveles de madurez de los Centros de Datos en relación los marcos de referencia de TI involucrados.

- Generar las recomendaciones necesarias para que el Centro de Datos auditado obtenga un nivel aceptable de tolerancia a fallas acorde al nivel de disponibilidad requerido.

CAPITULO II

2. Marco Teórico

2.1 Estándar TIA 942

La norma TIA-942 es un estándar que describe los requerimientos que deben ser considerados para implementar la infraestructura de un Centro de Datos. Se divide en cuatro subsistemas que son:

- Telecomunicaciones
- Arquitectura
- Sistema Eléctrico
- Sistema Mecánico

Este estándar que en sus orígenes se basa en una serie de especificaciones para comunicaciones y cableado estructurado, planteó la necesidad de evaluar los centros de datos sobre los subsistemas de infraestructura generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar.

El estándar TIA 942 y la categorización de Tiers se encuentran en pleno auge en América Latina. Esto es bueno porque lleva al replanteo de las necesidades de infraestructura de una manera racional y alineada con las necesidades propias de disponibilidad del negocio en que se encuentran las organizaciones. (El estandar TIA 942, 2007)

2.2 Estándar TIER

El TIER de un Datacenter (CPD, Centro de Procesamiento de Datos) es una clasificación ideada por el Uptime Institute que se plasmó en el estándar ANSI/TIA-942 y que básicamente establece 4 categorías, en función del nivel de redundancia de los componentes que soportan el Datacenter. (Clasificación TIER en el Data Center, 2012)

Las características básicas de cada uno de los niveles son:

- TIER I: Centro de datos Básico

Disponibilidad del 99.671%.

- TIER II: Centro de datos Redundante

Disponibilidad del 99.741%.

- TIER III: Centro de datos Concurrentemente mantenibles

Disponibilidad del 99.982%.

- TIER IV: Centro de datos Tolerante a fallos

Disponibilidad del 99.995%.

2.3 Normas de Control Interno expedidas por la Contraloría General del Estado

Las Normas de Control Interno, expedidas por la Contraloría General del Estado, tienen por objeto propiciar con su aplicación, el mejoramiento de los sistemas de control interno y la gestión pública, en relación a la utilización de los recursos estatales y la consecución de los objetivos institucionales, las normas de control interno desarrolladas incluyen: normas generales y otras específicas

relacionadas con la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos y recogen la utilización del marco integrado de control interno emitido por el Comité de Organizaciones que patrocina la Comisión Treadway (COSO), que plantea cinco componentes interrelacionados e integrados al proceso de administración, con la finalidad de ayudar a las entidades a lograr sus objetivos. En su estructura consta el grupo de normas 410 Tecnología de la Información, (Contraloría General del Estado, 2010)

2.4 ITIL versión 3

ITIL (Biblioteca de infraestructura de Tl) es una serie de publicaciones exhaustivas y consistentes que se utilizan para describir y optimizar un marco de trabajo para la Gestión de calidad de Servicio Tl dentro de una organización, alineado con el Standard internacional, ISO/IEC 20000 y contiene las siguientes publicaciones:

- Estrategia de Servicio
- Diseño de Servicio
- Transición de Servicio
- Operación de Servicio
- Mejoramiento Continuo de Servicio

Las publicaciones antes mencionadas definen el ciclo de vida del servicio por lo cual cada una de sus fases contiene sus respectivas funciones y procesos (el detalle de las funciones y procesos consta en el libro de ITIL). Las fases tienen las siguientes finalidades (ServiceTonic, 2011):

2.4.1 Estrategia del Servicio

La estrategia del Servicio promueve la visión de la gestión del servicio como un activo estratégico, y no sólo como una capacidad de la organización.

Las organizaciones usan la estrategia como una orientación en los siguientes aspectos:

- Identificar, seleccionar y priorizar oportunidades de negocio.
- Crear aspectos distintivos respecto de la competencia que refuercen el posicionamiento en el mercado.
- Asegurar que la organización es capaz de soportar el coste y el riesgo asociados a su catálogo de servicios.
- Mejorar la alineación de las capacidades de gestión de los Servicios con las estrategias de negocio.
- Preguntarse qué servicios deben implementarse y por qué antes de preguntarse el cómo hacerlo.

2.4.2 Diseño del Servicio

En este libro ITIL proporciona los principios de diseño y los métodos necesarios para convertir los objetivos de negocio estratégicos en un catálogo de servicios con sus activos asociados.

El principal objetivo del Diseño del servicio es diseñar los servicios nuevos o modificados, de forma alineada con los objetivos de negocio establecidos en la Estrategia del Servicio, para incorporarlos al Catálogo de Servicios e implantarlos posteriormente en producción.

2.4.3 Transición del Servicio

El principal objetivo de la etapa de Transición del Servicio es la implantación de los Servicios nuevos o modificados con el mínimo impacto para el negocio y dentro de los parámetros previstos de coste, tiempo y calidad.

2.4.4 Operación del Servicio

La Operación del Servicio es la fase en la que realmente los servicios aportan valor al negocio y donde los planes, diseños y mejoras del Ciclo de Vida del Servicio son ejecutados y evaluados.

La operación del Servicio se encarga de realizar todas las actividades necesarias para la prestación y el soporte de los servicios. Asimismo, es la fase que principalmente nutre de información a la fase de Mejora Continua del Servicio.

2.4.5 Mejora Continua del Servicio

El principal objetivo de la Mejora Continua del Servicio es alinear y realinear los servicios con las necesidades cambiantes de negocio identificando e implementando mejoras.

Son ámbitos de esta fase el resto de fases del ciclo de vida de un servicio, ya que son susceptibles de mejora tanto la estrategia, como el diseño, como la transición, como la operación de los servicios.

El ciclo de Deming: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act) constituye la columna vertebral de todos los procesos de mejora continua:

Planificar: establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado.

Hacer: implementar las mejoras planificadas. Si es posible, en una pequeña escala.

Verificar: pasado un periodo de tiempo previsto de antemano, recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora esperada.

Actuar: en función del resultado de la fase de verificación.

2.5 Cobit v4.1

COBIT alcanza un más agudo enfoque de negocios mediante el alineamiento de TI con los objetivos del negocio. La medición del desempeño de TI se debe basar en cuanto ésta posibilite y extiende la estrategia del negocio. El marco de referencia de COBIT fue creado con las siguientes características principales (ISACA, 2013):

- Enfoque al negocio
- Orientación a procesos
- Basado en riesgos y controles
- Apoyado por indicadores

COBIT describe el ciclo de vida de TI mediante la definición de cuatro Dominios:

- Planificación y Organización (PO)
- Adquisición e implementación (AI)

- Entrega de servicios y soporte (DS)
- Monitoreo y Evaluación (ME)

Cada uno de los Dominios listados contiene sus respectivos procesos, los mismos que son una serie de actividades con quiebres de control naturales. Los procesos especifican lo que el negocio necesita para alcanzar sus objetivos. La entrega de información es controlada por medio de 34 procesos de TI.

Las Actividades son aquéllas acciones que se requiere hacer para alcanzar resultados medibles. Además, las actividades tienen un ciclo de vida e incluyen tareas discretas.

2.6 Análisis de Impacto en el Negocio BIA

El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA, (*Business Impact Análisis*) es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un Plan de Continuidad del Negocio, el mismo que se enmarca en el sistema de gestión de continuidad de negocio y alineado con la norma ISO 22301.

De acuerdo al *Business Continuity Institute* se tienen cuatro objetivos principales al realizar un análisis de impacto:

CRÍTICOS

• Funciones que pueden realizarse sólo si las capacidades se reemplazan por otras idénticas.

• No pueden reemplazarse por métodos manuales.

• Muy baja tolerancia a interrupciones.

VITALES

• Pueden realizarse manualmente por un periodo breve.

• Costo de interrupción un poco más bajos, sólo si son restaurados dentro de un tiempo determinado (5 o menos días, por ejemplo).

SENSITIVOS

• Funciones que pueden realizarse manualmente por un periodo prolongado a un costo tolerable.

• El proceso manual puede ser complicado y requeriría de personal adicional.

NO CRITICOS

• Funciones que pueden interrumpirse por tiempos prolongados a un costo pequeño o nulo.

Adicionalmente se incluye dentro del Análisis de Impacto al Negocio, otro estudio que es importante para la identificación de los riesgos a los que se encuentran expuestos los Centros de Datos, por lo cual se indican a continuación los pasos para el Análisis de Riesgos.

2.6.1 Estudio de Riesgos en un Centro de Datos

El estudio de riesgos es una parte fundamental en la Guía de Auditoría, ya que el mismo va a permitir identificar las amenazas a las que se encuentran expuestos los Centros de Datos y valorar el impacto que supondría en las entidades públicas del Ecuador la materialización de dichas amenazas. En primer lugar conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la entidad. Se debe tener en cuenta que existe gran cantidad de incidentes relacionados con la seguridad de los

sistemas de información que comprometen los activos de las entidades, estas amenazas siempre han existido, por lo que toda entidad pública debe estar alerta a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo (Guagalango Ricard, 2011).

El análisis de riesgos informáticos es un proceso que engloba la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas.

Para el Análisis de Riegos se toma en cuenta las directrices del estándar ISO 27001, para lo cual es necesario primeramente definir los principales conceptos a tratar en el estudio de riesgos los mismos que son:

- Amenaza: Es la causa potencial de un daño o perjuicio a un activo.
- Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.
- Impacto: consecuencias de que la amenaza ocurra.
- Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.
- Salvaguarda: Medida técnica u organizativa que ayuda a paliar el riesgo.
- Riesgo residual: Riesgo remanente tras la aplicación de salvaguardas.

Con los conceptos indicados se debe mencionar que existen varias guías y metodologías que buscan hacer más objetivo el Análisis de Riesgos, entre los cuales constan Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), ISO 27005, Octave (Metodología de Análisis y Gestión de Riesgos *Operationally Critical Threat, Asset, and Vulnerability Evaluation)*, entre otras, de las cuales se realiza un ajuste según los requerimientos particulares para la Auditoría

de un Centro de Datos, por lo que se definen las siguientes actividades o fases principales para el presente análisis de riesgos (Chamorro, 2013):

- Identificación de Activos

  Se identifican los activos que se encuentran dentro del alcance definido, en este caso de identificaran los activos físicos que se encuentran hospedados en el Centro de Datos, los mismos que pueden ser computadores, medios magnéticos, equipos de hardware, etc.

- Identificación de los requerimientos legales y comerciales

  Al momento de identificar los activos físicos, se debe analizar los requerimientos contractuales de los activos para saber si existe algún requerimiento legal o comercial sobre los mismos y si otros activos dependen de estos.

- Tasación de Activos

  La tasación de activos se realiza bajo la afectación que produce la falla o pérdida de un activo en términos de confidencialidad, integridad y disponibilidad.

- Identificación de Amenazas y Vulnerabilidades

  La identificación de amenazas y vulnerabilidades se realiza en función de la naturaleza del activo, y se los clasifica según sea el caso en varios grupos como por ejemplo:

Tabla 1. Clasificación de Amenazas

Amenaza	Ejemplo de Amenaza
Instalaciones	Fuego, explosión, pérdida de energía, falla mecánica, daño por agua, etc.
Natural	Inundaciones, maremotos, sismos, tormentas, etc.
Sociales	Vandalismo, motines, protestas, sabotaje, etc.

Elaborado por: Christian Alonso Llerena Villa

- Cálculo de Amenazas y Vulnerabilidades.

Una vez que determinadas las amenazas y vulnerabilidades es necesario calcular la posibilidad de que puedan causar un riesgo. El cálculo se realizar en base a las amenazas deliberadas, accidentales, incidentes pasados y nuevas tendencias.

Posterior al Análisis de Riegos se realiza la Evaluación de Riesgos, el mismo que comprende las siguientes fases:

- Cálculo de Riesgo de Activos de Información

  El cálculo de riesgo de activos identifica y da prioridad a los riesgos basado en su impacto y su probabilidad de ocurrencia.

  Riesgo= Probabilidad x Impacto

- Evaluación de la prioridad de los riesgos
  La evaluación de la prioridad de los riesgos se realiza de acuerdo al siguiente criterio:

  Impacto económico del riesgo.
  Tiempo de Recuperación de la entidad.
  Posibilidad real de ocurrencia del riesgo.
  Posibilidad de interrumpir las actividades de la empresa.

- Informe de Medición de los Riesgos

  Se define el nivel de riesgo admisible y se decide las acciones a tomar con los activos involucrados con el uso de guía, estándares o normas relacionadas.

2.7 Norma ISO 27002 Seguridad Física y del Entorno

Es el estándar que contiene las directrices y los principios generales para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información dentro de una organización. La norma también pretende proporcionar una guía para el desarrollo de normas de seguridad de la organización y las prácticas eficaces de gestión de seguridad, por lo que describe un gran número de controles y sus respectivos mecanismos de control a ser implementados en los sistemas de gestión de seguridad de la información. (The ISO 27000 Diretory, 2008).

CAPÍTULO III

3. Desarrollo de un cuestionario para determinar el nivel de disponibilidad requerido en un Centro de Datos y Análisis de Riesgos

Para la formulación de la Guía para Auditar la Infraestructura Física de los Centros de Datos de las Entidades Públicas del Ecuador, primeramente es necesario elaborar un cuestionario que determinará un nivel de disponibilidad requerido en el Centro de Datos a ser auditado, este antecedente de suma importancia ya que la auditoría se realizará en base al cumplimiento de los requerimientos sugeridos en el estándar TIA 942, la misma que establece 4 tipos de Centros de Datos ideados por el estándar TIER, relacionados con la disponibilidad que están en capacidad de garantizar cada uno de ellos; esta disponibilidad ese encuentra sujeta a la redundancia de los componentes de su infraestructura, esto quiere decir que es necesario saber cuan disponible debe estar el centro de datos según los procesos de TI que se ejecutan.

En base a los marcos de referencia relacionados utilizados a nivel mundial, tales como ITIL, Cobit y BIA (Análisis de Impacto al Negocio o *Business Impact Análisis*) , se elaborará un cuestionario que será una herramienta del Auditor y que le permitirá determinar el nivel de contribución que tiene el área de TI, y por ende se determinará el tipo de Centro de Datos que requiere cada una de las entidades públicas del Ecuador.

Para la realización de este cuestionario se considera en primer lugar la naturaleza de la entidad auditada, por lo que es necesario definir las variables prioritarias que servirán para definir la influencia que tiene el Centro de Datos en las

actividades y procesos que realiza la entidad, cabe indicar que existen diversidad de entidades públicas que mantienen infraestructuras de Centro de Datos completamente diferentes que pueden ser catalogados como Centros de Datos de alta disponibilidad; pero se debe considerar que ese concepto es una interpretación subjetiva de disponibilidad ya que está sujeta al tipo de negocio y objetivos que persigue cada entidad.

Para la identificación de las variables que hacen posible la conformación del cuestionario se utilizaran los parámetros y conceptos propios de los estándares anteriormente citados en el marco teórico, tales como COBIT, ITIL y BIA. Adicionalmente se considera la utilización de las recomendaciones realizadas por el *UPTIME INSTITUTE* para la categorización de los Centros de Datos de acuerdo al tipo de negocio o actividad que realiza la organización. Una vez realizado el cuestionario para determinar el nivel de disponibilidad requerido, se procederá a realizar un análisis del principal estándar utilizado para la implementación de la infraestructura física en un Centro de Datos.

3.1 Identificación de variables y definición del cuestionario

Primeramente se ha considerado el uso de un cuestionario basado en los lineamientos que se indican para realizar el Análisis de Impacto al Negocio, cabe indicar que el BIA es el documento base de todo Plan de Continuidad del Negocio, ya que está orientado a determinar cuáles son los procesos o áreas esenciales para la continuidad de las operaciones y calcular su posible impacto, definición que se considera de vital importancia para determinar el nivel de disponibilidad que debe tener el Centro de Datos, sin estar condicionado a un Plan de Continuidad del

Negocio, puesto que el objetivo principal de la presente tesis es realizar una auditoría a las instalaciones físicas.

Los Análisis de Impacto son elaborados considerando los peores escenarios que se pueden presentar en una organización, sin embargo al ser el propósito principal identificar los procesos críticos de la entidad para establecer su relación con la operación del Centro de Datos, se procede a identificar aspectos como: la cantidad de usuarios internos y externos, la cantidad de procesos de TI que afecten al cumplimiento de los objetivos de la entidad, los tiempos máximos de recuperación, entre otros.

Se considera también que las actividades normalmente relacionadas al desarrollo de un Análisis de Impacto son:

• Procesos críticos del sistema

• Dependencias

• Impacto sobre las operaciones

• Determinar los tiempos de recuperación óptimos para los procesos críticos

Por otro lado también se incluye una categorización de los Impactos, entre los cuales se constatan los siguientes efectos:

- Pérdida de Ingresos
- Gastos Adicionales
- Aspectos Regulatorios y Legales
- Servicio al cliente

- Imagen

Bajo las categorías antes mencionadas se procede a elaborar un cuestionario de Análisis de Impacto al Negocio, que se unirán a las métricas del análisis de Cobit, y que darán como resultado el nivel de disponibilidad requerido para el Centro de Datos a ser auditado.

Con las premisas antes mencionadas se concluye entre las principales preguntas del cuestionario de Análisis de Impacto al Negocios, las siguientes interrogantes:

- Cantidad de procesos desarrollados por la Entidad
- Cantidad de procesos que se realizan en la unidad de Tecnología de la Información
- Frecuencia en la que se realizan los procesos de Tecnología
- Cuál es el principal impacto que se genera si se detienen los procesos de Tecnología de la Información
- Son los procesos dependientes de algún proveedor externo para su completa entrega.
- Cuál es el periodo máximo que el proceso del negocio puede estar no disponible.

Una vez que por medio del Análisis de Impacto al Negocio se han definido las preguntas para identificar la criticidad de TI en una entidad, se procede a complementar el cuestionario con el marco de referencia COBIT 4.1, tal como se detalló en el capítulo I, el marco de referencia tiene como objeto promover un marco

de gobierno de TI, por lo cual se ha considerado de vital importancia adicionar aspectos propios de los procesos y las métricas que se proponen en los dominios de Cobit, con el propósito de conocer de mejor manera la influencia y el alineamiento que tiene el área de Tecnología de la Información con los objetivos y metas de la entidad.

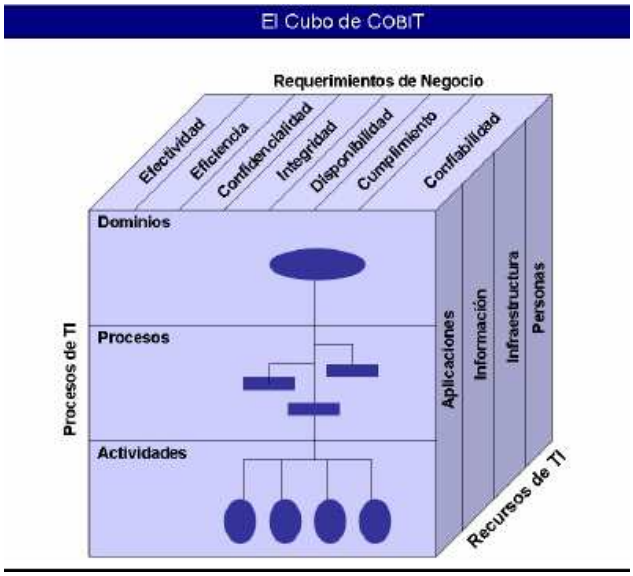

Figura 1. El cubo de Cobit
Fuente: Cobit 4.1

Inicialmente se toma como punto de partida el Cubo de Cobit, dado que Cobit propone un modelo que organiza las actividades de TI en 34 procesos que corresponden a 4 dominios, a su vez cada proceso cuenta con controles a ser implementados los cuales contienen sus respectivas métricas. Cabe recalcar que los dominios que forman parte de Cobit 4.1 y la cantidad de procesos que contiene cada uno de ellos se muestran en la siguiente tabla:

Tabla 2. Dominios y Procesos de Cobit

Dominio	Iniciales	Cantidad de Procesos
Planear y Organizar	PO	10
Adquirir e Implementar	AI	7
Entregar y Dar Soporte	DS	13
Monitorear y Evaluar	ME	4

Elaborado por: Christian Alonso Llerena Villa

En vista de que toda entidad pública del Ecuador, administra, procesa y genera información, la misma que es útil para lograr sus objetivos, se procede a utilizar cada uno de los Procesos de TI, los Criterios de la Información y los Recursos de TI que tienen relación directa con la funcionalidad y operación del Centro de Datos.

En consecuencia se procede a establecer la relación entre los procesos que constan en cada uno de los dominios antes mencionados con los Criterios de la Información, los mismos que son: Efectividad, Eficiencia, Confidencialidad, Integridad, Disponibilidad, Cumplimiento y Confiabilidad; tomando en cuenta la naturaleza del Centro de Datos, se ha considerado que el principal Criterio de la Información relacionado al funcionamiento del centro de datos es la Disponibilidad. Refiriéndose como Disponibilidad, a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas. (Isaca, 2007).En tal virtud se realiza un filtrado de todos los procesos relacionados con la Disponibilidad, los mismos que se encuentran previamente definidos en Cobit. Cabe indicar que todos los procesos seleccionados serán analizados por igual, independientemente de que se muestran clasificados con una “P” cuando la Disponibilidad es un objetivo primario de ese proceso y con una “S” si es un objetivo secundario. Adicionalmente se debe indicar que las dos primeras letras seguidas de un número que constan antes del nombre del proceso, se deben al nombre del dominio y al número del proceso.

Tabla 3. Relación de procesos de Cobit con la Disponibilidad de la Información.

Dominio	Procesos	Criterio de la Información= Disponibilidad
PLANEAR Y ORGANIZAR	PO1 Definir un Plan Estratégico de TI	
	PO2 Definir la Arquitectura de la Información	
	PO3 Determinar la Dirección Tecnológica	
	PO4 Definir los Procesos, Organización y Relaciones de TI	
	PO5 Administrar la Inversión en TI	
	PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia	
	PO7 Administrar Recursos Humanos de TI	
	PO8 Administrar la Calidad	
	PO9 Evaluar y Administrar los Riesgos de TI	P
	PO10 Administrar Proyectos	
ADQUIRIR E IMPLEMENTAR	AI1 Identificar soluciones automatizadas	
	AI2 Adquirir y mantener software aplicativo	
	AI3 Adquirir y mantener infraestructura tecnológica	S
	AI4 Facilitar la operación y el uso	S
	AI5 Adquirir recursos de TI	
	AI6 Administrar cambios	P
	AI7 Instalar y acreditar soluciones y cambios	S
ENTREGAR Y DAR SOPORTE	DS1 Definir y administrar los niveles de servicio	S
	DS2 Administrar los servicios de terceros	S
	DS3 Administrar el desempeño y la capacidad	S
	DS4 Garantizar la continuidad del servicio	P
	DS5 Garantizar la seguridad de los sistemas	S
	DS6 Identificar y asignar costos	
	DS7 Educar y entrenar a los usuarios	
	DS8 Administrar la mesa de servicio y los incidentes	
	DS9 Administrar la configuración	S
	DS10 Administrar los problemas	S
	DS11 Administrar los datos	
	DS12 Administrar el ambiente físico	P
	DS13 Administrar las operaciones	S
MONITOREAR Y EVALUAR	ME1 Monitorear y Evaluar el Desempeño de TI	S
	ME3 Garantizar el Cumplimiento Regulatorio	

Elaborado por: Christian Alonso Llerena Villa

En cuanto a los Recursos de TI, los mismos que son: las Aplicaciones, la Información, la Infraestructura y las Personas; al ser la Infraestructura de los Centros de Datos, el objetivo principal de la Guía de Auditoría, se analiza en la tabla N° 4 y se comprueba que todos los Procesos que están relacionados con la Disponibilidad, influyen sobre la Infraestructura.

Tabla 4. Relación de procesos de Cobit con la Disponibilidad e Infraestructura.

Procesos	Criterio de la Información= Disponibilidad	Aplicaciones	Información	Infraestructura	Personas
PO9 Evaluar y Administrar los Riesgos de TI	P			x	
AI3 Adquirir y mantener infraestructura tecnológica	S			x	
AI4 Facilitar la operación y el uso	S			x	
AI6 Administrar cambios	P			x	
AI7 Instalar y acreditar soluciones y cambios	S			x	
DS1 Definir y administrar los niveles de servicio	S			x	
DS2 Administrar los servicios de terceros	S			x	
DS3 Administrar el desempeño y la capacidad	S			x	
DS4 Garantizar la continuidad del servicio	P			x	
DS5 Garantizar la seguridad de los sistemas	S			x	
DS9 Administrar la configuración	S			x	
DS10 Administrar los problemas	S			x	
DS12 Administrar el ambiente físico	P			x	
DS13 Administrar las operaciones	S			x	
ME1 Monitorear y Evaluar el Desempeño de TI	S			x	
ME2 Monitorear y Evaluar el Control Interno	S			x	
ME4 Proporcionar Gobierno de TI	S			x	

Elaborado por: Christian Alonso Llerena Villa

Una vez que se han relacionado los Procesos, Criterios de la Información y Recursos de TI, se procede a analizar cada una de las métricas que contiene cada uno de los procesos involucrados en el marco de referencia para definir las preguntas que formarán parte del cuestionario que permitirá establecer el nivel de disponibilidad requerido en el Centro de Datos que será auditado. Cabe indicar que se analizan cada una de las métricas en base a las metas de TI, de los procesos y de las actividades.

Las métricas que se indican en cada uno de los procesos se obtienen del análisis de cada uno de ellos, considerando aquellas que contribuyan al propósito de determinar el impacto de TI en la entidad:

PO9 EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

- Porcentaje de eventos críticos de TI identificados que han sido evaluados.
- Número de riesgos de recientemente identificados.
- Número de incidentes significativos causados por riesgos no identificados por el proceso de evaluación de riesgos.

AI3 ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLÓGICA

- Número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será).
- Número de plataformas de tecnología distintas por función en la empresa.

AI4 FACILITAR LA OPERACIÓN Y EL USO

- Número de aplicaciones en las que los procedimientos de TI se integran de forma continua dentro de los procesos del negocio.

AI6 ADMINISTRAR CAMBIOS

- No se considera que las métricas de este proceso aporten al cuestionario.

AI7 INSTALAR Y ACREDITAR SOLUCIONES Y CAMBIOS

- Porcentaje de interesados satisfechos con la integridad de los datos de los nuevos sistemas.

- Llamadas de usuarios servicio de usuarios debidas a entrenamiento inadecuado.

DS1 DEFINIR Y ADMINISTRAR LOS NIVELES DE SERVICIO

- Establecer un entendimiento común de los niveles de servicio requeridos.

- Porcentaje de interesados del negocio satisfechos de que los servicios entregados cumplen con los niveles de servicio acordados.

- Porcentaje de usuarios satisfechos de que los servicios entregados cumplen con los niveles de servicio acordados.

- Porcentaje de servicios entregados que no están en el catálogo.

- Porcentaje de servicios que cumplen con los niveles de servicio.

DS2 ADMINISTRAR LOS SERVICIOS DE TERCEROS

- Número de quejas de los usuarios debidas a los servicios contratados.
- Porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicio.
- Nivel de satisfacción del negocio con comunicación efectiva por parte del Proveedor.

DS3 ADMINISTRAR EL DESEMPEÑO Y LA CAPACIDAD

- Número de procesos de negocio críticos no cubiertos por un plan definido de disponibilidad de servicios.

DS4 GARANTIZAR LA CONTINUIDAD DEL SERVICIO

- Número de procesos críticos del negocio que dependen de TI no cubiertos por un plan de continuidad.

DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS

- No se considera que las métricas de este proceso aporten al cuestionario.

DS9 ADMINISTRAR LA CONFIGURACIÓN

- No se considera que las métricas de este proceso aporten al cuestionario.

DS10 ADMINISTRAR LOS PROBLEMAS

- No se considera que las métricas de este proceso aporten al cuestionario.

DS12 ADMINISTRAR EL AMBIENTE FÍSICO

- Tiempo sin servicio ocasionado por incidentes del ambiente físico.

DS13 ADMINISTRAR LAS OPERACIONES

- Número de activos de hardware incluidos en los programas de mantenimiento preventivo.

ME1 MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI

- Porcentaje de procesos críticos monitoreados

ME2 MONITOREAR Y EVALUAR EL CONTROL INTERNO

- No se considera que las métricas de este proceso aporten al cuestionario

ME4 PROPORCIONAR GOBIERNO DE TI

- No se considera que las métricas de este proceso aporten al cuestionario.

Con las métricas obtenidas se procederá a consolidar en un solo cuestionario las preguntas necesarias para que el Auditor Informático pueda determinar el impacto y criticidad de TI en la entidad y por ende la disponibilidad que debe tener su respectivo Centro de Datos.

En vista de que se propone un cuestionario basado en los marcos de referencia de TI, también es necesario tomar en cuenta las buenas prácticas de ITIL, en virtud de que este marco de referencia provee un conjunto de directrices para la

Gestión de Servicios en las organizaciones, por lo que es necesario analizar el mismo con el propósito de identificar posibles variables adicionales que contribuyan al cuestionario. Para esto, primeramente se hace el siguiente mapeo entre los procesos previamente seleccionados de Cobit, hacia ITIL v3.Se debe tomar en cuenta que debido a su alto nivel, a la amplia cobertura y porque está basado en muchas prácticas existentes, frecuentemente se refiere a COBIT como un 'integrador', ubicando diferentes prácticas bajo un solo paraguas, (Institute, 2008), ya que ayuda a enlazar varias prácticas de TI con los requerimientos del negocio. En consecuencia se utiliza el documento denominado Alineando Cobit 4.1, ITIL v3 e ISO 27002 en beneficio de la empresa, para determinar el mapeo de los procesos involucrados y determinar si con los procesos de ITIL existen nuevas variables que aporten al cuestionario. En la tabla N° 5, se realiza el mapeo de los proceso de Cobit 4.1 e ITIL v3:

Tabla 5. Mapeo de los procesos de Cobit 4.1 hacia procesos de ITILv3

Procesos COBIT	**Información de Soporte ITIL v3**
PO9 Evaluar y Administrar los Riesgos de TI	Gestión de la Continuidad
AI3 Adquirir y mantener infraestructura tecnológica	Gestión de Eventos
AI4 Facilitar la operación y el uso	Gestión de Cambios
AI6 Administrar cambios	Gestión de Cambios
AI7 Instalar y acreditar soluciones y cambios	Gestión de Cambios
DS1 Definir y administrar los niveles de servicio	Gestión de la Demanda, Portafolio de Servicios
DS2 Administrar los servicios de terceros	Gestión de Proveedores
DS3 Administrar el desempeño y la capacidad	Gestión de la Capacidad
DS4 Garantizar la continuidad del servicio	Gestión de la Continuidad
DS5 Garantizar la seguridad de los sistemas	Gestión de Acceso a los Servicios
DS9 Administrar la configuración	Gestión de la Configuración
DS10 Administrar los problemas	Gestión de Problemas
DS12 Administrar el ambiente físico	Gestión de la Disponibilidad
DS13 Administrar las operaciones	Gestión de la Eventos
ME1 Monitorear y Evaluar el Desempeño de TI	Pruebas y validación

ME2 Monitorear y Evaluar el Control Interno	Pruebas y validación
ME4 Proporcionar Gobierno de TI	n/a

Elaborado por: Christian Alonso Llerena Villa

Con los procesos de ITIL obtenidos en el mapeo realizado que se muestra en la tabla N°5, y con el respectivo análisis los mismos con el uso del marco teórico, se concluye que la descripción de cada uno de los procesos de ITIL son equivalentes a los procesos de Cobit de manera general, por lo que no se adicionan nuevas métricas a las antes propuestas sino se ratifica que los marcos de referencia son complementarios y el cuestionario se elaborará en base al Análisis de Impacto al Negocio y a las métricas de Cobit que se desprendieron del análisis del Cubo de Cobit.

Los objetivos de cada una de las entidades públicas del Ecuador hace a cada una de ellas un ente único e individual, por tal motivo se ha sintetizado tanto de los parámetros del Análisis de Impacto al Negocios, como las métricas de los procesos de Cobit, en 25 preguntas que conforman el cuestionario que permitirá determinar el impacto de TI dentro de la entidad y con el cual se procederá a establecer el nivel de disponibilidad requerido en el Centro de Datos.

El cuestionario de 25 preguntas es el resultado de unificar todos los aspectos que han sido recogidos de los marcos de referencia antes mencionados, y se detalla en la tabla 6:

Tabla 6. Cuestionario para determinar la Criticidad de TI en una Entidad.

CUESTIONARIO
1. Cantidad de procesos en general que se realizan en la Entidad
2. Cantidad de procesos que se realizan en la unidad de Tecnología de la Información
3. # de procesos de negocio críticos identificados por un plan de disponibilidad de servicios o en el catálogo de servicios
4. # de procesos críticos del negocio que dependen de TI no cubiertos por un plan de continuidad
5. # de incidentes significativos diarios causados por riesgos identificados por la unidad de TI
6. # de procesos de negocio críticos soportados por la infraestructura del Centro de Datos
7. # de acuerdos de nivel de servicio pactados incluyendo contratos de soporte y acuerdos de nivel de operación
8. # de aplicaciones en las que los procedimientos de TI se integran directamente a los procesos del negocio
9. % de servicios entregados que están en el catálogo de servicios
10. % de usuarios que utilizan los datos de los sistemas
11. % de eventos críticos de TI identificados que son evaluados por TI
12. % de servicios que cumplen con los niveles de servicio
13. % de procesos críticos monitoreados
14. # de usuarios satisfechos con los servicios entregados
15. Cantidad de proveedores que apoyan los procesos de TI
16. Frecuencia en la que se realizan los procesos de Tecnología
17. Cuál es el periodo máximo que el proceso principal del negocio puede estar indisponible
18. El centro de servicios recibe peticiones de servicio de usuarios externos a la entidad
19. Son los procesos dependientes de algún proveedor externo para su completa entrega
20. El centro de datos es compartido con otras entidades
21. Existe disponibilidad de alternar la ejecución de los procesos de TI en otro centro de datos
22. La indisponibilidad de los servicios genera pérdida de ingresos en la entidad
23. La indisponibilidad de los servicios genera gastos adicionales

24. Los procesos críticos de TI se realizan en línea
25. Existen oficinas o sucursales remotas que dependen del Centro de Datos

Elaborado por: Christian Alonso Llerena Villa

Cada una de las preguntas que conforman el cuestionario, obtendrá un puntaje en base al criterio de la respuesta, tal como se muestra en la tabla N° 7,esto permitirá evaluar de una forma rápida los resultados que se obtengan una vez que el auditor de tecnología haya solicitado la respectiva información para contestar el mismo.

Tabla 7. Ponderación de las respuestas al Cuestionario

Preguntas	Respuestas	Ponderación
Preguntas de la 1 a la 8	Hasta 6	1
	Entre 7 y 20	2
	Entre 21 y 30	3
	Mayor a 30	4
Preguntas de la 9 a la 13	Hasta 25	1
	Entre 26 y 50	2
	Entre 51 y 75	3
	Mayor a 75	4
Pregunta 14	Hasta 500	1
	Entre 501 y 1000	2
	Entre 1001 y 1500	3
	Entre 1501 y 2000	4
Pregunta 15	Hasta 1	1
	Entre 2 y 3	2
	Entre 4 y 5	3
	Mayor a 6	4
Pregunta 16	Mensual	1
	Semanal	2
	8x5	3
	24x7	4
Pregunta 17	8 horas	1
	4 horas	2
	2 horas	3
	Media hora	4

Preguntas de la 18 a la 25	No	1
	Si	4

Elaborado por: Christian Alonso Llerena Villa

Finalmente se realiza la sumatoria del puntaje obtenido en cada respuesta, este resultado tiene como objeto clasificar la dependencia en relación al impacto y criticidad que tienen los procesos de TI en cualquier entidad del sector público del Ecuador, dentro de 4 rangos, como se muestra en la tabla N° 8.

Tabla 8. Dependencia de TI en relación al puntaje obtenido en el Cuestionario

Puntaje obtenido	**Dependencia de TI**
Hasta 50	Bajo
Entre 51 y 75	Medio
Entre 76 y 90	Alto
Mayor a 90	Muy Alto

Elaborado por: Christian Alonso Llerena Villa

La definición de la Disponibilidad requerida en el Centro de Datos es la siguiente:

BAJO: Los procesos de TI tienen una baja incidencia en los objetivos y metas de la entidad, por lo que la afectación en la disponibilidad del Centro de Datos no interfiere directamente en la consecución de los objetivos de la entidad.

MEDIO: Los procesos de TI se ejecutan frecuentemente y son necesarios para la continuidad de las operaciones del negocio, sin embargo la indisponibilidad momentánea del Centro de Datos no representa una afectación crítica que genere la pérdida ingresos, imagen o genere sanciones, incumplimientos regulatorios o gastos adicionales.

ALTO: Los procesos de TI son críticos para la continuidad de las operaciones que se realizan en la entidad y para el cumplimiento de sus objetivos y su incumplimiento puede ocasionar principalmente impactos financieros.

MUY ALTO: Los procesos de TI en caso de no estar disponibles generan pérdida ingresos, imagen, sanciones, incumplimientos regulatorios y gastos adicionales que ponen en riesgo la supervivencia de la entidad.

Se determina que el impacto y criticidad de los procesos de Tecnología de la Información están directamente relacionados con la Disponibilidad requerida en el Centro de Datos, adicionalmente se considera que la disponibilidad requerida también se la puede obtener del análisis de la naturaleza de la entidad, es decir se desprende de alinear los requisitos de la entidad con las categorizaciones del Centro de Datos en los cuales se basa el estándar ideado por el *Uptime Institute* que son los niveles TIER.

En este campo se hace referencia al documento "*Tier Classifications Define Site Infrastructure Performance*" (Clasificación TIER define el desempeño de la infraestructura del Sitio), publicado por el Uptime Institute, en el cual se resalta la necesidad que cada empresa, organización o entidad, tiene respecto a la disponibilidad de su Centro de Datos y engloba cada una de las categorizaciones según el negocio u objetivos de las organizaciones.

De ese modo se desprende que un Centro de Datos con necesidad de disponibilidad baja, o TIER 1 según el estándar, es apropiado para organizaciones como:

• Las pequeñas entidades u organizaciones en donde la tecnología de la información principalmente está orientada a mejorar los procesos de negocio internos.

• Las empresas cuyo principal uso y necesidad de tener presencia en la web sirven como una herramienta de marketing pasivo, es decir que no se requiere de mayor innovación tecnológica para captar mercado.

• Empresas nuevas basadas en servicios a través de la Internet que no tienen compromisos financieros sobre la calidad de servicio ofrecido a sus clientes.

Estas empresas normalmente no tienen un ingreso establecido corriente o un impacto financiero identificable de interrupción debido a la insuficiencia del Centro de Datos. La categorización Tier I se puede aplicar cuando los procesos de TI que se ejecutan en la entidad, tienen un requisito de baja disponibilidad, por ejemplo cuando se requiere disponibilidad 5 días a la semana. Las entidades pueden expresamente optar por un Centro de Datos adecuado acorde al nivel TIER I cuando está previsto abandonar el sitio cuando los requisitos de negocio aumenten y se contemple la opción de utilizar un Centro de Datos externo.

En relación a la categorización Tier II, se define que es apropiado para las organizaciones, tales como:

• Aquellas que disponen de Centros de llamadas o Call Centers en más de un solo lugar.

• Las empresas basadas en servicios por Internet sin sanciones económicas graves por incumplimiento en la calidad de servicio.

• Las entidades o empresas cuyas necesidades de tecnología de la información son en su mayoría limitados a las horas laborables tradicionales, permitiendo que los servicios de TI se apaguen fuera del horario normal de labores.

• Entidades destinadas a la investigación científica cuyos objetivos son a largo plazo y que por lo general no tienen la obligación de prestación de servicios en línea o en tiempo real.

Este tipo de entidades normalmente no dependen de la entrega en tiempo real de los productos o servicios. Las entidades pueden seleccionar infraestructura en su Centro de Datos acorde a Tier II cuando los impactos por fallas en la infraestructura han causado demasiados problemas en la disponibilidad ofrecida por Tier I.

Se considera que las entidades especialmente de tipo educativas, pueden seleccionar infraestructura de tipo Tier II porque no hay un impacto significativo de la interrupción temporal del Centro de Datos debido a un fallo.

Las aplicaciones típicas para las instalaciones de categoría III de Tier son:

• Las entidades o empresas que apoyan a los clientes internos y externos, 24x7, tales como centros de servicios y servicios de información, pero puede aceptar cortos períodos con servicio limitado debido a un error en el Centro de Datos.

• Las entidades o empresas cuyos recursos de TI soportan transacciones propias del negocio mediante procesos automáticos, en los que el impacto en los clientes por las paradas del sistema es manejable y aceptable.

• Las entidades o empresas que tienen clientes y empleados en varias zonas horarias y distintas regiones.

• Las entidades o empresas basadas en Internet que tienen compromisos de calidad de servicio que pueden ocasionar graves problemas financieros.

Las entidades o empresas que deben seleccionar infraestructura Tier III, lo harán debido a los altos requisitos de disponibilidad para los negocios o para alcanzar sus objetivos, y que han identificado un costo significativo debido a una parada prevista del Centro de Datos, adicionalmente están dispuestas a aceptar el impacto de la interrupción ante un acontecimiento imprevisto.

El nivel más alto de la categorización es el Tier IV, el mismo que se justifica con más frecuencia para el siguiente grupo de entidades o empresas públicas:

• Entidades o empresas que entregan y requieren presencia en el mercado internacional24 horas durante todo el año y donde los procesos son continuos como por ejemplo las transferencias bancarias internacionales, etc.

• Grandes empresas multinacionales con negocios basados en el comercio electrónico, las transacciones de mercado, o procesos de liquidación financiera.

• Las entidades o empresas basadas en Internet o proveedores de servicio de Data Center que tienen compromisos de calidad de servicio con graves problemas financieros.

Las entidades o empresas que tienen requisitos muy altos de disponibilidad para cumplir sus negocios en curso y en los que se ha identificado un claro costo de

interrupción debido a una parada del centro de datos deben seleccionar una infraestructura de Centro de Datos con categoría Tier IV, lo cual hace que la inversión en la infraestructura esté justificada en relación a la ventaja competitiva.

Las clasificaciones Tier se crearon para describir sistemáticamente los niveles de infraestructura necesarios para mantener las operaciones en un Centro de Datos desde un punto de vista de usuario, es decir la indisponibilidad a la que están sujetos los usuarios cuando existe una falla.

De este modo el Auditor Informático estará en la capacidad de determinar el nivel de disponibilidad requerido para el Centro de Datos auditado, lo cual permitirá mitigar que se produzca algún tiempo de inactividad no previsto (*downtime* no programado), los mismos que pueden surgir de por algún evento físico, como un fallo de hardware o software o alguna anomalía del entorno(Eduardo, 2010). Ejemplos de eventos de tiempo de inactividad no programados pueden ser cortes de energía, fallas de servidores o componentes RAM u otros componentes de hardware), debido a un recalentamiento, ruptura física de conexiones de red, etc.

Ante estos riesgos se determina que la infraestructura física cumple una función determinante para permitir la disponibilidad del Centro de Datos, los mismos que bajo una correcta adecuación de los elementos que forman parte de su infraestructura estará en capacidad de brindar el nivel de disponibilidad deseado.

Finalmente se concluye que con el uso del cuestionario propuesto y con el uso de la categorización en base al tipo de negocio, el Auditor Informático está en capacidad de determinar la disponibilidad que debe tener el Centro de Datos de la entidad pública en que realizará la acción de control, por lo que se considera necesario realizar un análisis del estándar TIA 942, con el propósito de identificar los

principales aspectos que son necesarios contemplar en la Guía de Auditoría para la Infraestructura de los Centros de Datos de las entidades públicas del Ecuador

3.2 Análisis del Estándar TIA 942

En virtud de que el objetivo de la Guía de Auditoría para los Centros de Datos de las Entidades Públicas del Ecuador, se basa en la comparación de un Centros de Datos con una de las categorizaciones antes mencionadas, según la disponibilidad requerida para el mismo, es muy importante realizar un análisis del estándar TIA 942, el mismo que permitirá conocer las consideraciones generales y requisitos propuestos en el estándar para la correcta implementación y funcionamiento de la infraestructura del Centro de Datos.

3.2.1 Clasificación de los tipos de Centros de Datos según la disponibilidad requerida

La clasificación de los centros de datos se basa en el estándar TIA 942 y las definiciones del estándar TIER, los mismos que definen cuatro tipos de centros de datos, cada uno de los cuales contiene los parámetros requeridos en su nivel de infraestructura. En la presente tesis, se determina que el Centro de Datos a ser auditado se comparara de acuerdo al nivel de disponibilidad requerido, es decir de acuerdo al resultado obtenido con el uso del cuestionario para determinar el impacto de TI en una entidad pública del Ecuador.

En la tabla N°9, se muestran los Grados de Disponibilidad indicados en el estándar TIA 942:

Tabla 9. Disponibilidad según categorización TIER

TIER	DISPONIBILIDAD
Tier I	99.671 %
Tier II	99.741 %
Tier III	99.982 %
Tier IV	99.995 %

Elaborado por: Christian Alonso Llerena Villa

Dado que el cumplimiento de los requerimientos de la norma está orientada a la certificación del Centro de Datos por parte del *Uptime Institute*, y en vista de que el objetivo de la Guía de Auditoría para los Centros de Datos de las Entidades Públicas del Ecuador está orientada a auditar los mismos bajo los lineamientos del estándar, mas no a la certificación, es menester realizar un análisis de cada uno de los requerimientos exigidos en cada uno de los grados de disponibilidad antes mencionados y adaptarlos según la realidad de las entidades públicas del Ecuador, así como a las facilidades operacionales y las leyes y reglamentos vigentes. Por tal motivo se definen cuatro tipos de Centros de Datos equivalente a los cuatro niveles TIER del estándar, los cuales estarán asociados a la disponibilidad requerida que se obtuvo del cuestionario antes propuesto.

Tabla 10. Definición de Tipos de Centro de Datos para la Guía de Auditoría

Estándar TIA 942	Guía de Auditoría	Disponibilidad Requerida
Tier I	Centro de Datos TIPO I	Baja
Tier II	Centro de Datos TIPO II	Media
Tier III	Centro de Datos TIPO III	Alta
Tier IV	Centro de Datos TIPO IV	Muy Alta

Elaborado por: Christian Alonso Llerena Villa

La aplicación de los niveles de la norma Tier, se realizan en base a cuatro sistemas:

- A nivel de Arquitectura
- A nivel de Telecomunicaciones
- A nivel Eléctrico
- A nivel Mecánico

Hay que destacar que el estándar TIA 942 fue creado por la *Telecommunication Industry Association*, que en sus primeras publicaciones de estándares proponen una serie de especificaciones para comunicaciones y cableado estructurado, que posteriormente avanzan sobre los subsistemas de infraestructura de un Centro de Datos, generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar en los Centros de Datos, por consiguiente es de gran importancia realizar un minucioso análisis del estándar TIA 942 para comprender cada uno de los requerimientos que se plantean en los distintos tipos de Centros de Datos.

Con lo antes descrito se constata en el análisis del estándar, que para el correcto diseño o ampliación de un Centro de Datos, se considera la existencia de los siguientes espacios dentro del Centro de Datos, los mismos que se encuentran en relación directa con otros espacios del edificio:

- Instalaciones de Entrada de Servicios
- Oficinas del Staff de Soporte
- Centro de Operaciones
- Cuarto de Equipos.

• Cuartos de Telecomunicaciones y de Equipos

• Cuartos Eléctrico & Mecánico (Cuarto de Baterías, UPS, tableros y Sistema de Aire acondicionado o HVAC)

• Cuartos de Almacenamiento

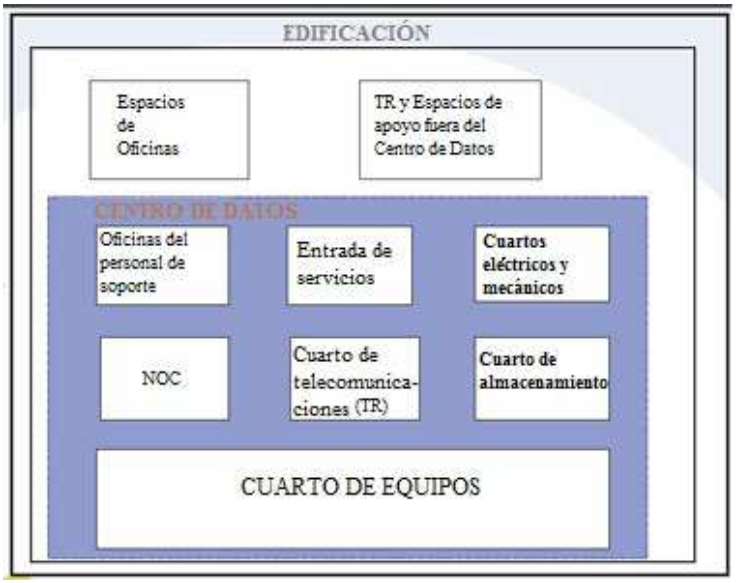

Figura 2. Relación de Espacios de un Centro de Datos
Fuente: TIA 942

Los Centro de Datos requieren de varios espacios dedicados a alojar diversos tipos de infraestructuras (mecánica, eléctrica, etc.), en tal virtud un Centro de Datos puede tener los espacios antes mencionados, aunque no necesariamente cada uno de ellos, (Figueroa, 2007).

Dependiendo del tamaño del centro de datos, no todos estos espacios se pueden usar dentro de la estructura. Estos espacios deben ser planeados considerando el crecimiento y la transición a las tecnologías en evolución. Estos espacios pueden o no estar separados por paredes del cuarto de equipos, cabe indicar que el estándar propone los lineamientos y directrices para el diseño, instalación, ampliación y mantenimiento de cualquier Centro de Datos o Cuarto de Equipos. Ante lo cual es necesario establecer el concepto de cada una de estas instalaciones:

Cuarto de Equipos (*Computer room*): Un espacio arquitectónico cuya función principal es dar cabida a los equipos de procesamiento de datos.

Centro de Datos (*Data Center*): Un edificio o parte de un edificio cuya función principal es la de albergar un Cuarto de Equipos y sus áreas de apoyo.

De los espacios mencionados hay que destacar que el principal espacio al que se refiere el estándar es el Cuarto de Equipos denominado también Cuarto de Cómputo o *Computer Room*, el mismo que dispone de las siguientes áreas:

- Cuarto de entrada de servicios
- área de distribución principal (MDA)
- área de distribución horizontal (HDA)
- área de distribución de la zona (ZDA)
- el área de distribución de equipos (EDA)

En la figura 3, se puede visualizar el espacio correspondiente al cuarto de equipos, en el cual se identifican sus áreas mencionadas anteriormente.

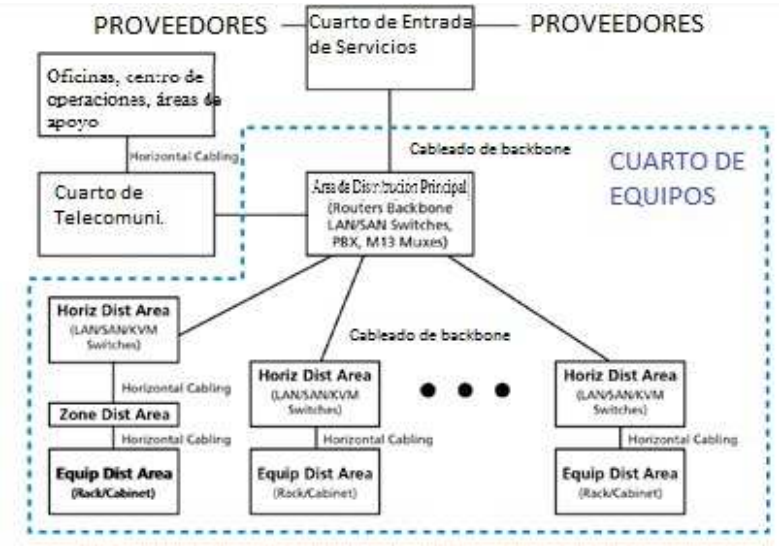

Figura 3. Áreas funcionales del Centro de Datos
Fuente: TIA 942

De los conceptos antes mencionados se desprende que cualquier entidad u organización puede disponer de un Centro de Datos o Cuarto de Equipos en función del espacio y áreas que forman parte de cada uno de ellos, sin embargo en la presente tesis se utilizará el término Centro de Datos para ambos casos puesto que es el nombre común que se utiliza para estos espacios independiente del tamaño y áreas que contengan los mismos.

En tal virtud se considera la existencia de Centros de Datos de tamaño reducido, en los que se pueden consolidar las conexiones en una sola área de distribución principal (MDA), en un solo armario o rack. El cuarto de telecomunicaciones para el cableado de las áreas de soporte y las instalaciones de entrada también puede ser consolidado en el área de distribución principal en este tipo de topología, como se muestra en la figura N° 4.

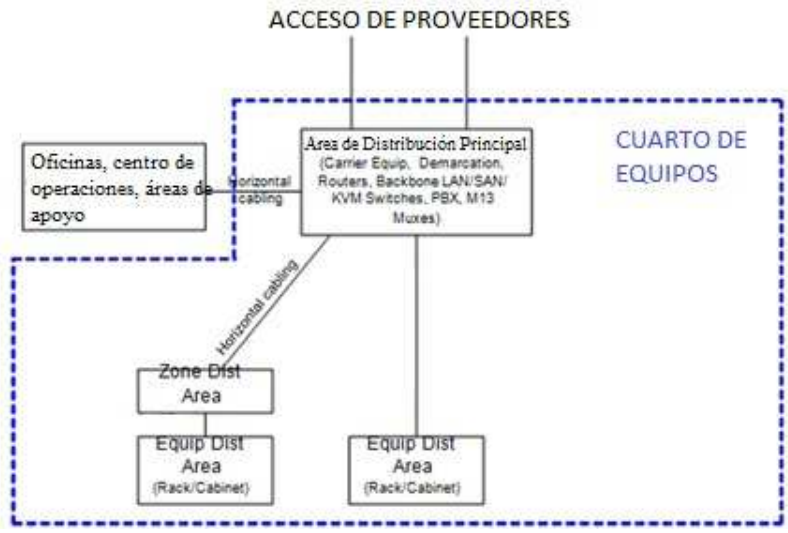

Figura 4. Ejemplo de topología de un Centro de Datos reducido
Fuente: TIA 942

Una vez que se ha especificado los espacios y las áreas que forman parte de un Centro de Datos, se procede a establecer los requerimientos generales de las

instalaciones, los mismos que se aplican para todos los Centros de Datos, independientemente del nivel de disponibilidad que se pretende alcanzar.

Acorde al estándar, a continuación se establecen los requerimientos principales para cada uno de los espacios que forman parte del Centro de Datos:

3.2.2 Requerimientos generales del Cuarto de Equipos

El cuarto de equipos es un espacio de ambiente controlado que sirve el único propósito de hospedar el equipamiento y el cableado directamente relacionado con los sistemas informáticos y otros sistemas de telecomunicaciones.

3.2.2.1 Aspectos Generales

Entre los aspectos generales que debe cumplir el cuarto de equipos se destacan:

3.2.2.1.1 Distribución del piso

La distribución del piso debe considerar los siguientes aspectos:

- Debe existir un estudio de carga del suelo, incluidos los equipos, cables, cables de conexión, y de los medios de comunicación.
- Debe existir espacios libres a los lados delos equipos que permitan realizar el mantenimiento de los mismos.
- Debe cumplir con los requisitos de flujo de aire, en los que se considera pasillos fríos y pasillos calientes.

- Debe existir estudios de alimentación de corriente y restricciones de longitud del circuito.

- Debe cumplir con requisitos de longitud de la conexión entre equipos.

3.2.2.1.2 Ubicación

En relación a la ubicación del cuarto de equipos se consideran los siguientes aspectos:

Por criterios de expansión del cuarto de equipo se debe evitar lugares que están junto a ascensores, paredes exteriores o junto a muros fijos.

El cuarto de equipos deberá estar situado lejos de fuentes de interferencia electromagnética. Ejemplos de tales fuentes de ruido incluyen transformadores eléctricos fuente de alimentación, motores y generadores de rayos x, equipos de radio o transmisores de radar y dispositivos de sellado de inducción.

Los cuartos de equipos no deben tener ventanas al exterior, como prevención para evitar el aumento de la carga de calor y por seguridad en el acceso.

3.2.2.1.3 Acceso

El cuarto de equipos debe contar con puertas que faciliten el acceso sólo al personal autorizado.

Las fuentes de radio tales como antenas de red inalámbricas, teléfonos celulares o radios pueden interferir con la apropiada operación de los equipos de telecomunicaciones y de tecnología de la información por lo que se debe revisar las

hojas técnicas de los fabricantes de los equipos acerca de la restricción o no en el uso de sistemas de radio inalámbricos dentro del cuarto de equipos.

3.2.2.2 Diseño arquitectónico

3.2.2.2.1 Tamaño

Se considera el aspecto del tamaño del Cuarto de Equipos adecuado para satisfacer los requisitos de los equipos que se hospedarán en el mismos, se considerará la información obtenida del proveedor de los equipos. Se debe considerar una expansión futura proyectada, así como las necesidades actuales.

Adicionalmente se permite el hospedaje en el cuarto de equipos de los equipos de control eléctrico, tales como distribución de energía o sistemas acondicionamiento y UPS hasta 100 kVA, con la excepción de las baterías de tipo húmedas. Si los UPS son de más de 100 kVA y contienen baterías de celda húmeda deben estar ubicados en un cuarto aparte.

No debe existir ningún tipo de tuberías, conductos, tubos neumáticos, etc. o equipos no relacionados con el apoyo del cuarto de equipos.

3.2.2.2.2 Altura del techo

Se considera que la altura mínima del techo debe ser de 2,6 m del piso terminado a cualquier obstáculo, como aspersores, accesorios de iluminación o cámaras.

3.2.2.2.3 Tratamiento

Los pisos, paredes y techos deberán ser sellados, pintados o construidos de un material para minimizar el polvo. Los acabados deben ser de color claro para mejorar la iluminación de la habitación y los pisos deben tener propiedades anti- estáticas.

3.2.2.2.4 Iluminación

La iluminación en los espacios ocupados por el personal deberá ser como mínimo de 500 lux en el plano horizontal y 200 lux en el plano vertical.

Las luminarias no deben ser alimentadas desde el mismo panel de distribución eléctrica de los equipos de telecomunicaciones. Debe existir señalética acorde a las exigencias del ente regulador ante la ausencia de iluminación para no obstaculizar la salida de emergencia.

3.2.2.2.5 Puertas

Las puertas deben tener un mínimo de 1 m de ancho y 2,13 m de alto, sin umbrales en las puertas, bisagras o tipo desmontables. Las puertas deben estar equipadas con cerraduras.

3.2.2.2.6 Resistencia del suelo

La capacidad de carga del suelo en el cuarto de equipos deberá ser suficiente para soportar la carga distribuida y concentrada de los equipos instalados y el cableado y los medios asociados. La capacidad de carga del piso distribuido mínima será de 150 lbf / ft2 (libras fuerza por pie cuadrado); y la capacidad de carga del piso distribuido recomendada es de 250 lbf / ft2.

3.2.2.2.7 Señalización

La señalización, si se usa, debe desarrollarse acorde al plan de seguridad del edificio.

3.2.2.2.8 Consideraciones Sísmicas

Las especificaciones para las instalaciones deberán adaptarse a las necesidades de zonas sísmicas aplicables según los procedimientos de construcción vigentes.

3.2.2.3 Diseño ambiental

En el diseño ambiental constan los siguientes elementos a ser tomados en cuenta:

3.2.2.3.1 HVAC (*Heating Ventilation Air Conditioner*)

El cuarto de equipos debe disponer de un sistema HVAC para ser reconocido como tal, ya sea que utilice el sistema principal del edificio o uno dedicado.

3.2.2.3.2 Funcionamiento continúo

HVAC se facilitará las 24 horas por día y los 365 días base por año. Si el sistema del edificio no puede asegurar la operación continua se proporciona una unidad dedicada para el cuarto de equipos.

3.2.2.3.3 Modo de espera (*Stand-by*)

El sistema de climatización del cuarto de equipos debe ser soportado por el generador eléctrico del cuarto de equipos, si hay alguno instalado. En caso de que no se disponga del mismo, el HVAC debe ser conectado al generador de reserva del edificio, si hay alguno instalado.

3.2.2.3.4 Parámetros operacionales

La temperatura y humedad se controlan para proporcionar rangos de operación continua para la temperatura y la humedad:

- Temperatura de bulbo seco: 18 °C a 27ºC(es la medida con un termómetro convencional de mercurio o similar)
- Humedad relativa máxima:60%
- Punto de rocío:5.5 °C hasta 15 °C
- Equipos de humidificación y des humidificación pueden ser necesarios dependiendo de las condiciones ambientales.

La temperatura ambiente y la humedad se miden después de que el equipo está en funcionamiento. Las mediciones se realizan a una distancia de 1.5 m por encima del nivel del suelo cada 3 a 6 m a lo largo de la línea central de los pasillos fríos y en cualquier ubicación en la entrada de aire del equipo de trabajo. Las mediciones de temperatura deben ser tomadas en varios lugares de la toma de aire de cualquier equipo con los posibles problemas de refrigeración.

3.2.2.3.5 Baterías

Si se utilizan baterías de reserva, debe existir una ventilación adecuada y contenedor en caso de derrames.

3.2.2.3.6 Vibración

Las vibraciones mecánicas junto al equipo o la infraestructura de cableado pueden provocar fallas en los servicios en el tiempo, como por ejemplo debido a la

pérdida de conexiones. En estos casos, el ingeniero estructural debe ser consultado para diseñar salvaguardas contra la excesiva vibración del cuarto de equipos.

3.2.2.4 Diseño eléctrico

3.2.2.4.1 Potencia

Se proveerán circuitos de alimentación separados para servir al cuarto de equipos los mismos que terminan en su propio tablero eléctrico o paneles.

El cuarto de equipos debe tener tomacorrientes dúplex (120V 20A) para las herramientas eléctricas, equipos de limpieza y equipos que no son adecuados para conectar a las tomas de corriente de los gabinetes. Estos tomacorrientes no deben estar en las mismas unidades de distribución de energía o paneles eléctricos de los circuitos eléctricos utilizados para las telecomunicaciones y equipo de cómputo en el cuarto. Los tomacorrientes deben tener una separación de 3,65 metros de distancia a lo largo de las paredes del cuarto de equipos, o más cerca si se especifica por las ordenanzas locales.

3.2.2.4.2 Energía de reserva

Los tableros eléctricos del cuarto de equipos deben ser soportados por el generador eléctrico, si existe uno instalado. Los generadores utilizados deben estar clasificados para cargas electrónicas. Si el cuarto de equipos no tiene un sistema generador eléctrico dedicado, los tableros eléctricos deberán ser conectados al generador de reserva del edificio, si existe alguno.

3.2.2.4.3 Puesta a tierra

Se considerará la puesta a tierra de telecomunicaciones especificados por el estándar ANSI/TIA/EIA-J-STD-607-A, en la cual se establece que el cuarto de equipos debe tener una red de tierra común.

3.2.2.4.4 Protección contra incendios

Los sistemas de protección contra incendios y extintores portátiles deberán cumplir con los requerimientos normativos vigentes expedidos por el ente regulador.

3.2.2.4.5 Infiltración del agua

Cuando exista riesgo de entrada de agua, se debe proveer un medio de evacuación como por ejemplo, un desagüe en el suelo. Además, al menos un drenaje para la evacuación de agua por cada 100 m2 área debe ser proporcionado. Las tuberías de agua y desagüe instalados en el cuarto deben estar ubicadas lejos de los equipos.

Una vez que se han considerado los principales requerimientos para el Cuarto de Equipos, se analizan los requerimientos para el resto de áreas y espacios del Centro de Datos.

3.2.3 Requerimientos para el cuarto de entrada de servicios

El cuarto de entrada de servicios, es un espacio preferentemente un cuarto, en el que el acceso es administrado por el propietario del Centro de Datos y donde se pueden hospedar los equipos o interfaces de las instalaciones de propiedad del proveedor de servicios, además dispone de una interfaz con el sistema de cableado hacia el Centro de Datos. Por lo general alberga los equipos de telecomunicaciones de los proveedores. Este espacio se denomina también Punto de Demarcación.

Se deberá poner especial atención en la distancia desde el punto de demarcación hacia los equipos terminales para verificar que no se exceda la distancia máxima de longitud de los cables y de ser el caso se considera el uso de repetidores.

En algunos Centros de Datos, pueden existir más de un cuarto de entrada de servicios los mismos que se requerirán por conceptos de redundancia o por necesidades de cumplimiento de las distancias máximas permitidas.

Si la entrada de servicios se encuentra dentro del Cuarto de Equipos se deberá poner atención en que los conductos no interfieran con el flujo de aire u otros tendidos de cable.

El cuarto de entrada debe ser dimensionado para satisfacer los requisitos máximos conocidos y previstos para:

- Vías de acceso del proveedor de acceso y cableado de campus;
- Tableros y espacio para la terminación de los servicios de acceso y cableado de campus;
- Racks del proveedor de acceso
- Equipos de propiedad del cliente que se encuentra el cuarto de entrada
- Racks de demarcación, incluyendo hardware de terminación para el cableado de la sala de informática
- Vías para el cuarto de equipos, el área principal de distribución, la zona de distribución y posiblemente el área de distribución horizontal
- Vías hacia otros cuartos de entrada de servicios en caso de existir.

El espacio requerido está relacionado más estrechamente con el número de proveedores de acceso, número de circuitos y tipo de circuitos.

Los demás requerimientos tales como altura, tratamiento, puertas, HVAC, iluminación, etc. serán similares a los requerimientos detallados para el Cuarto de Equipos.

3.2.4 Requerimientos para el área de distribución principal (MDA)

El área de distribución principal (MDA) es el espacio central donde se encuentra el punto de distribución para el sistema de cableado estructurado en el Centro de Datos. El centro de datos debe tener al menos un área de distribución principal. Los enrutadores de núcleo y los equipos principales de redes del Centro de Datos a menudo se encuentran en el área de distribución principal.

El área de distribución principal estará situada en un lugar central para evitar exceder las restricciones de distancia máxima de los cables de los circuitos del proveedor de acceso provenientes desde fuera. Adicionalmente en caso de encontrarse en un cuarto cerrado debe tener panel de alimentación de energía exclusivo para su respectivo UPS y HVAC.

Para los requerimientos arquitectónicos, mecánicos y eléctricos se debe referir a los mismos del Cuarto de Equipos.

3.2.5 Requerimientos para el área de distribución horizontal (HDA)

3.2.5.1 Aspectos generales

El área de distribución horizontal (HDA) es el espacio que soporta el cableado a las áreas de distribución de equipos. Los conmutadores LAN, SAN, consolas y KVM que apoyan el equipo final, también se encuentran normalmente en el área de distribución horizontal. El área principal de distribución puede servir como

un área de distribución horizontal de equipos cercanos o para todo el cuarto de equipos, cuando el cuarto de equipos es pequeño.

El número máximo de conexiones en el área de distribución horizontal debe ser ajustado en base a la capacidad de la bandeja de cables, dejando espacio suficiente para crecimiento futuro.

Los requerimientos arquitectónicos, mecánicos y eléctricos son los mismos del Cuarto de Equipos.

3.2.6 Requerimientos para la zona de distribución (ZDA)

La zona de distribución debe limitarse a servir a un máximo de 288 conexiones coaxiales o de par trenzado para evitar la congestión de cables, en particular para los armarios destinados a ser colocados por encima o debajo de los 60 cm de las baldosas.

No se requieren equipos activos en la zona de distribución, con la excepción de los equipos de alimentación.

3.2.7 Requerimientos para las áreas de distribución de equipos

Las áreas de distribución de equipos son los espacios asignados para los equipos finales, incluidos los sistemas de cómputo y equipos de telecomunicaciones.

El equipo final es por lo general el equipo instalado sobre el piso o montados en armarios o racks. Se debe verificar que existan receptáculos de energía suficientes para el hardware. Adicionalmente las longitudes de cable para el cableado de punto a

punto entre los equipos en el área de distribución de equipos deben ser inferiores a 15 metros.

3.2.8 Requerimientos para el cuarto de telecomunicaciones (TR)

En el Centros de Datos, el cuarto de telecomunicaciones (TR) es un espacio que soporta el cableado hacia las áreas fuera del cuarto de equipos. El TR se encuentra normalmente fuera del cuarto de equipos, pero puede ser combinado con el área de distribución principal o con las áreas de distribución horizontal.

El Centro de Datos puede soportar más de un cuarto de telecomunicaciones si las áreas a ser atendidas requieren más de un solo cuarto de telecomunicaciones.

3.2.9 Requerimientos para las áreas de apoyo al Centro de Datos

Las áreas de apoyo del centro de datos son espacios fuera del cuarto de equipos que se dedican a apoyar la instalación del mismo. Estos pueden incluir el centro de operaciones, oficinas de personal de apoyo, cuarto de seguridad, cuartos eléctricos, cuarto de máquinas, cuarto de almacenamiento y puntos de carga.

El centro de operaciones, cuarto de seguridad, y las oficinas de personal de apoyo deben disponer de cableado estructurado similar a las áreas de oficina estándar. Las consolas centrales de operación y consolas de seguridad requieren un mayor número de cables que el resto de áreas de trabajo. Se debe considerar que el centro de operación puede requerir cableado para pantallas montadas en la pared o el techo. Los cuartos eléctricos, cuartos de máquinas, cuarto de almacenamiento, cuarto de parada de equipos y puntos de carga deberán tener al menos un teléfono cada uno.

Los cuartos eléctricos y mecánicos también deben tener al menos una conexión de datos.

3.2.10 Requerimientos de los racks y gabinetes

Los racks deben estar equipados con rieles de montaje lateral en los que se montan los equipos y hardware. Los gabinetes pueden ser equipados con rieles laterales de montaje, paneles laterales, puertas delanteras y traseras y frecuentemente tienen cerraduras.

3.2.10.1 Pasillos Calientes y Fríos

Los gabinetes y racks deberán ser acomodados acorde a un patrón alternante, con las partes delanteras de los gabinetes y racks enfrentando uno al otro en una fila para crear pasillos "calientes" y "fríos".

Los pasillos fríos están en frente de racks y gabinetes, mientras que los pasillos calientes se encuentran detrás de los racks y gabinetes, como se observa en la figura Pasillos Calientes y Fríos.

Figura 5. Pasillos Calientes y Fríos
Fuente: Varios autores

Existen otras consideraciones a tomar en cuenta con los racks y gabinetes, tales como los lineamientos para la instalación de equipos, los mismos que se requiere que sean montados de manera que no afecte el esquema de enfriamiento en base a los pasillos fríos y calientes, esto se toma en cuanta en base a la existencia de equipos que pueden tener el enfriamiento hacia adelante. Otro aspecto es que el posicionamiento de los racks y gabinetes permita el levantamiento de las baldosas tanto adelante como atrás del rack, también se debe verificar que los gabinetes se encuentren alineados en la misma posición, como se muestra en la Figura N°6.

Figura 6. Baldosas alineadas y perforadas en los pasillos fríos
Fuente: Varios autores

Los racks con propiedades sísmicas serán atornillados a un soporte sísmico o atornillado directamente a la losa. Los racks que se apoyan en la planta de acceso se atornillan a la losa de cemento o un canal de metal fijado a la losa mediante varillas roscadas que penetran a través de las baldosas del suelo.

Espacios libres:

- Un mínimo de 1 m (3 ft) de espacio delantero será proveído para la instalación de los equipos. Un espacio libre delantero de 1.2 m (4 ft) es preferible para acomodar equipos más profundos.

- Un mínimo de 0.6 m (2 ft) de espacio trasero será proveído para acceso de servicio a la parte trasera de racks y gabinetes.
- Un espacio libre trasero de 1 m(3 ft) es preferible. Algunos equipos pueden requerir espacios de servicio más grandes que 1 metro.

Otros requerimientos de los racks y gabinetes son los siguientes:

- La altura máxima sugerida de los racks y gabinetes es de 2,4 metros y profundidad de 1.1 metros.
- Los gabinetes deben tener rieles ajustables y proveer al menos 42 unidades de rack.
- Se debe considerar gabinetes que dispongan de regletas eléctricas conectadas a diferentes fuentes de energía. Las regletas deben estar correctamente etiquetadas con el panel y el número de circuito del breaker.

3.2.11 Sistema de Cableado en el Centro de Datos

Los sistemas de cableado en el centro de datos se definen en los siguientes tipos:

- Cableado horizontal
- Cableado de backbone
- Conexión cruzada en el área de entrada de servicios o en el área de distribución principal (MDA)
- Conexión cruzada principal en el área de distribución principal (MDA)

- Conexión cruzada horizontal (HC) en el cuarto de telecomunicaciones, área de distribución horizontal o área de distribución principal(MDA)

Entre los aspectos a revisar se destacan en forma general los siguientes:

Los cables reconocidos, el hardware de conexión asociado, *jumpers, patchcords, cords* de equipos y cords del Área de Zona cumplirán todos los requerimientos aplicables especificados en: ANSI/TIA/EIA-568-B.2 y ANSI/TIA/EIA-568-B.3, como por ejemplo se tiene:

- Cable de par trenzado de 100 ohm:
- Categoría 3 o 5e que cumple ANSI/TIA/EIA-568-B.2
- Categoría 6 que cumple ANSI/TIA/EIA-568-B.2-1

En relación a la fibra óptica se destacan los siguientes puntos a revisar en el Centro de Datos:

Cable de fibra óptica MM (multimodo)

• 62.5/125 μm ó 50/125 μm que cumple ANSI/TIA/EIA-568-B.3

• 50/125 μm 850 nm optimizado láser que cumple ANSI/TIA-568-B.3-1 (recomendado)

Cable de fibra óptica SM (monomodo)

•ANSI/TIA/EIA-568-B.3

Los medios coaxiales reconocidos son:

• Cable coaxial 75 ohm (tipo 734 y 735)

• Conector coaxial (ANSI T1.404).

3.2.11.1 Cableado Horizontal

Se denomina cableado horizontal al cable que en el sistema de cableado normalmente corre horizontalmente en el piso o cielo del Centro de Datos.

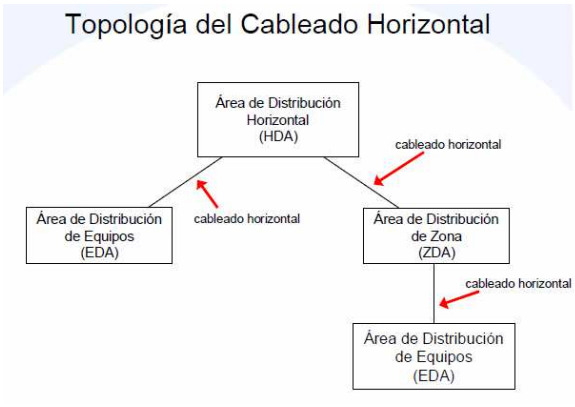

Figura 7. Topología del Cableado Horizontal
Fuente: TIA 942

El cableado horizontal debe considerar las siguientes características:

Cableado desde el área de distribución horizontal (HDA) hasta el área de distribución de equipos (EDA) incluye:

- Cables horizontales
- Cross-connects horizontales
- Patch Cords
- Opcional punto de consolidación
- Distancia del cable horizontal será máxima de 90 metros.

La topología es la siguiente:

El cableado horizontal es la porción del sistema de cableado de telecomunicaciones que se extiende desde la terminación en el área de distribución

de equipos (EDA) hasta la conexión horizontal en el área de distribución horizontal HDA o en el área de distribución principal en el MDA.

3.2.11.2 Cableado de backbone

La función del cableado de *backbone*, o cableado vertical, es proveer conexión entre el área de distribución principal (MDA), el área de distribución horizontal (HDA) y las instalaciones de entrada de servicios en el sistema de cableado del Centro de Datos.

La topología de cableado de backbone es la siguiente:

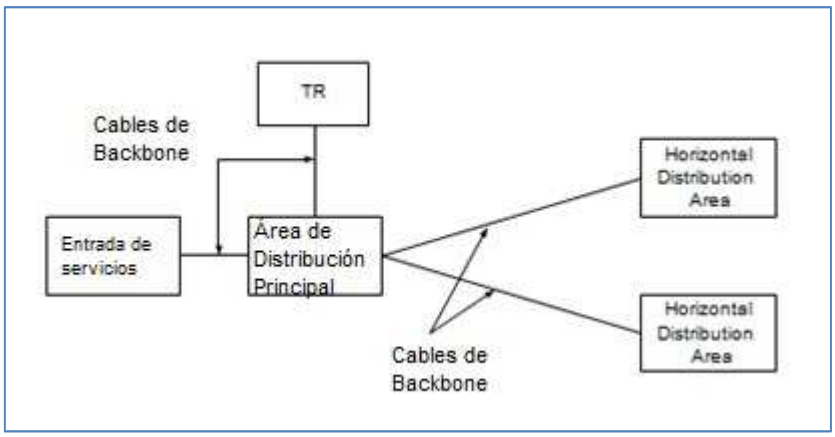

Figura 8. Topología de Cableado de Backbone
Fuente: TIA 942

Se debe considerar principalmente la revisión de las distancias máximas que soporta el cableado de backbone, el mismo que está relacionado al medio seleccionado, tomando en cuenta el límite de 90 metros para el cable categoría 5 E y categoría 6.

3.2.12 Vías del Cableado

Entre sus principales requerimientos de las vías de cableado se debe verificar lo siguiente:

- El cableado no será encaminado a través de espacios con acceso del público a menos que sea encerrado en conductos o se dirija por alguna vía segura.
- Todos los huecos de mantenimiento, cajas de revisión, cajas de empalme deberán estar cerrados con llave y monitoreados usando una cámara y/o una alarma.
- Las vías deben estar correctamente definidas con el propósito de minimizar zigzags, la distribución bajo el piso debe verificarse que no bloquee el flujo de aire.

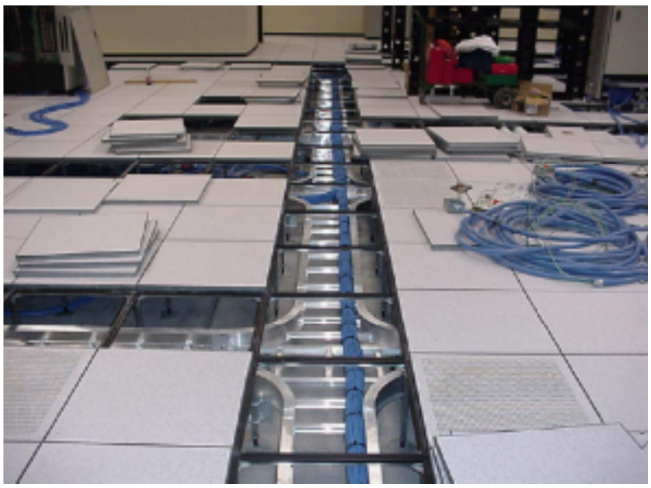

Figura 9. Vías de cableado que no bloquean el flujo de aire
Fuente: Varios autores

Se deben mantener distancias apropiadas entre cables eléctricos y de par trenzado, con las siguientes recomendaciones:

• Los circuitos eléctricos de bifurcación deberían estar en conducto de metal flexible hermético.

• Los circuitos eléctricos del alimentador a las unidades de distribución de potencia deberían estar en conducto de metal sólido.

Adicionalmente se debe considerar la separación del cableado, en los siguientes casos:

Bandejas de Cable:

- Cableado de fibra y de cobre deberían estar separados para mejorar la administración, minimizar el daño a cables de diámetro más pequeño y si es posible, la fibra debería estar encima del cobre.
- Se debe constatar que no se obstruya la accesibilidad a los cables ya que podrían interrumpir el flujo del aire frío.
- En el cuarto de Entrada de Servicios, preferentemente se de tener al menos 1 conducto subterráneo de 4 pulgadas para cada proveedor.

El cableado bajo el piso estará en bandejas de cable ventiladas con las siguientes consideraciones:

• Las bandejas pueden ser instaladas en múltiples capas

• Las bandejas con una profundidad máxima de 6" (150mm)

Una vez que se ha realizado un minucioso análisis y se han obtenido las principales consideraciones y requerimientos que indica el estándar TIA 942 para la infraestructura del Centro de Datos, se procede a consolidar los criterios basados en la categorización TIER, la misma que se basa en la información recogida por el *Uptime Institute* con el propósito de proveer las mejores prácticas para mejorar el diseño y la administración de los Centros de Datos. Cabe indicar que en el anexo G del estándar TIA 942 se definen los requerimientos de cada nivel TIER (ver Anexo

TIA 942 Anexo G), los mismos que se resumen en cada uno de los tipos de Centros de Datos que se proponen en esta Guía de Auditoria.

CAPITULO IV

4. Formulación de la Guía de Auditoría.

Una vez que se ha definido el procedimiento para determinar el impacto que tiene TI en una entidad del sector público del Ecuador con el respectivo análisis de riesgos y se han identificado los lineamientos a seguir que se indican en el estándar TIA 942, sobre la infraestructura del Centro de Datos, se procede a establecer los requerimientos para evaluar la infraestructura del mismo. Cabe indicar que también se incorporan los controles propuestos en la norma ISO 27002, en el capítulo que se refiere a la Seguridad Física y del Ambiente, con el propósito de verificar si dichos controles se deben adicionar a los requerimientos del estándar TIA 942; los controles son los siguientes:

- Perímetro de seguridad física.

  Control:

  Se recomienda que se utilicen perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjetas o escritorios de recepción atendidos por personas) para proteger áreas que contengan información e instalaciones del procesamiento de información.

- Controles de acceso físico

  Control:

  Se recomienda que las áreas seguras se resguarden con controles de acceso adecuados que garanticen que solo se permite el acceso a personas autorizadas.

- Aseguramiento de oficinas, recintos e instalaciones.

Control:

Se recomienda que se diseñe y aplique seguridad física para oficinas, recintos e instalaciones.

- Protección contra amenazas externas y del ambiente.

Control:

Se recomienda que se diseñe y aplique medios de protección contra daños potenciales causados por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o provocado por el hombre.

En conclusión, se determina que los controles propuestos en la norma ISO 27002, se encuentran intrínsecamente incluidos en los requerimientos del estándar TIA 942.

También es necesario establecer la debida correlación de los marcos de referencia utilizados para el análisis de la infraestructura de los Centros de Datos de las entidades públicas del Ecuador con las Normas de Control Interno expedidas por la Contraloría General del Estado, las mismas que se basan en Cobit 4.1,ya que de ese modo se puede corroborar que existe una relación directa entre ellas, lo cual permite que el Auditor base sus recomendaciones citando el cumplimiento de las normas que rigen el sector público del Ecuador, dando el sustento legal respectivo.

En tal virtud se destaca dentro del grupo de Normas de Tecnología de la Información, el subgrupo 410-10 Seguridad de tecnología de información, que indica:

“La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos”.

El inciso 6 indica lo siguiente:

“Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;”

De este modo se concluye que la realización de una auditoria al Centro de Datos de cualquier entidad pública del Ecuador se enmarca en el cumplimiento de la Norma de Control Interno antes mencionada. El esquema para la realización de la presente Guía de Auditoría es el siguiente:

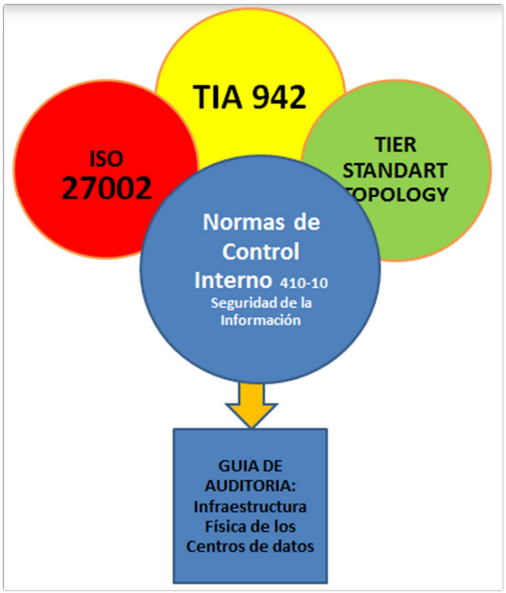

Figura 10. Relación entre los marcos de referencia utilizados en la Guía de Auditoría
Elaborado por: Christian Alonso Llerena Villa

También se debe considerar previo a la evaluación del Centro de Datos, el conocimiento de que activos de hardware se encuentran en el mismo por lo que es necesario realizar el análisis de riesgos, con los lineamientos que se indican a continuación.

4.1 Guía para el Análisis de Riesgos en un Centro de Datos

La realización del Análisis de Riesgos, el mismo que permitirá identificar los principales riesgos a los que están expuestos los activos en relación directa con la infraestructura física de los Centros de Datos, previamente identificará la situación actual del Centro de Datos auditado, para su posterior evaluación bajo los lineamientos del estándar TIA 942.

Con el seguimiento de las fases del Análisis de Riesgos, indicadas en el capítulo II, Marco Teórico, se realiza el siguiente procedimiento:

4.1.1 Identificación de Activos

El primer paso es identificar los activos que se están hospedados en el Centro de Datos mediante una inspección en el sitio que permitirá realizar el levantamiento de los activos de hardware, estos se han agrupado en la siguiente clasificación de activos que comúnmente se encuentran en los Centros de Datos, según se muestra en la siguiente tabla:

Tabla 11. Clasificación de Activos de un Centro de Datos

Activos que se encuentran en el Centro de Datos (hardware en general)	Cantidad	**Descripción**
Servidores		
Switches		
Routers		
Modems		
Líneas Telefónicas		
Central Telefónica		
Dispositivos de almacenamiento (discos duros, storage)		
Grabadores de video		
Enlaces de datos e internet		
Otros		

Elaborado por: Christian Alonso Llerena Villa

Cabe indicar que no se considera la identificación de requerimientos legales, ya que ese criterio se encuentra expuesto en el capítulo IV, como parte de la Formulación de la Guía de Auditoría, por lo que se procede a la tasación de activos.

4.1.2 Tasación de Activos

Una vez que se han identificado los activos se procede a realizar la tasación de activos. La tasación de activos se realiza basada en sus dimensiones o atributos, los mismos que son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Dado que el objetivo de la Guía de Auditoria, es evaluar la infraestructura física de los Centros de Datos, se considera únicamente el atributo “Disponibilidad” en la tasación de activos, con el propósito de asignar un grado de valor según la importancia que representa que se encuentre disponible dicho activo para los objetivos de la entidad, el cual se asignará acorde a la tabla N° 12:

Tabla 12. Criterio para Tasación de Activos

Valor	Significado	Criterio= Disponibilidad
1	Muy bajo	Daño irrelevante
2	Bajo	Daño menor
3	Medio	Daño importante
4	Alto	Daño grave
5	Muy alto	Daño muy grave

Elaborado por: Christian Alonso Llerena Villa

Los valores asignados a la Disponibilidad de cada uno de los activos se deducen del análisis de la importancia de dicho activo para la realización de las funciones o procesos indispensables para las actividades que realiza la entidad auditada. Este criterio se fundamenta en el Análisis de Impacto al Negocio realizado previamente, a manera de ejemplo se puede tomar el Servidor Web (donde se encuentra hospedado el sitio web), al realizar el análisis en relación a la Disponibilidad, la tasación por el impacto que representa en una entidad de tipo comercial va a ser Muy Alto, mientras que en una entidad de tipo educativa puede ser Bajo. Estos parámetros corresponden al criterio del Auditor Informático con la ayuda del Análisis de Impacto al Negocio mencionado anteriormente.

4.1.3 Identificación de las Amenazas y Vulnerabilidades

El siguiente paso es la identificación de las Amenazas y Vulnerabilidades, a continuación se presenta la tabla de amenazas de tipo físico presentes en un Centro de Datos, cabe indicar que las amenazas se seleccionan en base al objetivo de la Guía de Auditoría, es decir las que pueden afectar al normal funcionamiento del Centro de Datos en relación directa con la Infraestructura Física del mismo.

Tabla 13. Amenazas al Entorno Físico de un Centro de Datos

N°	Amenazas
1	Temperatura
2	Humedad
3	Fugas de líquidos o agua
4	Falta de refrigeración y falla de circulación de aire
5	Error humano y acceso del personal
6	Humo, Incendios
7	Pérdida de energía

Elaborado por: Christian Alonso Llerena Villa

Con las amenazas antes mencionadas, es necesario determinar las vulnerabilidades que se pueden presentar el la infraestructura física del Centro de Datos, que pueden afectar al mismo, por lo que se han definido las siguientes vulnerabilidades que tiene el entorno físico de un Centro de Datos:

Tabla 14. Principales Vulnerabilidades del Entorno Físico de un Centro de Datos

Vulnerabilidades
Falla en los sistemas de Aire Acondicionado
Falla o ruptura de las tuberías o desagües cercanos
Falla en el diseño arquitectónico
Falla en la distribución del aire
Falla en los dispositivos de seguridad de acceso
Falla en el suministro eléctrico
Falla en los ups o generador eléctrico
Acceso de personal no autorizado
Falla del sistema contra incendios

Elaborado por: Christian Alonso Llerena Villa

4.1.4 Cálculo de las Amenazas y Vulnerabilidades

A continuación se procede a realizar la estimación de la Probabilidad de las Amenazas. Para determinar la probabilidad se debe analizar las vulnerabilidades que pueden ser explotadas por alguna de las amenazas listadas. Con la lista de vulnerabilidades indicadas previamente, el auditor determinará la probabilidad de

ocurrencia mediante el siguiente cuestionario que le permitirá conocer el tipo de controles que existen en el Centro de Datos:

Tabla 15. Cálculo de Probabilidad relacionada a las vulnerabilidades del Centro de Datos

Ame-naza	**Cálculo de Probabilidad en relación a las vulnerabilidades.**	Si	**No**	Par-cial	**Sub Total**	Total
1	¿Se realiza periódicamente el mantenimiento del Sistema de aire acondicionado?					
	¿Continúa funcionando el Sistema de Aire acondicionado en casos de pérdida de suministro de energía?					
2	¿Se ha revisado periódicamente el estado de las tuberías de agua cercanas al Centro de Datos?					
	¿Las paredes del Centro de Datos contienen algún tipo de protección contra la humedad?					
3	¿Existen servicios higiénicos, cocinas o lugares donde exista flujo constante de agua?					
	¿Se ha revisado el estado de los desagües cercanos al Centro de Datos?					
4	¿La ubicación de los racks permite la correcta circulación del aire?					
	¿El espacio y distribución del Centro de Datos se encuentra correctamente diseñado?					
5	¿Existe un sistema de control de acceso para el Centro de Datos?					
	¿Se encuentra establecida la nómina de personal que puede acceder al Centro de Datos?					
6	¿Se realiza periódicamente el mantenimiento del Sistema contra incendios?					
	¿Se han realizado pruebas para verificar el funcionamiento del sistema contra incendios?					
7	¿Se realiza periódicamente el mantenimiento de los UPS y generador eléctrico?					
	¿Existe un estudio que demuestre que los Ups o generador eléctrico soportan la carga requerida?					

Elaborado por: Christian Alonso Llerena Villa

El criterio para valorar la probabilidad está basado en el total de la suma de los sub totales de las preguntas por cada amenaza, para lo cual el auditor utilizará el método de la entrevista o de la inspección física del Centro de Datos y con el siguiente criterio de evaluación:

- SI = 0
- NO = 2
- PARCIAL = 1

El resultado del valor total obtenido para cada amenaza en términos de probabilidad, se especifica en la siguiente tabla:

Tabla 16. Valoración de la Probabilidad de Amenaza

Valor	Significado
0	Muy bajo
1	Bajo
2	Medio
3	Alto
4	Muy alto

Elaborado por: Christian Alonso Llerena Villa

Una vez que se ha determinado el proceso para obtener el impacto de cada uno de los activos y la probabilidad que tiene cada una de las amenazas se procede a realizar la Evaluación de Riesgos, cuyos pasos son los siguientes:

4.1.5 Cálculo del Riesgo de los Activos de Información.

El cálculo de riego se realizará con el uso de la Matriz de Riesgos del Centro de Datos, el procedimiento es el siguiente:

4.1.5.1 Procedimiento para realizar el Análisis de Riesgos

1.- Identificar los activos con el uso de la tabla “Clasificación de Activos de un Centro de Datos” (tabla N°11). Los activos identificados se colocarán en la columna “Activos” de la matriz de riesgos.

2.- Realizar la tasación de cada uno de los activos en base a la importancia que representa en términos de Disponibilidad requerida para los procesos críticos de la entidad, por lo que estos valores serán utilizados como el Impacto. Los valores obtenidos con el uso de la tabla “Criterios para tasación de activos” (tabla N°12), se ubicaran en la matriz de riesgos en la columna “Impacto”.

3.- Responder al cuestionario de “Cálculo de Probabilidad relacionada a las vulnerabilidades del Centro de Datos” (tabla N°15), se utilizara el método de la entrevista o de inspección del Centro de Datos, los resultados obtenidos se colocarán en la matriz de riesgos en la fila “Probabilidad de la Amenaza”.

4.- Valorar el riesgo mediante la multiplicación del impacto de cada activo por la probabilidad de cada amenaza.

5.- Una vez que se han obtenido los valores del riesgo de cada uno de los activos se ha logrado identificar aquellos que tienen mayor riesgo en el Centro de Datos auditado y se procede a ordenarlos de mayor a menor en la tabla Prioridad de Riesgos.

MATRIZ DE RIESGOS		Temperatura	Humedad	Fugas de agua	Falta de refrigeración y falla de circulación de aire	Error humano y acceso del personal	Humo, Incendios	Pérdida de energía
Probabilidad de la Amenaza								
Activo	Impacto	Cálculo de Riesgos de los Activos						

Figura 11. Matriz para el cálculo de riesgos de los activos
Elaborado por: Christian Alonso Llerena Villa

Una vez que se han obtenido los riesgos relacionados a la Infraestructura Física del Centro de Datos para cada uno de los activos que se encuentran en el mismo, es necesario establecer la prioridad de los riesgos.

4.1.6 Evaluación e informe de la prioridad de los riesgos.

La prioridad se establece en función de los resultados obtenidos en la Matriz de Riesgos, es decir los valores más altos corresponden a los activos con mayor riesgo según cada amenaza, es decir se ordenan de mayor a menor según el riesgo obtenido en la matriz de riesgo.

Tabla 17. Prioridad de los riesgos

Activo	Valor de Riesgo	Amenaza

Elaborado por: Christian Alonso Llerena Villa

Una vez que el auditor ha identificado los activos que tienen alto riesgo de sufrir alguna falla asociada a las amenazas que existen en la Infraestructura Física del Centro de Datos, es menester tomar las medidas correspondientes para mitigar el riesgo, para esto se utilizará el estándar principal en el diseño e implementación de Centros de Datos, el estándar TIA 942, ya que el mismo contiene los lineamientos que ayudan a garantizar que la Infraestructura Física proteja correctamente a los activos que se encuentran en el Centro de Datos.

4.2 Procedimientos para realizar la auditoria del Centro de Datos

Para realizar la auditoria de un Centro de Datos, el Auditor primeramente analizará los riesgos en el Centro de Datos, luego verificará el cumplimiento de los requerimientos generales que aplican para todos los Centros de Datos sin importar el

nivel de disponibilidad requerido, y posteriormente evaluará los requerimientos específicos que se detallan para cada uno de los tipos de Centros de Datos.

Para esto procederá a realizar la revisión de las instalaciones con el fin de constatar la existencia de cada uno de los requerimientos que se mencionan a continuación. Cabe indicar que por cada requerimiento se procede a definir el procedimiento para verificar el cumplimiento del mismo, adicionalmente se debe indicar que los requerimientos indicados para cada tipo de Centro de Datos provienen de la realización de un resumen del anexo G del estándar TIA 942 (*Data Center Infraestructure Tiers*), considerando los principales factores que se deben verificar al momento de auditar la infraestructura del Centro de Datos.

Es importante recalcar que algunos requerimientos del estándar se pueden cumplir únicamente cuando la construcción del Centro de Datos estuvo realizada con los lineamientos del estándar desde la fase de diseño del mismo, por tal razón no se consideran los requerimientos que pueden generar recomendaciones que contengan cambios mayores a nivel arquitectónico.

También se debe considerar que cada uno de los niveles de los tipos de Centros de Datos que se proponen y acorde a lo indicado en el estándar, dispone de un nivel de redundancia en sus componentes, la clasificación de la redundancia de los componentes se expresa con la letra N, la cual proviene de "*Need",* es decir, la necesidad de redundancia de los componentes, como se muestra en la siguiente tabla:

Tabla 18. Redundancia de la infraestructura

Redundancia	Necesidad de redundancia de la infraestructura
N	Requerimiento básico sin redundancia
N+1	Provee una módulo, unidad, vía o sistema adicional al requerimiento básico.
N+2	Provee dos módulos, unidades, vías o sistemas adicionales al requerimiento básico.
2 N	Provee dos unidades completas, vías o sistemas por cada uno de los requerimientos básicos.
2 (N+1)	Provee dos unidades completas, vías o sistemas de tipo N+1.

Elaborado por: Christian Alonso Llerena Villa

En base a las definiciones de redundancia indicadas, cada nivel o tipo de Centro de Datos tiene las siguientes características:

Centro de Datos Tipo 1 – TIER 1

- Susceptible a las interrupciones tanto planificadas y actividad planificada.
- Ruta Individual de poder y de distribución de refrigeración, no dispone de componentes redundantes (N).
- Puede o no tener un piso elevado, UPS o generador, ya que es un requerimiento recomendado.
- Tiempo de inactividad anual de 28,8 horas.
- Se debe cerrar completamente para realizar un mantenimiento preventivo.

Centro de Datos Tipo 2 - Componentes redundantes (N+1):

- Es menos susceptible a la interrupción de ambos planificada y actividad planificada.
- Ruta individual por el poder y la interrupción de refrigeración, incluye componentes redundantes (1 N).

- Incluye un piso elevado, UPS y generador.
- Toma de 3 a 6 meses para poner en práctica.
- Tiempo de inactividad anual de 22,0 horas.
- Mantenimiento de la trayectoria de alimentación y otras partes de la infraestructura requiere una parada de procesamiento.

Centro de Datos Tipo 3 - Mantenible al mismo tiempo:

- Permite la actividad planeada sin interrumpir el funcionamiento de los ordenadores y hardware, pero los eventos no planificados seguirán causando interrupciones.
- Múltiples rutas de distribución de energía y enfriamiento, pero con solamente una trayectoria activa, incluye componentes redundantes(N +1).
- Toma de 15 a 20 meses para implementar.
- Tiempo de inactividad anual de 1,6 horas.
- Incluye un piso elevado y suficiente capacidad y distribución para llevar carga por una ruta mientras se realiza el mantenimiento de la otra.

Centro de Datos Tipo 4 - Tolerancia a fallos

- Las actividades planificadas no interrumpen el suministro a los componentes críticos y el Centro de Datos puede sostener al menos un evento no planeado, sin impacto en la carga crítica.
- Múltiples fuentes de alimentación activas y rutas de distribución de refrigeración, incluye componentes redundantes (2 N +1), por ejemplo 2 UPS cada uno con redundancia N +1.
- Toma de 15 a 20 meses para implementar.
- Tiempo de inactividad anual de 0,4 horas.

Una vez que se han dado a conocer los lineamientos bajo los cuales se procederá a la verificación de los componentes de la infraestructura y se detalla en modo general las especificaciones de cada uno de los Centros de Datos, se procede a definir un conjunto de requerimientos generales que se aplican para los mismos, independiente del tipo o nivel de disponibilidad al que se haga referencia.

Los requerimientos generales permitirán realizar un análisis de la infraestructura básica del Centro de Datos y posteriormente se realizará un análisis más detallado evaluando el mismo con el nivel requerido.

Los requerimientos generales se detallan a continuación, y el cumplimiento o no de los mismos serán anotados en el respectivo casillero.

Tabla 19 Tabla de requerimientos generales para un Centro de Datos

REQUERIMIENTOS GENERALES	**SI**	**NO**
El administrador del Centro de Datos dispone de un estudio de la carga del suelo		
Existen espacios libres a los lados de los equipos que se encuentran en el cuarto de equipos		
¿Se constata que existe un correcto flujo del aire al verificar la ubicación de las bandejas de cables dentro del piso elevado?		
¿Existen estudios eléctricos que determinen la correcta alimentación de corriente hacia los equipos?		
¿Se cumple con requisitos de longitud de la conexión entre equipos?		
¿Están los equipos situados lejos de fuentes de interferencia electromagnética?		
El cuarto de equipos no debe tener ventanas al exterior		
El cuarto de equipos debe contar con puertas que faciliten el acceso sólo al personal autorizado		
Se permite el hospedaje en el cuarto de equipos de los equipos de control eléctrico, tales como distribución de energía o sistemas acondicionamiento y UPS hasta 100 kVA		
Los pisos, paredes y techos deberán ser sellados, pintados o construidos de un material para minimizar el polvo. Los acabados deben ser de color claro para mejorar la iluminación de la habitación y los pisos deben tener propiedades anti- estáticas.		
Las luminarias no deben ser alimentadas desde el mismo panel de distribución eléctrica de los equipos de telecomunicaciones		
Debe existir señalización de salidas y emergencia igual a las de todo el edificio		

Continúa…

REQUERIMIENTOS GENERALES	SI	NO
El sistema de climatización del cuarto de equipos debe ser soportado por el generador eléctrico del cuarto de equipos o generador del edificio		
La temperatura en el cuarto de equipos estará dentro del rango de: 18 °C a 27 °C		
¿Se analizó que no existan vibraciones mecánicas junto a los equipos que pueden provocar fallas en los servicios?		
Se proveerán circuitos de alimentación separados para servir al cuarto de equipos.		
El cuarto de equipos debe tener tomacorrientes dúplex (120V 20A) para las herramientas eléctricas, equipos de limpieza para no utilizar las tomas de los gabinetes		
La distancia desde el punto de demarcación hacia los equipos terminales no excede la distancia máxima de longitud de los cables		
En el cuarto de equipos existen receptáculos de energía suficientes para todo el hardware?		
Las longitudes de cable para el cableado de punto a punto entre los equipos en el área de distribución de equipos deben ser inferiores a 15 metros		
Existe un mínimo de 1 m de espacio delantero proveído para la instalación de nuevos equipos y 0.6 m de espacio trasero		
Existen extintores portátiles en el Centro de Datos, los mismos que deben contar con la fecha de caducidad		
¿La ubicación de los racks es adecuada para que se creen pasillos calientes y fríos?		
La altura máxima de los racks en el cuarto de equipos es de 2.4 metros		
Todas las cajas de revisión de las rutas del cableado se encuentran cerrados con llave		

Elaborado por: Christian Alonso Llerena Villa

Una vez que el Auditor Informático ha realizado la evaluación de los requerimientos generales, procederá a verificar los requerimientos específicos del Centro de Datos mediante la constatación del cumplimiento de cada uno de los ítems, la tabla consta del requerimiento puntual de la infraestructura física, junto con el parámetro que será evaluado, la columna control indica la forma en que se evaluará el cumplimiento de dicho parámetro y en el casillero de SI y No se anotará el cumplimiento.

4.2.1 Guía para auditar un Centro de Datos tipo I

El auditor procederá a verificar el cumplimiento de cada uno de los ítems:

REQUERIMIENTO	PARÁMETRO	CONTROL	CUMPLIMIENTO SI/NO	
TELECOMUNICACIONES				
Se revisaran los requerimientos generales del estándar en cuanto a longitud de cableado y vías.	SI	En base a los requerimientos detallados en el análisis del estándar TIA 942		
El cableado, racks y gabinetes deben estar correctamente etiquetados	SI	Se verificará que todos los cables se encuentren correctamente etiquetados		
ARQUITECTONICO				
Resistencia al fuego	Según la norma	Se consultará los lineamientos básicos del Cuerpo de Bomberos		
Altura del techo	2.6 m mínimo	Se medirá con el uso de un flexómetro		
Tamaño de la puerta	1m de ancho y 2.13 de alto mínimo	Se medirá con el uso de un flexómetro		
Oficinas Administrativas				

Separaciones anti fuego de otras áreas del Centro de Datos	Según la norma	Se recomienda la separación de áreas especialmente el Cuarto de Equipos		
Control de acceso de seguridad				
Cuarto de UPS, Salidas de emergencia, Centro de Operaciones	Cerradura de tipo industrial	Se verificara la cerradura instalada		
Puertas en el cuarto de equipos	Cerradura de tipo industrial	Se verificara la cerradura instalada		
Monitoreo CCTV	Opcional	Se recomienda la instalación de un CCTV		
Carga de peso sobre el piso elevado	150 lbf/ sq ft	Se revisaran las especificaciones técnicas o se solicitara al proveedor		
ELÉCTRICO				
Número de vías de distribución	1	No se requiere más de una		
Entrada de servicios	1	La entrada deberá cumplir los requerimientos generales de área de Entrada de Servicios		
Certificación del cableado eléctrico	SI	Se solicitará certificar el cableado		
Puntos de falla	1 o mas	Se citara al menos 3 puntos de falla		

Sistema de Transferencia de Carga Eléctrica	SI	Verificar q disponga de un switch de transferencia automática		
Generado Eléctrico	Opcional	Se comprobara su funcionamiento en caso de existir		
Generadores de tamaño adecuado según la capacidad de UPS	SI	Se analizara la capacidad del UPS y del generador con sus respectivas hojas de especificaciones		
Capacidad del generador	8 horas (si los UPS tienen respaldo de 8 minutos no es necesario el generador)	Se verificara con la respectiva hoja de especificaciones		
Ups				
Nivel de voltaje	120/208V en cargas de hasta 1440 kVA y 480V para cargas mayores a 1440 kVA	Se verificara con la respectiva hoja de especificaciones		
Apagado de fuente de alimentación de ventiladores	SI	Se verificara con la respectiva hoja de especificaciones		
Visor de monitoreo en el UPS	SI	Se debe inspeccionar el UPS y determinar el cumplimiento		
Baterías				

Tiempo mínimo de espera en carga completa	5 minutos	Se realizara una prueba del estado de las baterías en horario programado		
Contenedor para derrames	SI	Se verificará que las baterías dispongan de un contenedor		
Test de carga de la batería	Cada 2 años	Se solicitará los informes de mantenimiento		
MECÁNICOS				
Evitar tuberías de agua no asociadas al Centro de Datos	SI	Se recomendará si es posible la reubicación de las tuberías de agua		
Desagües en el Cuarto de Equipos	SI	Se verificará que existan desagües en el Centro de Datos		
Control de humedad en el Cuarto de Equipos	SI	Se utilizará las opciones del aire acondicionado para verificar la humedad		
Humedad Relativa	30% a 60%	Se utilizará las opciones del aire acondicionado para verificar la humedad		

Temperatura del ambiente	18° C a 27° °C	Se utilizará un termómetro para constatar la temperatura ambiente		
Servicio eléctrico a los equipos mecánicos	Una vía	El tendido eléctrico de una vía es aceptado		
Terminales de aire acondicionado	SI	Se requiere constatar que exista al menos una		
Supresor de Fuego				
Sistema supresor de fuego	No	No se requiere sistema anti fuego		

4.2.2 Guía para auditar un Centro de Datos tipo II

El auditor procederá a verificar el cumplimiento de cada uno de los ítems:

REQUERIMIENTO	PARÁMETRO	CONTROL	CUMPLIMIENTO SI/NO	
TELECOMUNICACIONES				
Se revisaran los requerimientos generales del estándar en cuanto a longitud de cableado y vías.	SI	En base a los requerimientos detallados en el análisis del estándar TIA 942		

El cableado, racks y gabinetes deben estar correctamente etiquetados	SI	Se verificará que todos los cables se encuentren correctamente etiquetados		
ARQUITECTONICO				
Resistencia al fuego	Según la norma	Se consultará los lineamientos básicos del Cuerpo de Bomberos		
Altura del techo	2.6 m mínimo	Se medirá con el uso de un flexómetro		
Tamaño de la puerta	1m de ancho y 2.13 de alto mínimo	Se medirá con el uso de un flexómetro		
Oficinas Administrativas				
Separaciones anti fuego de otras áreas del Centro de Datos	SI	Se recomienda la separación de áreas especialmente el Cuarto de Equipos		
Control de Acceso de Seguridad				
Cuarto de UPS, Salidas de emergencia, Centro de Operaciones	Cerradura de tipo industrial	Se verificara la cerradura instalada		
Puertas en el cuarto de equipos	Cerradura de tipo industrial	Se verificara la cerradura instalada		
Monitoreo CCTV	No es indispensable	Se recomienda la instalación de un CCTV		
Carga de peso sobre el piso elevado	150 lbf/ sq ft	Se revisaran las especificaciones técnicas o se solicitara al proveedor		
ELÉCTRICO				
Número de vías de distribución	1	No se requiere más de una		

Entrada de servicios	1	La entrada deberá cumplir los requerimientos generales de área de Entrada de Servicios		
Certificación del cableado eléctrico	SI	Se solicitará certificar el cableado		
Puntos de falla	1 o mas	Se identificará al menos 3 puntos de falla		
Sistema de Transferencia de Carga Eléctrica	SI	Verificar q disponga de un switch de transferencia automática		
Generado Eléctrico	Opcional	Se comprobara su funcionamiento en caso de existir		
Generadores de tamaño adecuado según la capacidad de UPS	SI	Se analizara la capacidad del UPS y del generador con sus respectivas hojas de especificaciones		
Capacidad del generador	8 horas (si los UPS tienen respaldo de 8 minutos no es necesario el generador)	Se verificara con la respectiva hoja de especificaciones		
UPS				
Nivel de voltaje	120/208V en cargas de hasta 1440 kVA y 480V para cargas mayores a 1440 kVA	Se verificara con la respectiva hoja de especificaciones		
Apagado de fuente de alimentación de ventiladores	SI	Se verificara con la respectiva hoja de especificaciones		
Visor de monitoreo en el UPS	SI	Se debe inspeccionar el UPS y determinar el cumplimiento		
Baterías				

Tiempo mínimo de espera en carga completa	5 minutos	Se realizara una prueba del estado de las baterías en horario programado		
Contenedor para derrames	SI	Se verifica que las baterías dispongan de un contenedor		
Test de carga de la batería	Cada 2 años	Se solicitara los informes de mantenimiento		
MECÁNICOS				
Evitar tubería de agua no asociadas al Centro de Datos	SI	Se recomendara si es posible la reubicación de las tuberías de agua		
Desagües en el Cuarto de Equipos	SI	Se verificara que existan desagües en el Centro de Datos		
Control de humedad en el Cuarto de Equipos	SI	Se utilizara las opciones del aire acondicionado para verificar la humedad		
Humedad Relativa	30% a 60%	Se utilizara las opciones del aire acondicionado para verificar la humedad		
Temperatura del ambiente	18° C a 27° °C	Se utilizara un termómetro para constatar la temperatura ambiente		
Servicio eléctrico a los equipos mecánicos	Una vía	El tendido eléctrico de una vía es aceptado		
Terminales de aire acondicionado	SI	Se requiere constatar que exista al menos una		
Supresor de Fuego				
Sistema supresor de fuego	No	No se requiere sistema anti fuego		

4.2.3 Guía para auditar un Centro de Datos tipo III

El auditor procederá a verificar el cumplimiento de cada uno de los ítems:

REQUERIMIENTO	PARÁMETRO	CONTROL	CUMPLIMIENTO SI/NO	
TELECOMUNICACIONES				
cableado, racks, gabinetes correctamente etiquetados	Si	Se verificará que todos los componentes del cableado se encuentren correctamente etiquetados		
entradas de acceso de servicios con rutas diversas y pozos de mantenimiento con un mínimo de 20 m de separación	Si	Se verificará que exista más de una entrada de servicios con rutas distintas		
entrada secundaria	Si	Se verificará q exista entrada adicional de servicios		
Rutas de cableado vertical (backbone) redundantes.	Si	Se verificará el cableado de backbone		
Routers y switches tienen fuentes de poder y procesadores redundantes	Si	Se verificará que los routers y switches cumplan este requerimiento		
múltiples routers y switches para redundancia	Si	Se verificará que los routers y switches cumplan este requerimiento		
ARQUITECTÓNICO				
requerimientos de resistencia al fuego		Verificar que exista algún elemento que brinde resistencia al fuego		
paredes de partición del cuarto de equipos interno	1 hora mínimo			
techo y techo falso	1 hora mínimo			

componentes de construcción				
barreras de vapor para paredes y techo del cuarto de equipos	Si	Verificar que exista algún elemento que brinde resistencia al paso del vapor de agua		
construcción del panel de piso	todo de acero	Se verificará la estructura del panel		
techo falso en el cuarto de equipos				
altura de techo	3m mínimo, no menos de 46 cm sobre el equipo más alto	Se medirá con el uso de un flexómetro		
puertas y ventanas				
tamaño de la puerta	No menos que 1m de ancho en el cuarto de equipos, eléctrico y mecánico. No menos que 2.13 m de alto	Se medirá con el uso de un flexómetro		
la construcción provee protección contra radiación electromagnética	SI	Se verificará que exista protección electromagnética		
oficinas administrativas				
físicamente separado de otras áreas del centro de datos	SI	Se realizará la inspección del sitio		
oficina de seguridad	SI	Se verificará que exista una oficina de seguridad		
centro de operaciones	SI	Se verificará que exista un cuarto de operaciones		
baños y áreas de descanso				
proximidad al cuarto de equipos y áreas de soporte	si están inmediatamente al lado, deben estar provistas de una barrera de prevención de fugas	Se realizará la inspección del sitio		

UPS y cuarto de Baterías				
ancho de pasillos para mantenimiento, reparación o para remover equipos	No menos de un metro	Se realizará la inspección del sitio		
proximidad al cuarto de equipos	inmediatamente adyacentes	Se realizará la inspección del sitio		
áreas de almacenamiento de combustible y generadores				
proximidad al cuarto de equipos y áreas de soporte	si está dentro del edificio del centro de datos, debe estar provista con un mínimo de 2 horas de separación de fuego de las otras áreas	Se verificará que exista algún elemento retardante de fuego		
Seguridad				
personal de seguridad por turno	Al menos 1	Se realizará la indagación sobre el personal por turno		
control de accesos de seguridad y monitoreo en:				
Generadores	detección de intrusos	Se verificará la existencia del control de accesos		
cuartos de UPS, telefonía y MEP	tarjeta de acceso	Se verificará la existencia del control de accesos		
puertas de salida de emergencia	puertas con código	Se verificará la existencia del control de accesos		
ventanas o aberturas accesibles desde el interior	detección de intrusos	Se verificará la existencia del control de accesos		
centro de operaciones de seguridad	tarjeta de acceso	Se verificará la existencia del control de accesos		

centro de operaciones de red	tarjeta de acceso	Se verificará la existencia del control de accesos		
cuartos de equipamiento de seguridad	tarjeta de acceso	Se verificará la existencia del control de accesos		
puertas en el cuarto de equipos	acceso con tarjeta o biométrico para entrada y salida	Se verificará la existencia del control de accesos		
monitoreo cctv				
perímetro del edificio y parqueaderos	SI	Se verificará la existencia de cámaras		
Generadores	SI	Se verificará la existencia de cámaras		
puertas de control de acceso	SI	Se verificará la existencia de cámaras		
pisos del cuarto de computadores	SI	Se verificará la existencia de cámaras		
cuarto de UPS, telefonía y MEP	SI	Se verificará la existencia de cámaras		
Cctv				
cctv grabando toda la actividad de todas las cámaras	Sí; digital	Se verificará que se cumpla este requerimiento		
tasa de grabación (cuadros por segundo)	20 frames/secs (min)	Se verificará que se cumpla este requerimiento		
ELÉCTRICO				
número de vías de entrega	1 activa y 1 pasiva	Se verificará que existan las vías requeridas		
el sistema permite mantenimiento concurrente	Si	Se verificará las especificaciones del sistema		
equipo del sistema eléctrico etiquetado y certificado	Si	Se verificará que se cumpla este requerimiento		
sistema de transferencia para cargas criticas	switch de transferencia automática con bypass de	Se verificará que se cumpla este requerimiento, para lo		

	mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	cual se harán las pruebas programadas quitando el suministro eléctrico		
capacidad de combustible del generador (a carga completa)	72 horas	Se revisarán las hojas de especificaciones		
Ups				
redundancia de ups	N+1			
topología de ups	módulos redundantes en paralelo o módulos redundantes distribuidos o sistema de bloque redundante	Se revisarán las hojas de especificaciones		
alimentación Ups para todo los equipos de computación y telecomunicaciones	Si	Se verificara el diagrama de instalación del Ups		
Puesta a tierra				
sistema pararrayos	Si	Se verificará el cumplimiento de este requerimiento		
infraestructura de data center aterrizada	Si	Se verificará el cumplimiento de este requerimiento		
monitoreo de sistema				
método de notificación	consola, email, mensaje de	Se verificará que exista algún		

	texto	método de notificación		
configuración de baterías				
tiempo mínimo de stand by a carga completa	15 minutes	Se realizarán las pruebas requeridas		
contenedor de derrames de acido	Si	Se verificará la existencia del contenedor requerido		
pruebas de batería a carga completa/calendario de inspección	cada 2 años	Se solicitará las hojas de los mantenimientos realizados		
cuarto de baterías				
separado del cuarto de equipos	Si	Se verificará el cumplimiento de este requerimiento		
cadenas individuales de batería aisladas unas de otras	Si	Se verificará el cumplimiento de este requerimiento		
sistema de monitoreo de baterías	Auto monitoreo de UPS	Se verificará el cumplimiento de este requerimiento		
sistemas de generación en stand by				
dimensionamiento del generador	dimensionado para toda la carga del edificio con redundancia N+1	Se verificará el análisis para el dimensionamiento del generador		
mantenimiento de equipo				
personal de mantenimiento	24 horas en sitio de lunes a viernes, fines de semana con llamada	Se solicitará la información y se verificará que se cumpla el requerimiento		
mantenimiento preventivo	programa de mantenimiento preventivo limitado	Se verificará el cumplimiento del programa de mantenimiento		

MECÁNICOS				
rutas de tuberías de agua y desagüe no asociada al equipo del data center en los espacios del data center	no permitido	Se verificará el cumplimiento de este requerimiento con los planos del edificio		
drenaje de piso en el cuarto de computación para drenar agua condensada, agua del humidificador y agua de la descarga de los aspersores	Si	Se verificará el cumplimiento de este requerimiento con los planos del edifico		
servicio eléctrico para el equipamiento mecánico	caminos múltiples de energía eléctrica para equipos de a/c conectados en forma de tablero para redundancia de enfriamiento	Se verificará el cumplimiento de este requerimiento		
sistema de control HVAC				
sistema de control	si falla el control del sistema, no se detendrá el enfriamiento de las áreas criticas	Se verificará el cumplimiento de este requerimiento		
fuente de poder para el sistema de control HVAC	redundante, fuente eléctrica de ups para equipo de HVAC	Se verificará el cumplimiento de este requerimiento		
sistema de combustible				
tanque de almacenamiento de volumen	múltiples tanques de almacenamiento	Se verificará que existe más de un tanque de almacenamiento		

supresión de fuego				
sistema de detección de incendios	Si	Se verificará que exista un sistema de detección de incendios		
sistema de aspersores	pre acción cuando se requiere	Se verificará que existan aspersores		
sistema de detección de derrames de agua	Si	Se verificará que existan sensores de nivel de agua		

4.2.4 Guía para auditar un Centro de Datos tipo IV

El auditor procederá a verificar el cumplimiento de cada uno de los ítems:

REQUERIMIENTO	PARÁMETRO	CONTROL	CUMPLIMIENTO SI/NO	
TELECOMUNICACIONES				
cableado, racks, gabinetes correctamente etiquetados	SI	Se verificará que todos los componentes del cableado se encuentren correctamente etiquetados		
entradas de acceso de servicios con rutas diversas y pozos de mantenimiento con un mínimo de 20 m de separación	SI	Se verificará que exista más de una entrada de servicios con rutas distintas		
entrada secundaria	SI	Se verificará q exista entrada adicional de servicios		
Rutas de cableado vertical (backbone) redundantes.	SI	Se verificará el cableado de backbone		
Routers y switches tienen fuentes de poder y procesadores redundantes	SI	Se verificará que los routers y switches cumplan este requerimiento		
múltiples routers y switches para redundancia	SI	Se verificará que los routers y switches cumplan este requerimiento		
Patchcords y jumpers etiquetados en ambos extremos con el nombre de la conexión en los dos extremos del cable	SI	Se verificará el cumplimiento de este requerimiento		
ARQUITECTÓNICO				
Parqueaderos				
áreas de parqueo separadas para visitantes y empleados	Si, físicamente separado por una pared o muro	Se verificara el cumplimiento de este requerimiento		

separación de estaciones de carga	Si, físicamente separado por una pared o muro	Se verificara el cumplimiento de este requerimiento		
proximidad del parqueadero de visitas al perímetro del edificio del data center	18.3 m y con muros de división que prevengan que los vehículos circules cerca al centro de datos	Se verificara el cumplimiento de este requerimiento		
construcción del edificio				
requerimientos de resistencia al fuego		Verificar que exista algún elemento que brinde resistencia al fuego		
paredes de partición para los cuartos interiores que no son del cuarto de equipos	1 hora mínimo			
paredes de partición del cuarto de computadores interno	2 horas mínimo			
recintos cerrados	2 horas mínimo			
techo y techo falso	2 horas mínimo			
piso y piso falso	2 horas mínimo			
componentes de construcción				
barreras de vapor para paredes y techo del cuarto de equipos	Si	Verificar que exista algún elemento que brinde resistencia al paso del vapor de agua		
múltiples entradas al edificio con puntos de revisión de seguridad	Si	Se verificará la estructura del panel		
construcción del panel de piso	Todo de acero o relleno de concreto	Se verificará el material de los paneles del piso		
techo falso en las áreas de computación				
altura de techo	3 m mínimo	Se medirá con el uso de un flexómetro		
puertas y ventanas				
clasificación para fuego	No menos de 1 1/2 horas en el cuarto de equipos)	Verificar que exista algún elemento que brinde resistencia al paso del vapor de agua		

tamaño de la puerta	No menos de 1.2 m de ancho y 2.13m alto	Se medirá con el uso de un flexómetro		
la construcción provee protección contra radiación electromagnética	Si	Se verificará si existe protección contra radiación electromagnética		
lobby de entrada	Si			
físicamente separado de otras áreas del data center	Si	Se verificará el cumplimiento de este requerimiento		
mostrador de seguridad	Si	Se verificará el cumplimiento de este requerimiento		
oficinas administrativas				
físicamente separado de otras áreas del data center	Si	Se realizará la inspección del sitio		
oficina de seguridad	Si	Se verificará que exista una oficina de seguridad		
visión de 180 grados en equipo de seguridad y cuarto de monitoreo	Si			
centro de operaciones	Si	Se verificará que exista un cuarto de operaciones		
físicamente separado de otras áreas del data center	Si	Se verificará el cumplimiento de este requerimiento		
proximidad al cuarto de computación	Accesible directamente	Se verificará el cumplimiento de este requerimiento		
baños y áreas de descanso				
proximidad al cuarto de computación y áreas de soporte	Si están inmediatamente al lado, deben estar provistas de una barrera de prevención de fugas	Se realizará la inspección del sitio		
área de envió y recepción				
físicamente separado de otras áreas del data center	Si	Se verificará el cumplimiento de este requerimiento		
número de estaciones de carga	1	Se verificará el cumplimiento de este requerimiento		

estaciones de carga separadas de las áreas de parqueo	Si, separadas con pared	Se verificará el cumplimiento de este requerimiento		
counter de seguridad	Si	Se verificará el cumplimiento de este requerimiento		
áreas de almacenamiento de combustible y generadores				
proximidad al cuarto de computación y áreas de soporte	si está dentro del edificio del centro de datos, debe estar provista con un mínimo de 2 horas de separación de fuego de las otras áreas	Se verificará que exista algún elemento retardante de fuego		
proximidad a áreas de acceso al publico	mínimo 19 m de separación	Se verificará el cumplimiento de este requerimiento		
Seguridad				
capacidad ups de equipo de campo	generador del edificio + baterías de 24 horas mínimo	Se verificará con las hojas de especificaciones de los equipos		
personal de seguridad de turno en horario laborable	2	Se realizará la indagación sobre el personal por turno		
personal de seguridad por turno	Al menos 1	Se realizará la indagación sobre el personal por turno		
control de accesos de seguridad y monitoreo en:				
Generadores	detección de intrusos	Se verificará la existencia del control de accesos		
cuartos de UPS, telefonía y MEP	tarjeta de acceso	Se verificará la existencia del control de accesos		
puertas de salida de emergencia	puertas con código	Se verificará la existencia del control de accesos		
ventanas o aberturas accesibles desde el interior	detección de intrusos	Se verificará la existencia del control de accesos		
centro de operaciones de seguridad	tarjeta de acceso	Se verificará la existencia del control de accesos		

centro de operaciones de red	tarjeta de acceso	Se verificará la existencia del control de accesos		
cuartos de equipamiento de seguridad	tarjeta de acceso	Se verificará la existencia del control de accesos		
puertas en los cuartos de computación	acceso con tarjeta o biométrico para entrada y salida	Se verificará la existencia del control de accesos		
puertas en el perímetro del edificio	tarjeta de acceso si existen puertas	Se verificará la existencia del control de accesos		
monitoreo cctv				
perímetro del edificio y parqueaderos	Si	Se verificará la existencia de cámaras		
Generadores	Si	Se verificará la existencia de cámaras		
puertas de control de acceso	Si	Se verificará la existencia de cámaras		
pisos del cuarto de computadores	Si	Se verificará la existencia de cámaras		
cuarto de UPS, telefonía y MEP	Si	Se verificará la existencia de cámaras		
Cctv				
cctv grabando toda la actividad de todas las cámaras	Sí; digital	Se verificará que se cumpla este requerimiento		
tasa de grabación (cuadros por segundo)	20 frames/secs (min)	Se verificará que se cumpla este requerimiento		
Estructural				
equipo de comunicaciones racks/ gabinetes anclados a la base o con soporte en la base y arriba	Totalmente abrazado	Se verificará que se cumpla este requerimiento		
capacidad de carga del piso superpuesta la carga activa	12 kPa (250 Ibf/sq ft)	Se verificará el estudio de implementación del piso		
capacidad de carga del piso para cargas suspendidas desde la parte inferior	2.4 kPa (50 Ibf/sq ft)	Se verificará el estudio de implementación del piso		
ELÉCTRICO				

número de vías de entrega	2 activas	Se verificará que existan las vías requeridas		
el sistema permite mantenimiento concurrente	Si	Se verificará las especificaciones del sistema		
equipo del sistema eléctrico etiquetado con certificación de un laboratorio de pruebas	Si	Se verificará que se cumpla este requerimiento		
puntos de falla simples	No deben existir puntos simples de falla en los sistemas de distribución eléctrica	Se verificará las instalaciones y comprobar que no existan puntos de falla simples		
sistema de transferencia para cargas criticas	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	Se verificará que se cumpla este requerimiento, para lo cual se harán las pruebas programadas quitando el suministro eléctrico		
generadores correctamente dimensionados de acuerdo a la capacidad instalada de UPS	Si	Se verificará los estudios para la implementación del generador		
capacidad de combustible del generador (a carga completa)	96 horas.	Se verificará con la hoja de especificaciones del generador		
ups				
redundancia de ups	2N			
topología de ups	módulos redundantes en paralelo o módulos redundantes distribuidos o sistema de bloque redundante	Se revisarán las hojas de especificaciones		
bypass de mantenimiento de ups	Energía tomada de un Ups de reserva alimentado con un bus diferente	Se verificará la topología del sistema de ups		

distribución de energía del ups y nivel de voltaje	Nivel de voltaje de 120/208 V para cargas de hasta 1440 kVA y 480 V para cargas mayores a 1440 kVa	Se verificara con la hoja de especificaciones del ups		
alimentación Ups para todo el equipo de computación y telecomunicaciones	Si	Se verificará los diagramas de conexión de los ups		
ups en paneles de distribución separados para equipos de computación y telecomunicaciones	Si	Se verificará el cumplimiento de este requerimiento		
Puesta a tierra				
sistema pararrayos	Si	Se verificará el cumplimiento de este requerimiento		
entrada de tierra de servicios y tierra de generadores completamente de acuerdo a la normativa correspondiente	Si	Se verificará el cumplimiento en base al análisis de los estudios de implementación		
infraestructura de data center aterrizada	Si	Se verificará el cumplimiento de este requerimiento		
monitoreo de sistema				
display local en el ups	Si	Se verificará los ups		
método de notificación	consola, email, mensaje de texto	Se verificará el cumplimiento de este requerimiento		
control remoto	Si	Se verificará el cumplimiento de este requerimiento		
envió de mensajes de texto automático a los ingenieros de servicios	Si	Se verificará el cumplimiento de este requerimiento		
configuración de la batería				
cadena común de batería para todos los módulos	No	Se verificará el diagrama de instalación de ups		
una cadena de batería por modulo	Si	Se verificará la hoja de especificaciones del ups		
tiempo mínimo de stand by a carga completa	15 minutos	Se verificará la hoja de especificaciones del ups		

contenedor de derrames de acido	Si	Se verificará la existencia del contenedor requerido		
pruebas de batería a carga completa/calendario de inspección	Anualmente	Se solicitará las hojas de los mantenimientos realizados		
Cuarto de baterías				
separado del cuarto de equipos	Si	Se verificará el cumplimiento de este requerimiento		
cadenas individuales de batería aisladas unas de otras	Si	Se verificará el cumplimiento de este requerimiento		
vidrio a prueba de golpes en la puerta del cuarto de baterías	Si	Se verificará el cumplimiento de este requerimiento		
sistema de monitoreo de baterías	Sistema centralizado para chequear la temperatura, voltaje e impedancia de cada celda	Se verificara la hoja de especificaciones del sistema de monitoreo de baterías		
recinto del sistema de ups rotativo (con generadores de diésel)				
unidades separadas por paredes anti fuego	Si	Se verificará el cumplimiento de este requerimiento		
tanques de combustible en el exterior	Si	Se verificará el cumplimiento de este requerimiento		
tanques de combustible en la misma habitación que las unidades	No	Se verificará el cumplimiento de este requerimiento		
sistemas de generación en stand by				
dimensionamiento del generador	Dimensionado con la carga total del edificio con redundancia 2N	Se verificara con los estudios de implementación del generador		
generadores en un solo bus	No	Se verificará el diagrama de instalación de los generadores		
mantenimiento de equipo				

personal de mantenimiento	En sitio 24/7	Se solicitará la información y se verificará que se cumpla el requerimiento		
mantenimiento preventivo	programa de mantenimiento preventivo limitado	Se verificará el cumplimiento del programa de mantenimiento		
MECÁNICOS				
rutas de tuberías de agua y desagüe no asociada al equipo del data center en los espacios del data center	No permitido	Se verificará el cumplimiento de este requerimiento		
drenaje de piso en el cuarto de computación para drenar agua condensada, agua del humidificador y agua de la descarga de los aspersores	Si	Se verificará el cumplimiento de este requerimiento con la inspección al sitio		
sistema de enfriamiento de agua o aire				
unidades terminales de aire acondicionado interiores	cantidad de unidades de a/c suficiente para mantener al área critica durante la perdida de una fuente de energía eléctrica	Se verificará el análisis de implementación de Aire acondicionado		
servicio eléctrico para el equipamiento mecánico	múltiples caminos para energía eléctrica para el equipo de a/c	Se verificará el diagrama de instalación del servicio eléctrico		
sistema de tuberías	múltiples tubos de suministro	Se verificará el diagrama de implementación del sistema de enfriamiento		
sistema de control HVAC				
sistema de control	si falla el control del sistema, no se detendrá el enfriamiento de las áreas criticas	Se verificará el cumplimiento de este requerimiento		
fuente de poder para el sistema de control HVAC	redundante, fuente eléctrica de ups para equipo de HVAC	Se verificará el cumplimiento de este requerimiento		
sistema de combustible				

tanque de almacenamiento de volumen	múltiples tanques de almacenamiento	Se verificará que existe más de un tanque de almacenamiento		
supresión de fuego				
sistema de detección de incendios	Si	Se verificará que exista un sistema de detección de incendios		
sistema de aspersores	Pre-activados cuando sea requerido	Se verificará que existan aspersores		
sistema de supresión de gases	Si	Se verificará que existan supresores de gases		
sistema de detección de humo	Si	Se verificará que existan sensores para detección de humo		
sistema de detección de derrames de agua	Si	Se verificará que existan sensores de nivel de agua		

Una vez que el Auditor Informático ha realizado la evaluación de los requerimientos generales y específicos de las instalaciones del Centro de Datos auditado, procederá a realizar el análisis de los resultados obtenidos, los mismos que le permitirán obtener el Nivel de Madurez, el cual permite tener los fundamentos para generar las conclusiones y recomendaciones pertinentes.

4.3 Determinación del nivel de madurez del Centro de Datos

Una vez que se ha evaluado la infraestructura física del Centro de Datos auditado, es menester establecer los parámetros necesarios que permitan conocer el estado actual de dicha infraestructura en relación al estado óptimo.

Para esto, el auditor informático utilizará al modelo del nivel de madurez que consta dentro de Cobit y que proviene del modelo de madurez definido por el *Software Engineering Institute*, el mismo que fue orientado a la madurez de la capacidad del desarrollo de software, con el fin es identificar dónde se encuentran los problemas y cómo fijar prioridades para las mejoras. Este modelo es aplicable a cualquier recurso de TI, y en este caso permitirá determinar si la infraestructura física del Centro de Datos está correctamente adecuada para proteger a los activos que se encuentran en él. Para esto es importante que el auditor realice una evaluación de los resultados obtenidos con el uso de este modelo de madurez, también conocido como Modelo Genérico de Madurez, el mismo que consiste en desarrollar un método de asignación de puntos para calificar al Centro de Datos en un parámetro que va desde Inexistente hasta Optimizada (de 0 a 5).

Esta medición permitirá posteriormente conocer los pasos a seguir para alcanzar un nivel óptimo de que garantice la disponibilidad acorde al tipo de Centro de Datos es decir el nivel 5, en tal virtud, el modelo de madurez de la infraestructura física del Centro de Datos se basa en un método de medición de cada sistema evaluado, es decir se procede a agrupar los cuatro sistemas Arquitectónico, Telecomunicaciones, Eléctrico y Mecánico, para determinar la madurez de cada uno de ellos.

El procedimiento para obtener el nivel de madurez es el siguiente:

Primeramente se debe tomar en cuenta la cantidad de ítems que tiene cada uno de los sub sistemas correspondientes a cada Tipo de Centro de Datos:

Tabla 20. Cantidad de Ítems evaluados en cada Tipo de Centro de Datos

Centro de Datos	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Telecomunicaciones	2	2	6	7
Arquitectónico	8	8	30	53
Eléctrico	14	14	20	36
Mecánico	8	8	9	13

Elaborado por: Christian Alonso Llerena Villa

La evaluación se realizará asignando un valor de 1 punto por cada ítem que tiene respuesta SI y 0 por cada respuesta NO, posteriormente se obtendrá el porcentaje del resultado obtenido.

Esto se realizara por regla de tres simple, es decir se establecerá la proporcionalidad de los valores con respuesta SI, en relación al número total de ítems, para lo cual se utilizará la tabla N°21:

Tabla 21. Cálculo del porcentaje de cumplimiento de los requerimientos del Centro de Datos

Centro de datos TIPO	Total Ítems (a)	Ítems con respuesta SI (b)	Cálculo Porcentaje (b x 100)/a
Arquitectónico			
Telecomunicaciones			
Eléctrico			
Mecánico			

Elaborado por: Christian Alonso Llerena Villa

Una vez que se ha obtenido el porcentaje de cumplimiento de los requerimientos, se procede a definir el nivel de madurez con el uso de la tabla N° 22:

Tabla 22. Nivel de Madurez en relación al porcentaje de cumplimiento

Porcentaje de cumplimiento obtenido	Nivel de madurez
0-16	0
17-33	1
34-50	2
51-67	3
68-84	4
85-100	5

Elaborado por: Christian Alonso Llerena Villa

Con la evaluación propuesta se ha obtenido un nivel de madurez para cada uno de los sub sistemas que forman parte de la infraestructura física del Centro de Datos por lo que el siguiente paso es analizar estos resultados. Adicionalmente se puede utilizar el siguiente gráfico para visualizar el estado actual frente al estado óptimo deseado.

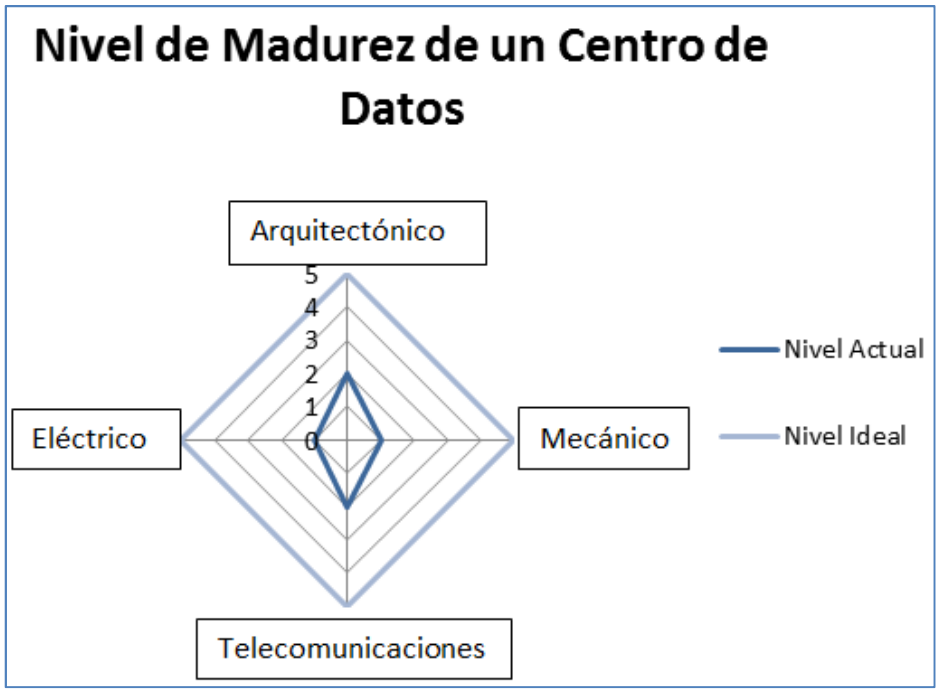

Figura 12. Ejemplo de representación gráfica del Nivel de Madurez
Elaborado por: Christian Alonso Llerena Villa

4.4 Análisis de resultados

El análisis del nivel de madurez obtenido tiene como objeto proveer una comparación práctica entre la realidad y lo deseado.

Para esto es necesario que los valores que presentados en la escala del modelo de madurez estén definidos, y que den el significado para saber dónde se encuentra actualmente y provean las medidas a tomar para llegar a un nivel óptimo, para eso se define el nivel 0 del modelo como aquel en el que la madurez del Centro de Datos es mínima y no muestra ningún progreso, mientras que en el nivel 5 se puede calificar al Centro de Datos como óptimo. Es así que se considera necesario definir cada uno de los grados del modelo de madurez, por lo que se ha establecido un criterio específico para cada uno de ellos, según se muestra en la siguiente tabla:

Tabla 23. Definición de los niveles de madurez de la infraestructura física de un Centro de Datos

Nivel	Definición
0	No Existente- Carencia de infraestructura física en el Centro de Datos que este alineada con algún estándar o buena práctica.
1	Inicial- Existe evidencia que la entidad ha reconocido la necesidad de alinear la Infraestructura física con algún estándar relacionado. Sin embargo dicha infraestructura no se encuentra correctamente organizada y no se han tomado medidas para mejorar dicha infraestructura.
2	Repetible- Se ha implementado una infraestructura física en el Centro de Datos según los lineamientos de algún estándar pero no existe una completa eficiencia en cada uno de los sub sistemas que forman parte de dicha infraestructura.
3	Definido- Toda la infraestructura física del Centro de Datos se encuentra organizada, sin embargo no todos los sub sistemas que forman parte de la infraestructura física cumplen con los requerimientos del estándar.
4	Administrado- La infraestructura física del Centro de Datos está alineada con el estándar y pueden existir umbrales que no presentan un nivel óptimo en su adecuación
5	Optimizado- Toda la infraestructura física se encuentra correctamente alineada con un estándar y con las mejores prácticas actuales.

Elaborado por: Christian Alonso Llerena Villa

Con la escala antes indicada, el Auditor Informático está en la capacidad de recomendar el tipo de acciones a tomar en cada uno de los sub sistemas que forman parte de la Infraestructura Física de un Centro de Datos, para esto se debe referir a los ítems de cada sistema en los que las respuestas en la evaluación han sido negativas y con base en esas premisas procede a recomendar la implementación o adecuación de la infraestructura física necesaria a fin de prever cualquier falla que puede afectar al Centro de Datos. Cabe indicar que la tabla de requerimientos generales es de carácter mandatorio, por lo que el Auditor concluirá en el informe que se adopten las medidas necesarias para cumplir cada uno de los ítems que se muestran en dicha tabla.

CAPÍTULO V

5. Conclusiones y Recomendaciones

5.1 Conclusiones

- Es necesario realizar Auditorías a los Centros de Datos de las entidades públicas del Ecuador ya que se ha evidenciado que las mismas contribuyen a mantener una adecuada infraestructura física del mismo, con el propósito de asegurar que los activos que se encuentran hospedados en este lugar estén correctamente protegidos ante los riesgos causados por las amenazas físicas que comprometen su normal funcionamiento.

- Los Centros de Datos de las entidades públicas pueden estar equipados con diversos niveles de redundancia en lo que concierne a su infraestructura física, esta robustez debe ser evaluada en relación a la criticidad de los procesos de tecnología de la información que se ejecuten en dicha entidad.

- El Análisis de Impacto al Negocio es una herramienta que permite conocer y cuantificar la importancia y la dependencia que tiene una entidad en relación a los servicios tecnológicos de los cuales hace uso, determinando su frecuencia y necesidad de disponibilidad según los objetivos y naturaleza de la entidad.

- Es necesario conocer cuáles son los activos que se encuentran hospedados en el Centro de Datos para determinar el riesgo que corren los mismos en caso de que la infraestructura física del Centro de Datos presente

fallas, identificando los activos críticos para la entidad y el tipo de riesgo que tiene mayor probabilidad de ocurrencia.

- Existen varios marcos de referencia de TI que pueden ser aprovechados para la realización de una Guía de Auditoría, por lo que se ha utilizado varios estándares que fundamentan los procedimientos que se han diseñado para la realización de la evaluación de la infraestructura física de los Centros de Datos de cualquier entidad pública del Ecuador.

- Las normas de control Interno de la Contraloría General del Estado constituyen la base legal para justificar las recomendaciones que se desprenden de la evaluación de un Centro de Datos, por lo que se analizaron las mismas y se estableció su relación con los marcos de referencia utilizados a nivel mundial en el campo de Tecnología de la Información.

- Con la realización de una auditoría al Centro de Datos se apoya de gran manera a la tarea de garantizar la disponibilidad de los activos que son fundamentales para el desarrollo normal de las actividades y procesos tecnológicos que se desarrollan en cualquier entidad del sector público del Ecuador.

- Una adecuada infraestructura física en un Centro de Datos minimizará el riesgo de que factores como: fuego, sobre calentamiento de equipos, cortes de energía, fuga de agua, acceso de personal no autorizado, entre otros; paralicen o dañen los activos que procesan y generan información para la entidad y detengan sus operaciones.

- La ejecución de auditorías periódicamente, y que estas estén basadas en los lineamientos propuestos en los principales marcos de referencia y estándares de la industria, permite asegurar que las entidades públicas del Ecuador estén en capacidad de mantener disponibles sus servicios tecnológicos.

5.2 Recomendaciones

- Se recomienda que el Auditor realice la evaluación de toda la infraestructura física de un Centro de Datos utilizando la presente Guía de Auditoría ya que la misma aplica a cualquier entidad del sector público del Ecuador.

- Se recomienda que las entidades públicas del Ecuador adopten los lineamientos del estándar más utilizado en el diseño e implementación de Centros de Datos para su mejoramiento continuo en función de lograr una mayor disponibilidad en sus servicios tecnológicos.

- Es necesario que el auditor informe debidamente al Administrador del Centro de Datos auditado, sobre los estándares y marcos de referencia que han sido utilizados en la presente Guía de Auditoría.

- Se deben impulsar la adopción de estándares internacionales en las entidades del sector público para promover el mejoramiento continuo de los recursos y servicios de tecnología de la información.

- Se debe programar una nueva auditoría a los Centros de Datos que han sido auditados con esta Guía para constatar el seguimiento de las recomendaciones antes planteadas.

BIBLIOGRAFIA

El estandar TIA 942. (07 de 2007). Recuperado el 02 26 de 2013, de www.ventasdeseguridad.com

The ISO 27000 Diretory. (2008). Recuperado el 2 de 03 de 2013, de http://www.27000.org/iso-27002.htm

Contraloría General del Estado. (02 de 2010). Recuperado el 4 de 02 de 2013, de http://www.contraloria.gob.ec

Clasificación TIER en el Data Center. (07 de 2012). Recuperado el 24 de 02 de 2013, de http://blog.aodbc.es/2012/07/10/clasificacion-tier-en-el-datacenter-el-estandar-ansitia-942/

ISACA. (2013). Recuperado el 2013, de http://www.isaca.org/cobit/pages/default.aspx

Chamorro, V. (2013). *Plan de Seguridad de la Información basado en el estándar ISO 13335.* Quito.

Eduardo, A. I. (2010). Desarrollo de una propuesta metodológica para la implementación de . Esmeraldas, Ecuador.

Figueroa, I. M. (2007). *DEPARTAMENTO ACADÉMICO DE INFORMÁTICA - UNSAAC.* Obtenido de http://in.unsaac.edu.pe/

Guagalango Ricard, M. P. (2011). *Evaluación técnica de la seguridad informática del Data Center de la ESPE.* Sangolquí.

Institute, I. G. (2008). Alineando Cobit 4.1, ITIL v3 e ISO 27002 en beneficio de la empresa. Estados Unidos: ITGI.

Isaca. (2007). *www.isaca.org.*

ServiceTonic. (02 de Mayo de 2011). *ServiceTonic.* Recuperado el Agosto de 2013, de http://servicetonic.wordpress.com/2011/05/02/introduccion-a-itil-v3/

Spera, C. (2012). Las claves en la administración de energía del Data Center. *Logicalis Now*, 13-14.

Briones Carlos, Diseño del Banco Central del Ecuador, Sucursal Cuenca., *Cuenca*