PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

PROPUESTO POR: Dr. Manuel Francisco Tupia Anticona
tupia.mf@pucp.edu.pe

ELABORADO POR: Jocelyne Estelita Nogueira Solís
jnogueira@pucp.pe

AREA DEL PROYECTO: Tecnologías de Información

TIPO DE PROYECTO: Análisis y Diseño

Lima, 15 de octubre del 2013

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN DEL PROYECTO

Los datos y la información son las herramientas que nos permiten realizar desde operaciones muy sencillas, como una compra en un supermercado, así como acciones complejas como tomar decisiones, motivo por el cual el cuidado de la información es una tarea imprescindible, sobre todo, cuando la información que se maneja es de vital importancia para el funcionamiento de una empresa u organización.

Los Data Center se han convertido en los lugares más utilizados para el almacenamiento de información importante pues, sean propios o tercerizados, proveen servicios que facilitan al cliente el mantener la información segura y disponible constantemente. Sin embargo, no se cuenta con un mecanismo que permita a los clientes asegurar que su información es almacenada de la mejor manera.

En este proyecto presentaremos la situación actual de los servicios de Data Center brindados en el país, demostrando la ausencia de una metodología que pueda ser usada para auditar los mismos y así poder asegurarle al cliente que el Data Center donde está depositando su información la tendrá adecuadamente almacenada y evitando que, de presentarse un riesgo, ésta pueda ser deteriorada o eliminada. De la misma forma, con las evidencias existentes se procederá al desarrollo de un conjunto de pasos que irán formando los procedimientos que faciliten la detección de las fallas de seguridad física y medio ambiental de los Data Center y que, a su vez, podrían afectar la continuidad de negocio.

CAPÍTULO 1: INTRODUCCIÓN AL PROYECTO

1.1 Introducción

En el presente capítulo presentaremos de forma precisa y detallada el problema que viene enfrentándose en la actualidad con respecto al tema de la seguridad de información en los Data Center, principalmente para empresas, señalando cuáles son las debilidades de éstos y cómo éstas se convierten en riesgos potenciales.

Ya con el problema detallado y conociendo cuáles son los puntos débiles que deben ser tratados, se detallarán los objetivos que el presente proyecto busca cumplir, así como el detalle del alcance y las limitaciones que se presentan para la realización del mismo.

Finalmente, se detallará la metodología a utilizarse para la elaboración ordenada del proyecto, la metodología necesaria para lograr el procedimiento de auditoría que propone este proyecto y el detalle del análisis que demuestra la viabilidad del mismo de acuerdo a su planificación.

1.2 Definición de la problemática

Durante los últimos 40 años[1], los datos y la información que se puede obtener a partir de ellos se han convertido en las herramientas más importantes para el día a día de las empresas. Sea para conocer más a sus clientes y proveedores o para ofrecer un producto cada vez mejor, los sistemas de información han comenzado a ser más utilizados de tal manera que se han vuelto imprescindibles para dicha organización.

Dado las recientes necesidades de alto desempeño y manejo de gran cantidad de datos por parte de los mencionados sistemas de información es menester el uso de grandes infraestructuras de servidores que almacenan los datos y que puedan brindar los servicios requeridos para las empresas.

[1] [TIER,2008]

Implementar estas infraestructuras de servidores trae consigo grandes inversiones financieras, la organización de personal capacitado para dar soporte a las mismas, así como espacios físicos (locaciones) considerables para alojar este tipo de hardware, inversiones que muchas veces se encuentran fuera de los presupuestos de muchas organizaciones que lo requieren.

En consecuencia, el negocio de tercerizar los denominados centros de cómputo o Data Centers ha aumentado su demanda de forma considerable, pues muchas organizaciones no pueden continuar manteniendo estructuras de servidores ineficientes o costosas de dar mantenimiento. Entre las muchas consideraciones técnicas que las empresas que brindan los servicios de alojamiento (housing) y prestaciones de equipos (hosting) deben tener en cuenta la seguridad física y medio ambiental como requerimiento básico de los clientes.

En un Data Center son sumamente importantes tanto la confiabilidad como la flexibilidad y la disponibilidad, por lo tanto deben seguirse buenas prácticas internaciones sobre seguridad física y medio ambiental, como el estándar y clasificación TIER, que garanticen el seguimiento de normas internacionalmente aceptadas.

La auditoría es un mecanismo que permite evaluar el grado de cumplimiento de – por ejemplo- una norma específica de seguridad y así poder tomar las medidas más convenientes en caso se requiera corregir ciertas desviaciones. La auditoría de seguridad de información es una de las tareas bases para comprobar que los datos y la información están siendo manejados de la manera correcta, garantizando su salvaguarda y tomando medidas para prevenir inconvenientes de pérdida, alteración no autorizada y carencia de disponibilidad.
Como se mencionó anteriormente, los Data Centers son los lugares donde se almacena información y sistemas de gran importancia para una organización y por lo tanto el cumplimiento de medidas de seguridad que aseguren la permanencia y buen estado de los datos es fundamental.

La auditoría de un Data Center es una tarea compleja, pues abarca dos instancias importantes pero sumamente diferentes que se explican a continuación:

1. La primera es el análisis de la información que se contiene y las formas de acceso a esa información. Los centros de datos manejan información delicada que debe ser protegida de personas mal intencionadas que quieran hacer mal uso de ella o que sin intención la alteren, provocando inconsistencia en la información.

2. La segunda es la protección del Data Center como facilidad en la que se alojan recursos de hardware importantes tanto para la empresa que brinda los servicios de hosting y housing como para los clientes de éstas, asegurando el correcto funcionamiento de estos equipos y verificando que la facilidad cumpla con las medidas necesarias para que, por ningún motivo, se interrumpan los procesos que son ejecutados en su interior.

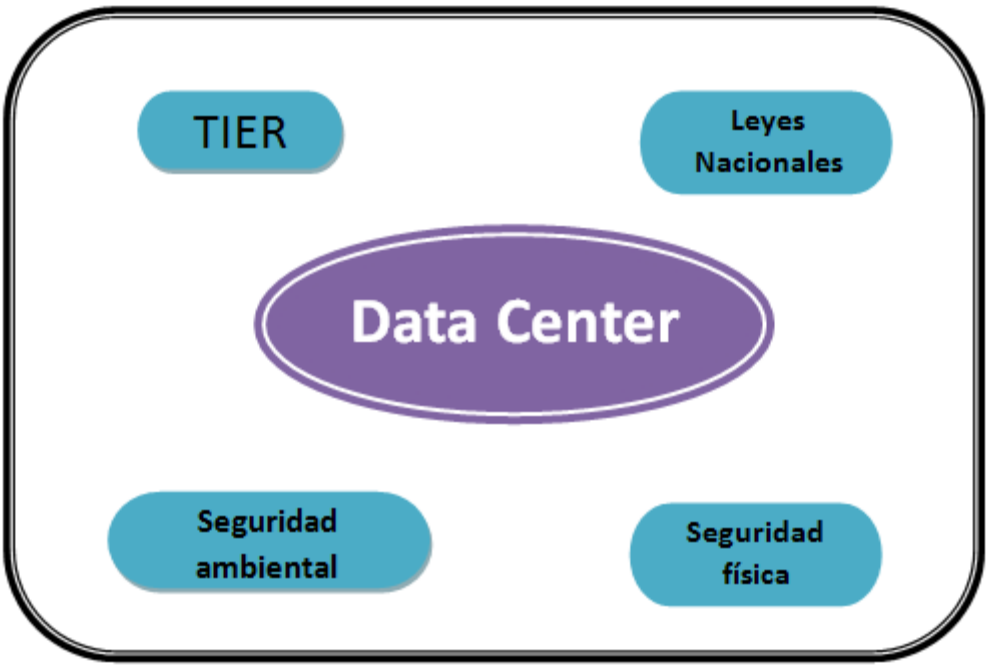

Ilustración 1: Representación del contexto en el que se desarrolla el problema

La existencia de una metodología que guie a los auditores en la verificación de cada uno de los puntos clave de un Data Center, permite que las vulnerabilidades queden reducidas, logrando que el Data Center sea un lugar seguro y eficaz para el

funcionamiento de la organización. Sin embargo, las realidades de las empresas no son las mismas y la forma de funcionamiento de éstas depende también de las realidades del territorio y de sus marcos regulatorios respectivos, siendo éste un problema bastante complicado de resolver. Seguir una metodología que no encaja con la actualidad podría traer consigo la consideración de factores que, en la realidad del Data Center, no existen junto con no considerar factores que sí podrían ser vulnerables y objetos de amenaza en los aspectos físicos y ambientales.

Finalmente, podemos concluir indicando que el problema que se trata en el presente proyecto es la inseguridad que tienen las personas que almacenan su más importante información en Data Center, sea propio o tercerizado, al no existir una metodología que asegure que el lugar donde está siendo almacenada es seguro y le brindará continuidad de acceso y operación de la misma.

1.3 Objetivo general

Diseñar un procedimiento de auditoría física y medio ambiental para centros de datos (Data Center) basado en la clasificación y estándar internacional TIER, con la finalidad de verificar las condiciones de seguridad de información con las que cuentan dichas instalaciones.

1.4 Objetivos específicos

Los objetivos específicos del proyecto a desarrollarse son:

1. Identificar los activos de información involucrados en la seguridad física y medio ambiental del Data Center.
2. Investigar las características más importantes relacionadas a seguridad física y ambiental expuestas por la clasificación y estándar internacional TIER para Data Center.
3. Identificar las vulnerabilidades, riesgos y amenazas comunes en seguridad física y medio ambiental.
4. Elaborar una guía metodológica para conducir una auditoría ordenada, sistemática, repetible, eficiente e integral.

1.5 Resultados esperados

De acuerdo a los objetivos específicos los resultados esperados son:

1. Identificar los activos de información involucrados en la seguridad física y medio ambiental del Data Center.
   - ✓ Inventario de activos de información involucrados en el proceso de auditoría física y medioambiental en Data Centers. Este inventario contendrá los elementos necesarios para la instalación y funcionamiento adecuado de un Data Center, considerando principalmente la seguridad física y ambiental.

2. Investigar las características más importantes relacionadas a seguridad física y ambiental expuestas por la clasificación y estándar internacional TIER para Data Center.
   - ✓ Survey de la norma TIER publicada por Uptime Insitute, el cual permitirá tener un mejor conocimiento de la aplicación y clasificación de los distintos tipos de instalaciones de Data Center según las características que presenten (incluyendo las características de seguridad física y medio ambiental, objeto de estudio).

3. Identificar las vulnerabilidades, riesgos y amenazas comunes en seguridad física y medio ambiental
   - ✓ Documento con el Análisis de Impacto de Negocio (BIA), el cual demostrará el impacto que tienen los riesgos sobre seguridad física y medioambiental en los activos de información presentes en cualquier Data Center y la continuidad de operaciones de los mismos.

4. Elaborar una guía metodológica para conducir una auditoría ordenada, sistemática, repetible, eficiente e integral.
   - ✓ Metodología documentada, la cual consistirá en el documento en el que se detalla paso a paso las acciones para ejecutar correctamente una auditoría física y medio ambiental para un Data Center, basada en la clasificación y norma TIER.

1.6 Alcance y limitaciones

1.6.1 Alcance

El presente proyecto de fin de carrera planteará una metodología necesaria para la realización de una auditoría física y medio ambiental a un Data Center, en base al estándar internacional TIER para Data Center y teniendo como referencia el marco de control COBIT 5.0

Esta metodología está destinada para su aplicación en empresas que ofrecen los servicios de hosting y housing tercerizado así como para empresas que cuentan con un Data Center propio y el cuál cuenta con más de 30 servidores.

Caso de estudio: Empresa del estado que solicita auditoría con el objetivo de analizar la infraestructura actual del Data Center para evaluar la idoneidad de la seguridad física y ambiental en él.

El presente proyecto no tomará en cuenta temas ni software relacionado a la seguridad lógica del Data Center, ya que se ha establecido como centro de estudio lo relacionado a los aspectos de seguridad física y medio ambiental. Sin embargo, es importante resaltar que tampoco se tomará en cuenta la revisión de software relacionado a la seguridad física y medio ambiental, – por ejemplo – el software de CCTV.

En el desarrollo de este proyecto se tomará como punto de partida la clasificación y estándar internacional TIER, que permite describir la disponibilidad, confiabilidad y el costo de construcción y mantenimiento de los Data Center, permitiendo que éste pueda ser apto y tenga las condiciones adecuadas para que el cliente pueda disponer de su información cuando lo necesite y estando ésta resguardada de la mejor manera.

1.6.2 Limitaciones

La única limitación que este proyecto presenta es no poder hacer referencia a todos los niveles establecidos por el estándar TIER, como se detalla a continuación.

TIER nos presenta cuatro niveles de clasificación, con las siguientes características:

- Tier I: Infraestructura básica: Aplicado a negocios pequeños, en los cuales se usa TI únicamente para procesos internos.
  a. Componentes no redundantes
  b. Única vía de distribución no redundante
  c. Una falla en un componente o en la distribución impactará el funcionamiento de los sistemas de cómputo.
  d. Infraestructura susceptible a interrupciones por cualquier evento planeado o no planeado.
- Tier II: Infraestructura con componentes redundantes: Aplicado a negocios pequeños, en los cuales se utiliza TI limitado al horario de oficina y que no ofrecen servicios en línea a cualquier hora.
  a. Componentes redundantes
  b. Única vía de distribución no redundante
  c. Infraestructura susceptible a interrupciones por cualquier evento planeado o no planeado
  d. Requiere generadores y fuente de suministro eléctrico con batería que sean redundantes.
- Tier III: Infraestructura con Mantenimiento simultáneo: Aplicable en compañías que dan soporte 24/7 como centros de servicio e información.
  a. Componentes redundantes
  b. Vías de distribución de energía redundantes (una activa y una pasiva)
  c. Los componentes pueden ser removidos durante un evento planeado sin generar interrupciones en el sistema.
  d. Susceptible a actividades no planeadas
- Tier IV: Infraestructura Tolerante a Fallas: Aplicable en compañías que brindan servicio 24x365, compañías basadas en comercio electrónico o de transacciones online, así como entidades financieras.
  a. Componentes redundantes
  b. Múltiples vías de distribución de electricidad
  c. Los componentes pueden ser removidos durante un evento planeado sin generar interrupciones en el sistema.

En nuestro país contamos con una normativa de concesiones eléctricas, Decreto Ley 25844 (9 de noviembre de 1992) - Artículo 30° - el cual señala que la actividad

de distribución de Servicio Público de Electricidad en una zona determinada, sólo puede ser desarrollada por un solo titular con carácter exclusivo. El concesionario de distribución podrá efectuar ampliaciones de su zona de concesión. Para tal efecto, está obligado a presentar al Ministerio de Energía y Minas, previamente, un informe que señale la delimitación de la zona donde efectuará la ampliación, acompañado del Calendario de Ejecución de Obras. Siendo esta ley el motivo principal por el cuál en nuestro país y en el desarrollo del presente estudio se tratará la clasificación TIER únicamente en los niveles I y II. [LCE, 2009]

1.7 Métodos y procedimientos

1.7.1 Metodología del proyecto

Para el desarrollo de este proyecto de fin de carrera se hará uso de la metodología Plan-Do-Check-Act, también llamada Ciclo de Deming y basado en la mejora de calidad.

Esta metodología consta de cuatro pasos, los cuales son repetidos una y otra vez para situaciones de cambios y solución de problemas.

Los pasos son:

a. Plan (Planificar): Se refiere a la identificación y análisis del problema, obteniendo con este análisis un plan de trabajo que permita llegar a una solución.
   En el caso del proyecto, en la fase de planificación se establecerán los objetivos de cada uno de los entregables, los cuales no solo deben basarse en la planificación de entregables del curso, sino también en el avance de la planificación realizada para concluir con el proyecto.

b. Do (Hacer): El desarrollo del plan realizado en la etapa anterior y la realización de pruebas y medición de resultados de la solución.
   En la presente fase se hará el planteamiento de la metodología en sí, las herramientas para su elaboración y los pasos que se seguirán para su implementación, con el fin de cumplir los objetivos del proyecto.

c. Check (Verificar): Se revisan y analizan los resultados de manera que se pueda obtener una medida de la efectividad de la solución y, a la vez, una retroalimentación de lo que se podría mejorar.
   En esta etapa se trabaja en compañía del asesor para realizar la revisión de los pasos que van a incluirse en la metodología, así como detallar las correcciones que se harán sobre los avances para lograr una metodología adecuada.

d. Act (Actuar): Aplicaciones de las correcciones que se obtuvieron en la etapa anterior. En esta fase se realizarán las correcciones anteriormente indicadas por el asesor sobre la metodología que se desarrolla, de la misma forma se procederá a realizar diversas pruebas de los pasos propuestos en la empresa que será caso de estudio para lograr así un resultado de ensayo-error y poder sacar nuevas conclusiones e ideas que sean favorables para la metodología.

Como se ha mostrado a través de la descripción de cada uno de los pasos, esta metodología se adapta a una variedad bastante amplia de procesos y por lo tanto se adaptará a la realización del presente proyecto. De la misma forma es importante mencionar que el ciclo de Deming es una de las metodologías más utilizadas en lo que refiere a auditoría.

1.7.2 Metodología del producto

El resultado de este proyecto de fin de carrera es el establecimiento de una metodología de auditoría, sin embargo, la auditoría puede llevarse a cabo con distintos enfoques y la aplicación de uno u otro dependerá de cada sujeto de auditoría.

COBIT 5.0 es un marco de control internacionalmente reconocido que se basa en el análisis y armonización de estándares y mejores prácticas de TI existentes, cubriendo el rango completo de actividades de TI, brindando orientación y convirtiéndose en centro de la auditoría.

Con la utilización e implantación de COBIT 5.0 para la seguridad de información, se obtienen un gran número de beneficios para la empresa, como son:

- Reducir la complejidad e incrementar el costo-efectividad que permita una fácil integración de los estándares y buenas prácticas de la seguridad de información con los requerimientos del negocio.
- Incrementar la satisfacción del cliente asegurándole total seguridad de información.
- Conocer los riesgos y generar medidas para controlarlos.
- Mejorar el soporte a la innovación y competitividad

Actividades que nos permitirán la obtención de una metodología eficaz para la auditoría.

De la misma forma nos basaremos en la clasificación y estándar TIER, que nos permitirá hablar de la confiabilidad y disponibilidad de datos en un Data Center, brindándonos información de los puntos a tomar en cuenta para la realización de la auditoría en lo que respecta a medidas que deben ser tomadas para que el rendimiento del Data Center sea el adecuado para el cliente.

1.8 Justificación y viabilidad

El proyecto que se presenta en este documento tiene como objetivo el establecimiento de un conjunto de procedimientos que colaboren con el auditor en la sustentación de sus hallazgos para la determinación de los imperfectos que podría tener un Data Center y que podrían ser perjudiciales para los usuarios de los mismos.

La propuesta de este proyecto se basa en marcos de control reconocidos internacionalmente, como COBIT 5.0 y en estándares también internacionales como TIER, que nos permitirán basarnos en procesos e indicadores que nos aseguran efectividad de la evaluación.

La viabilidad de la metodología que será desarrollada en este documento abarca las empresas que ofrecen servicio tercerizado de hosting y housing, así como empresas que cuentan con su propio Data Center pero el cuál es de dimensiones mayores a 30 servidores.

En cuanto a otros aspectos de viabilidad:

- Técnica: Para la realización de la metodología será necesario que el ejecutor tenga conocimientos del marco de control COBIT 5.0, así como del estándar TIER en todos sus niveles.
- Temporal: El presente proyecto podrá ser aplicado mientras la norma TIER se encuentre vigente.
- Económica: No será necesaria la compra de ninguno de los marcos y estándares a utilizarse pues debido a una inscripción del desarrollador de este proyecto como “Student Member” de la asociación ISACA le permitirán obtener de forma gratuita los mismos.

El detalle del plan de proyecto se podrá observar en el Anexo A.

CAPÍTULO 2: MARCO TEÓRICO Y ESTADO DEL ARTE

2.1 Introducción

En el presente capítulo se detallarán los términos que deben ser necesariamente entendidos para el desarrollo del proyecto, así como ítems de gran importancia en los Data Center y que serán parte del análisis.

Finalmente, se detallarán los mecanismos utilizados en la actualidad para la auditoría de seguridad física y medio ambiental así como los ítems que son tratados, prosiguiendo con un análisis de los mismos.

2.2 Marco teórico

2.2.1 Auditoría

La auditoría se define como un proceso sistemático, independiente, ordenado y documentado que permite presentar la realidad, así como obtener y evaluar evidencias desde un punto de vista objetivo, para verificar el cumplimiento de normas o estándares que hayan sido establecidos con algún fin. [2]

Es importante en estos momentos recalcar que la auditoría no tiene como objetivo fiscalizar las labores de un área o departamento determinado, ni muchos menos realizar la mejora de los errores que se pudieran encontrar, su objetivo es únicamente la emisión de una opinión profesional.

Al hablar de auditoría podemos encontrar clasificaciones de diferentes tipos. Una de estas clasificaciones se da de acuerdo al personal que la realiza, siendo los tipos:

a. Auditoría interna: Se refiere al caso en el que el equipo auditor forma parte de la organización.

[2] [Piattini, Del Peso,2001]

b. Auditoría externa: El equipo auditor no forma parte de la organización a la que se audita, es un equipo tercerizado.

De la misma forma, la auditoría puede ser clasificada de acuerdo al aspecto que se pretende analizar, dividiéndose en:

a. Contables o financieras: El objetivo es determinar la exactitud de la situación contables y financieros de la organización.
b. Administrativa: El objetivo es determinar la eficiencia de la productividad operativa dentro de una organización.
c. De sistemas, informática, TI o de seguridad de información: El objeto es la validación y verificación de los sistemas, procesos y resultados en los que se use la tecnología, sea en la legislación como en la integridad de la información.
d. Operativas: El objetivo es determinar el grado de economía, eficiencia y eficacia en la planificación, control y uso de los recursos y el correcto uso de éstos dentro de procesos planificados y documentados correctamente.
e. Especializada: El objetivo es evaluar el correcto funcionamiento de algún aspecto propio de la organización.

Para la realización de una auditoría es necesario manejar términos que permitan entender cada uno de los pasos del plan de auditoría. A continuación se mencionan algunos de los términos más importantes:

- Criterio: Se refiere al conjunto de políticas, procedimientos o requisitos que son utilizados como una referencia para proceder con la auditoría.
- Evidencia: Cualquier información que le permita al auditor verificar que se cumplan los criterios o normas que han sido establecidas y contar con un sustento que permita probar las conclusiones deducidas y las recomendaciones que se están dando.
- Hallazgo: Se denomina de esta forma al resultado de la comparación y evaluación de las evidencias contra los criterios que se manejen, pudiendo así establecer si fue o no conforme con los criterios establecidos. De la misma forma, estos hallazgos permiten al auditor reconocer oportunidades de mejora y poder reportarlas.

Ilustración 2: Representación de un hallazgo.

- Riesgos: Es el potencial de que exista una amenaza que pueda explotar una de las vulnerabilidades de los activos de la organización, produciéndole daño. Existen diferentes tipos de riesgos, entre ellos podemos diferenciar:
  - Riesgos de control: Se refiere a riesgo que no puede ser detectado por los controles que se encuentran establecidos en ese momento.
  - Riesgos de detección: Se refiere a la posibilidad de no identificar correctamente los riesgos y por ello indicar que no existen problemas cuando en la realidad si los hay.
  - Riesgos de negocio.
  - Riesgos inherentes: Riesgos que ya existen y que no cuentan con un control.
- Controles: Son el conjunto de procedimientos, políticas y estructuras de la organización que permite reducir riesgos y que proveen un grado de certeza de que los objetivos del negocio podrán ser alcanzados. Existen diferentes tipos de controles, entre ellos podemos encontrar:
  - Preventivo: su labor es detectar problemas antes de que puedan ocurrir. La detección se hace por medio de monitoreo constante.
  - Disuasivo: Su intención es disuadir la comisión de acciones que quieran sobrepasar las políticas o procedimientos establecidos y considerados correctos.
  - Detectivo: Detectan y reportan los problemas, que pueden ser generados por distintos factores, cuando estos ocurren.
  - Correctivo: Tratan de corregir o disminuir el impacto de alguna amenaza que ya ha sido consumada.

- Compensatorio: Intentará reducir la probabilidad de que se produzca un problema.

Para dar inicio a un proceso de auditoría, al igual que en cualquier otro proyecto, sea de corto o largo plazo, debe realizarse un plan de trabajo para que así se determinen cuáles son las actividades que llevará al auditor a lograr los objetivos planteados para este proceso.

Lo principal para empezar el proceso de la auditoría es determinar los objetivos que se busca alcanzar con ésta. Estos objetivos dependerán de qué es lo que se necesita analizar, de acuerdo a las necesidades de la organización. Una vez establecidos los objetivos se pueden seleccionar los elementos del negocio que serán auditados y los recursos que serán necesarios para poder auditarlos. Cada objetivo de la auditoría deberá tener asociado un control, y estos controles serán los encargados de asegurar el cumplimiento de los objetivos del negocio.[3]

Con los objetivos ya establecidos se puede dar inicio al análisis del estado actual de cada uno de los controles identificados, detectando los riesgos que están siendo correctamente controlados por éstos y aquellos que no han sido previamente considerados y por lo tanto siguen siendo una amenaza.

Una vez terminadas las pruebas se da inicio a la etapa de construcción del informe, para ellos se debe contar con un registro de las evidencias encontradas, de manera que los hallazgos puedan ser sustentados y comparados con los criterios que se han establecido por la auditoría. Como parte importante del informe también debe brindarse recomendaciones que permitan a la organización tener un mejor desempeño en cuanto al establecimiento de controles que les aseguren el cumplimiento de sus objetivos.

2.2.2 Auditoría de Sistemas / TI

Según la definición dada por ISACA[4], la auditoría de SI es el proceso de recoger, agrupar y evaluar evidencias para determinar:

- Si los equipos y activos de información[5] en general son usados de acuerdo a los estándares que se hayan establecido.

[3] [Piattini, Del Peso,2001]

[4] Organización líder en Auditoria de Sistemas y Seguridad de los Activos de Información

- Si los equipos y activos de información están alineados a los objetivos de la organización.
- Si los datos son manejados de forma correcta de manera que se cumplan los principios de integridad, disponibilidad y confiabilidad.

Su objetivo principal es apoyar a la organización a validar que los sistemas de información y tecnologías de información con las que cuentan se encuentran controlados, protegidos y alineados a los objetivos organizacionales, asegurando que funcionen correctamente y aporten valor a los procesos de la organización.

Como en toda auditoría, al inicio se deben definir cuáles son los aspectos que serán auditados, de manera que el análisis se enfoque en ellos y se realice el trabajo correcto. Los aspectos más importantes a evaluar son:

- Seguridad de información (o seguridad computacional): verificar que los activos tengan como características confidencialidad, integridad y disponibilidad.
- Calidad: verificar la eficiencia del uso de las tecnologías de manera que se cumpla con las expectativas de la empresa.
- Fiabilidad: verificar que la información manejada por las tecnologías sea información en la que se podrá confiar en todo momento.
- Nivel de servicio: verificar el cumplimiento de los niveles de satisfacción requeridos y señalados.
- Capacidad de infraestructura: verificar que las características sean usadas de la manera más eficiente y aprovechando el total de su capacidad.

La auditoría de sistemas de información, en su gran mayoría, suele basarse en riesgos, lo que significa que se focalizarán en los elementos que la misma empresa ha evaluado como críticos.

Para dar inicio a la auditoría basada en riesgos se requiere el trabajo previo de la empresa que solicita la auditoría, pues serán ellos los encargados de evaluar cuáles son los elementos de mayor criticidad ya que al conocer el funcionamiento

[5] [ISO, 2005b] Cualquier componente (sea humano, tecnológico, software, etc.) que sustenta uno o más procesos de negocios de una unidad o área de negocio.

de su negocio deben también conocer cuáles son los elementos que de fallar podrían traer abajo la organización.

Una vez identificados los riesgos más relevantes, la auditoría puede ser más eficiente, pues se enfocará en los elementos más críticos, siendo esto lo más conveniente pues al no poderse cubrir todos los aspectos que se necesitan evaluar, se puede priorizar aquellos que generarían más riesgos para la organización.

La siguiente fase del proyecto de auditoría es cuantificar y categorizar los riesgos, los cuales son muy subjetivos a la realidad y entorno de la empresa y que también depende de los aspectos que se auditarán. La idea de esta etapa, como su nombre lo dice, es cuantificar, asignar un valor numérico de acuerdo a cada uno de los sujetos de auditoría y una vez con todos los valores se procede a ponderar todos éstos, de manera que aquél que tenga mayor valor sea considerado el más importante y el primero a analizar durante la planificación.

Durante la ejecución de la auditoría es muy posible encontrar en el camino los controles asociados al proceso que se está auditando, de ser así, se deberá verificar que estos estén cumpliendo con su labor de controlar las amenazas y para ello se realiza lo que se conoce como pruebas de cumplimiento. Las pruebas de cumplimiento verifican que los controles existan, se hayan aplicado de la forma correcta y que sean efectivos en su labor.

Por otra parte, el manejo de evidencias y materialidad en la ejecución de una auditoría son claves para el correcto desempeño de ésta, pues las evidencias y la forma en que han sido obtenidas deberá plasmarse en los informe finales de la auditoría.

La manera más eficiente de mantener documentadas las evidencias que se van encontrando es por medio de los papeles de trabajo del auditor, donde se recopilan todas las investigaciones y evidencias que se van encontrando. Estos papeles facilitarán la preparación del informe final, explicarán muchas de las opiniones que se darán en éste y servirán de guía para las siguientes revisiones que se realicen.

Finalmente, el último paso para el cierre del proceso de auditoría es la realización del informe final. Este informe irá dirigido a muchas personas, por lo cual el lenguaje en el que es escrito debe ser entendible por todos los miembros de la organización y, en caso de querer un informe con más detalles, se pueden generar versiones adicionales, dependiendo de a quien irá dirigida, como por ejemplo resumen ejecutivo, informe técnico, entre otros.

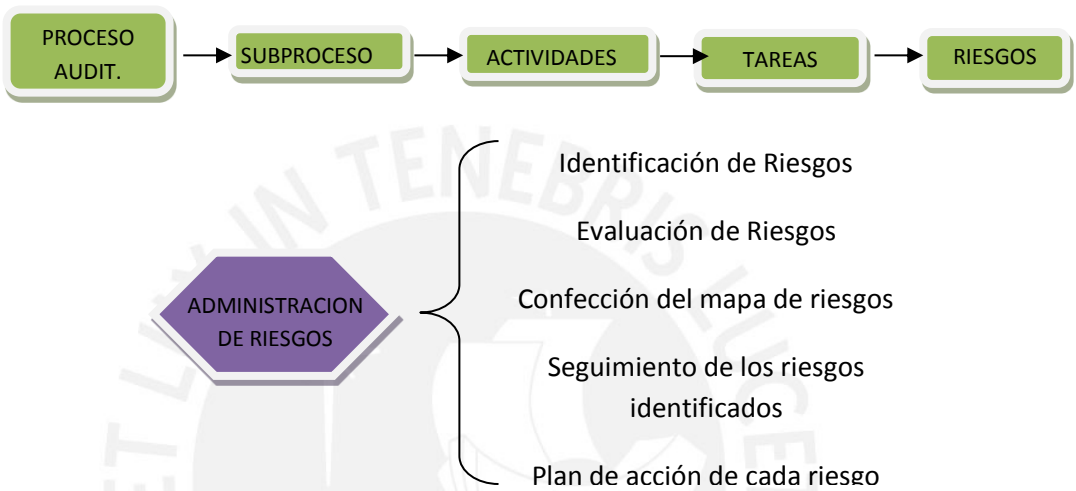

Ilustración 3: Proceso de auditoría basado en riesgos.

2.2.3 Marcos para la auditoría

Los marcos de control son un conjunto de buenas prácticas internacionalmente reconocidas cuyo objetivo es organizar los pasos para la verificación, análisis y corrección de los procesos o servicios de una organización, permitiendo comprobar que la forma en que están funcionando se encuentre dentro de los parámetros que se han definido para ello.

"Los marcos tienen como finalidad facilitar la labor de monitoreo, evaluación e integración de los esfuerzos de varias gerencias en áreas específicas, en pos de controlar determinados procesos de negocio, incluyendo a los procesos de TI.

Notemos aquí el beneficio de relacionar estos conceptos con los de auditoría por ser muy cercanos"[6]

Un punto bastante importante a considerar al mencionar a los marcos de la auditoría es que éstos se han definido de manera genérica, por lo cual la realidad de cada empresa jugará un papel muy importante cuando se tenga como objetivo ponerlos en práctica.

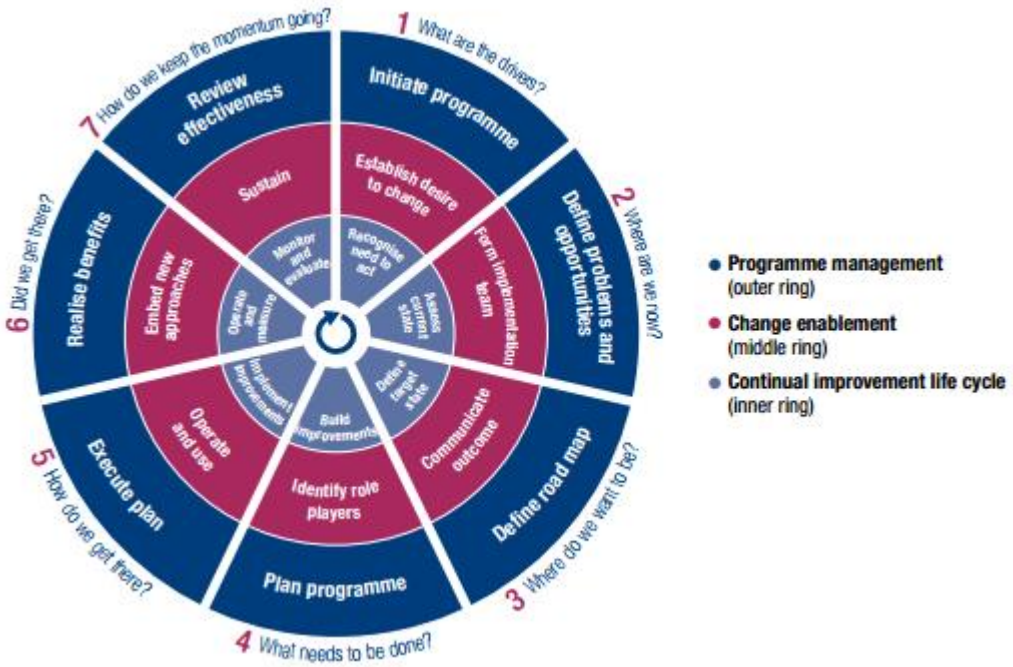

Ilustración 4: COBIT 5.0 [ISACA, 2012]

2.2.4 Gobierno de TI

Según ITGI[7] el concepto de gobierno se define como "El conjunto de responsabilidades y prácticas del consejo de administración y dirección de la empresa con la finalidad de brindar dirección estratégica, garantizar el logro de los objetivos organizacionales, determinar la mejor forma de administración de los riesgos y verificación del buen uso de los recursos"[8].

[6] [TUPIA,2011]
[7] [ISACA,2010] Instituto de gobierno de TI
[8] [ITGI,2003]

En el caso de esta investigación nos interesa un tipo de gobierno en particular, el Gobierno de TI.

El Gobierno de TI es una parte integral de las empresas y consiste en una estructura de relaciones y procesos cuyos objetivos son:

- Brindar dirección a la empresa en el logro de los objetivos del negocio
- Lograr que la implementación de los procesos de TI sea adecuada
- Asegurar el retorno de valor de las inversiones hechas en TI
- Gestionar de forma adecuada los riesgos que trae la TI

La labor principal del Gobierno de TI es conseguir la alineación de todas las tecnologías de TI a los objetivos de la organización, así como a las estrategias que se usarán para el logro de esos objetivos.

Los principios en los que se basa el Gobierno de TI son:

1. Principio de dirección y control: Este principio es fundamental para una efectiva implantación de Gobierno de TI.

   Con respecto a la dirección, el papel principal lo tiene la Alta Dirección, pues debe identificar, planear, ejecutar y monitorear los proyectos de TI que serán soporte para las actividades de la organización, verificando que éstos estén cumpliendo con los objetivos que se trazaron para ellos.

   En cuanto al control, el papel nuevamente vuelve a tenerlo la Alta Dirección, quien debe monitorear constantemente los proyectos de TI, para lograr que éstos se desarrollen sin mayores inconvenientes.
2. Principio de responsabilidad: Este principio tiene su base en la necesidad de conocer las responsabilidades asignadas a cada persona sobre el establecimiento, implementación, control y monitoreo de las actividades del Gobierno de TI.

   Consiste en la definición de políticas, procedimientos y responsabilidades, tarea realizada por un conjunto de personas relacionadas al Gobierno de TI en conjunto con el CEO.
3. Principio de imputabilidad y trazabilidad: Los proyectos de TI y las tecnologías de información existentes en la organización deben estar respondiendo a las

necesidades dentro de la empresa, el monitoreo de las actividades permite verificar su utilidad, aporte y devenir, siendo éste el objetivo de la trazabilidad. De la misma forma, debe ser posible conocer quiénes son los responsables de cada etapa o actividad del proyecto y cómo va el avance de esa etapa, de esta manera, se podrán gestionar las acciones correctivas cuando sea conveniente.

Las relaciones dentro de las áreas de TI son:

- Alineación estratégica: alineación de las tecnologías a los objetivos organizacionales para asegurar el funcionamiento como soporte.
- Gestión de riesgos: identificar, manejar y reducir el impacto que podría representar cada riesgo sobre los procesos de negocio y los activos de información involucrados.
- Entrega de valor: Asegurar que las inversiones de TI devuelvan valor a la empresa en el logro de sus objetivos.
- Gestión de recursos: Velar por el uso adecuado de los recursos asignados al funcionamiento de la TI.
- Medición del desempeño: monitorear los proyectos y procesos relacionados a la TI, evaluando su desempeño con respecto a los objetivos de negocio.

El correcto establecimiento y manejo del Gobierno de TI en una organización, permitirá obtener ventajas importantes para el manejo y confianza de la organización. Brindará:

- Confianza por parte de la Alta dirección: quien al conocer el funcionamiento del área y al colaborar con ella, podrá confiar en que se busca el cumplimiento de los objetivos. Esta ventaja es bastante significativa principalmente en los casos en que otras gerencias no confían en las labores del área de Sistemas/TI.
- Sensibilidad de las necesidades de negocio: con el estudio de los objetivos y al relacionar cada TI con uno de los objetivos organizacionales, se puede asegurar que se conoce casi totalmente las necesidades de negocio y que se buscará constantemente la forma de favorecer al cumplimiento de estas necesidades.

- Aseguramiento de los retornos de las inversiones en TI: al relacionar los objetivos de negocio con los proyectos de TI se asegura que éstos tienen como objetivo resolver necesidades y por lo tanto retornar valor al dinero invertido en ellos.
- Prestación de servicios más confiables: Con el gobierno de TI se busca que las áreas que trabajan simultáneamente con el área de Sistemas/TI puedan conocer el funcionamiento y manera de operar de ésta, de manera que sientan más confianza al resultado del servicio que se brinda, así como el área de Sistemas/TI podrá tener una mejor visión de cómo brindar mejores servicios.
- Mayor transparencia en el manejo de la gerencia de TI: El manejo de la gerencia será conocido por toda la organización.

2.2.5 Gobierno de Seguridad de la Información

La seguridad de información es "El conjunto de procesos y actividades que permiten mantener libre de peligros y daños por accidente o ataque a los activos de información que forman parte de una organización"[9] independiente de cómo sea creada, manejada, transportada o almacenada.

El Gobierno de la Seguridad de Información se establece con las responsabilidades y actividades realizadas por la Alta Dirección para guiar y dirigir eficientemente los mecanismos de seguridad de información de los activos de información y así conseguir los objetivos del negocio.

Ilustración 5: Representación de seguridad de información.

[9] BOSSWORTH (apud Tupia Anticona, 2010, p.50)

Un error bastante típico y muy grave que se comete en las organizaciones es considerar que la seguridad de información es responsabilidad única del área de Sistemas/TI. La Alta Dirección debe ser la encargada de instituir políticas que sean dadas a conocer a todas las áreas, siendo el área de Sistemas/TI una de ellas, sobre las reglas que permitirán asegurar la seguridad de la información que se maneja y que es de gran importancia para el logro de los objetivos organizacionales.

La seguridad de información es uno de los temas más importantes a considerar en una organización, pues todos los procesos manejados dependen de la información que se obtenga mensual, semanal o diariamente, y si ésta no es protegida, no solo podría generar riesgos de propagación de información sensible, sino que podría impedir el cumplimiento de al menos uno de los objetivos de negocio.

2.2.6 COBIT 5.0

Para el desarrollo de esta guía, es importante resaltar el apoyo de un marco de control en especial. El marco con el que se trabajará será COBIT 5.0

COBIT 5 brinda un marco de control que permite a las empresas alcanzar sus objetivos para el manejo de la TI, manteniendo un balance entre los beneficios que TI ofrece y optimizando el nivel de riesgo que trae consigo.

COBIT 5 permite una administración integral de la TI teniendo en cuenta la totalidad de extremo a extremo de la empresa, considerando las áreas responsables de la TI así como la relación de interés con las áreas que hacen uso de ellas.

Para lograr el éxito de las TI, es decir, para que puedan satisfacer las necesidades del negocio, se deben implementar un sistema de controles internos o marco de control. Es en estas circunstancias que COBIT 5.0 entra en juego basándose en cinco principios:

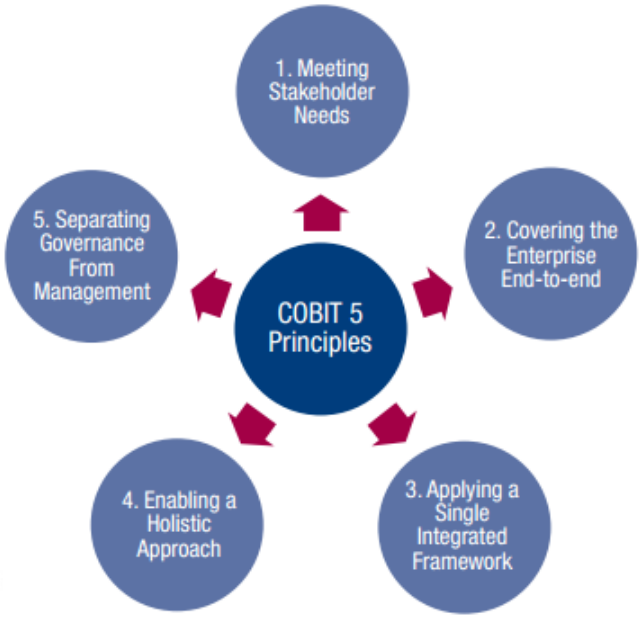

Ilustración 6: Principios de COBIT 5 [ISACA, 2012]

1. Conocer las necesidades de los interesados: Los interesados en TI son todas las personas que hacen uso de ella y por lo tanto, conocer sus necesidades facilitará el cumplimiento de los objetivos que le encarguen a la TI y con ello el cumplimiento de los objetivos del negocio.
2. Cubrir la empresa de extremo a extremo: Cubrir todos los procesos de la empresa y no solo aquellos que sean función de TI. Considerar la información así como la tecnología como activos que pueden ser aprovechados en cualquier extremo de la empresa.
3. Aplicar un marco único e integrado: Existe una gran variedad de estándares, normas y marcos relacionados a subconjuntos de actividades de TI. COBIT 5, por abarcar de extremo a extremo la empresa, permite integrar de manera simple y eficaz estas otras normas y marcos.
4. Enfoque integral: COBIT apoya la implementación de un Gobierno de TI que abarque la totalidad de la empresa.
5. Separación del Gobierno con la administración: COBIT 5.0 establece una gran distinción entre las funciones del gobierno y de la administración ya que abarcan diferentes actividades y tienen diferentes objetivos, por lo tanto necesitan diferentes estructuras organizativas.

Una de las características básicas de COBIT 5 es el tener un enfoque de procesos, motivo por el cuál, como se mencionó líneas arriba, se hace una distinción entre los procesos de Gobierno con los procesos de gestión, generando diferencias en sus definiciones como se menciona a continuación:

- Procesos del gobierno: Se refiere a los procesos relacionados a la optimización de riesgos, así como a la optimización de recursos, incluyendo actividades que permitan evaluar y proporcionar la correcta orientación a la seguridad de información.
- Procesos de gestión: Se refiere a los procesos que contienen actividades que permitan cubrir la responsabilidad de las áreas de planeamiento, construcción, ejecución y monitoreo de la seguridad de información

Una vez dado a conocer las generalidades de COBIT es importante mencionar y explicar que este marco de control implementa un ciclo de vida que permite a la empresa hacer frente a la complejidad y desafíos típicamente encontrados en la seguridad de información.

Este ciclo de vida cuenta con 7 fases, las cuales deben ser seguidas iterativamente con el objetivo de obtener una constante mejora.

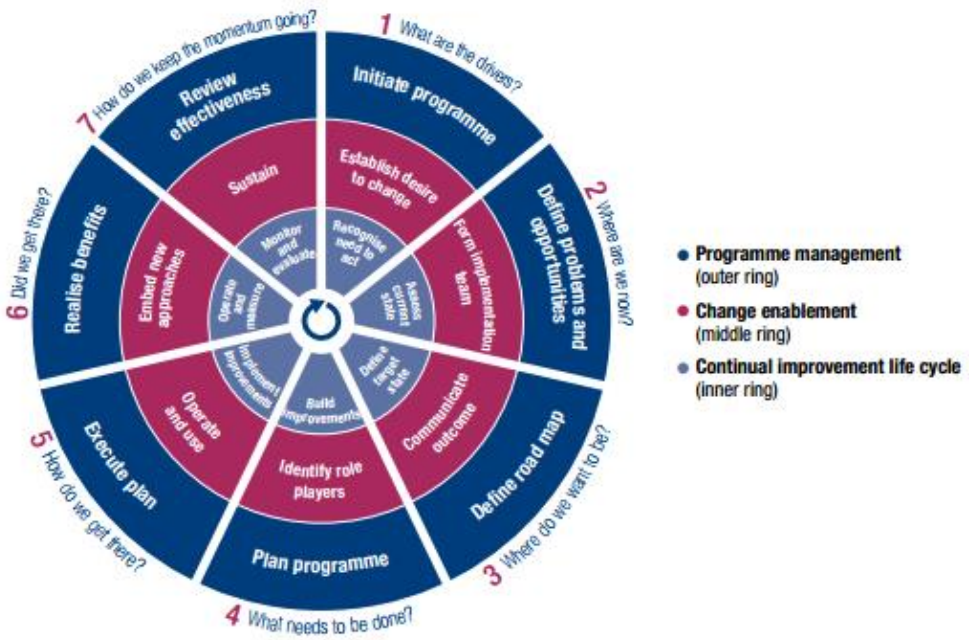

Ilustración 7: Ciclo de vida de COBIT 5 [ISACA, 2012]

1. Fase 1: Consiste en comprender el impacto que genera el cambio a realizarse, los clientes de TI a los que afecta y cuál es la capacidad de la realidad empresarial para adaptarse a ese cambio.
2. Fase 2: Esta fase se centra en definir el alcance de la implementación de COBIT en el entorno empresarial, determinando cuáles son las áreas prioritarias. En esta fase se debe también hacer una evaluación del estado actual, para así identificar los problemas y deficiencias actualmente existentes.
3. Fase 3: El objetivo es generar una mejora así como un análisis más detallado que permita identificar deficiencias y posibles soluciones, dando prioridad a aquellas que sean más fáciles de alcanzar y que producirán mayor beneficio.
4. Fase 4: En esta fase se busca analizar posibles soluciones teniendo como soporte del análisis los denominados casos de negocios[10] de manera que pueda apoyar al inicio de un proyecto cuyos beneficios han sido identificados y podrán ser monitoreados, asegurándose la alineación al negocio y el cumplimiento de los objetivos.
5. Fase 5: En esta fase se implementan las soluciones analizadas y elegidas en las fases anteriores, para lo cual se necesita el apoyo de la Alta dirección así como de los interesados en la información.
6. Fase 6: Siendo la penúltima fase, las actividades se centran en constatar que los objetivos que buscaban cumplirse estén siendo alcanzados y son sostenibles.
7. Fase 7: Como última fase, tiene como objetivo revisar el éxito total de la iniciativa, identificando nuevos requisitos de seguridad de información y reforzando la idea de mejora continua[11].

COBIT 5.0 define las actividades de TI en un conjunto de procesos agrupados en dominios. Estos procesos se encuentran especificados en un lenguaje simple para que todos los miembros de la empresa puedan entender la forma de administración de TI.

[10] Caso de negocio: Propuesta que busca conseguir la aprobación para dar inicio a la ejecución de un proyecto. Proporciona una descripción de viables opciones, sus análisis y una decisión recomendada describiendo todas sus características, tales como beneficios, costos, riesgos, tiempo, el impacto en los interesados, y así sucesivamente. [SCTC, 2009]

11 [ISACA 2012]

De la misma forma brinda un marco para la medición y monitoreo del desempeño de TI, de manera que puedan integrarse las mejores prácticas de administración no solo a la organización sino también a los proveedores de servicios.

Los dominios que COBIT ha definido son:

1. Evaluar, dirigir y Monitorear (EDM): Este dominio contiene un conjunto de procesos que permiten analizar los requisitos para el gobierno de TI de la empresa y con ellos establecer y mantener estructuras eficaces que apoyen los principios con procesos y prácticas que tengan responsabilidades definidas.
2. Alinear, planificar y organizar (APO): Este dominio tiene como fin aclarar los objetivos de la gestión de información y TI de acuerdo a la misión, visión y objetivos de la empresa, para así planificar y organizar cómo una adecuada gestión ayudará al cumplimiento de las metas de la organización.
3. Construir, adquirir e implementar (BAI): Su objetivo es la administración de los proyectos de inversión en tecnología, de manera que las tecnologías se encuentren alineadas a la estrategia del negocio. Iniciar, planificar, controlar y ejecutar los proyectos viables así como hacer una revisión posterior a la implementación.
4. Entrega, servicio y soporte (DSS): Coordinar y ejecutar actividades y procedimientos adecuados para brindar un correcto y completo soporte interno y externo de TI.
5. Monitorear, evaluar y asistir (MEA): Recopilar información, evaluar y monitorear el correcto funcionamiento de los procesos que se hayan definido previamente así como el cumplimiento de normas que hayan sido establecidas. En el caso de que la evaluación de resultados negativos proceder a asistir al proceso para que pueda modificarse y contribuir de la forma establecida.[12]

[12] [ISACA, 2012]

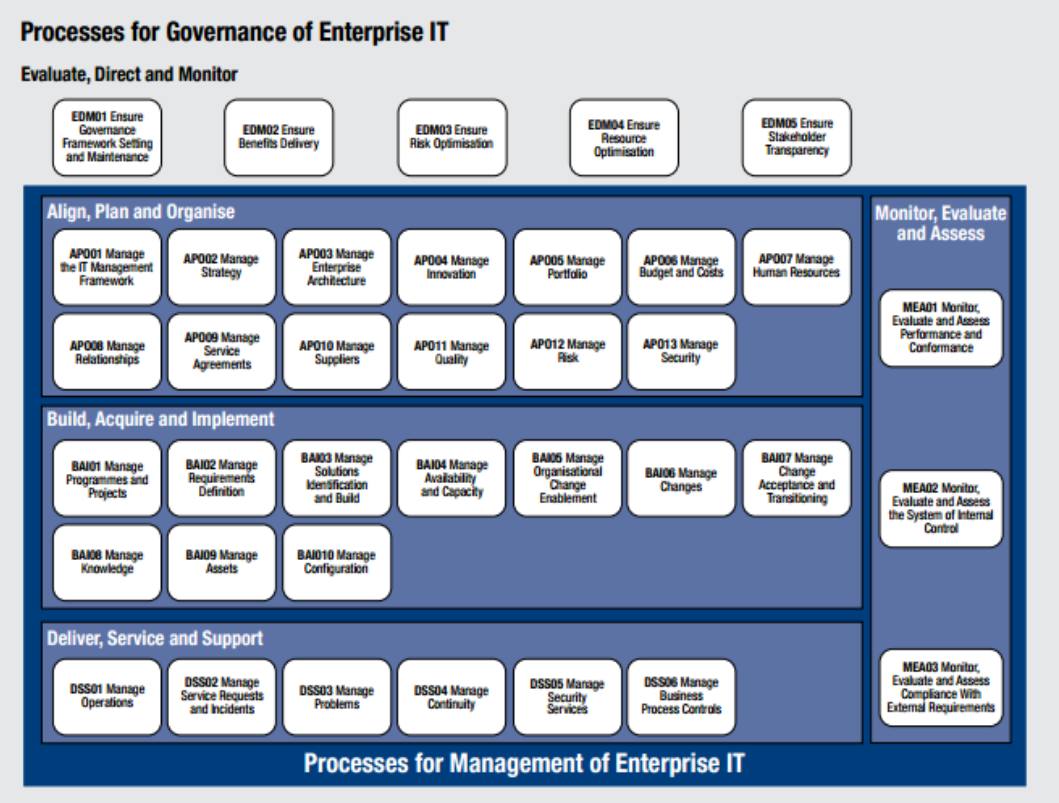

Ilustración 8: Modelo de procesos de COBIT 5 [ISACA, 2012]

Finalmente, podemos decir que COBIT permite administrar y controlar las actividades de TI y los recursos que los soportan, basados en sus objetivos de control y alineados utilizando las metas y métricas aplicadas para cada realidad.

2.2.7 Definición Data Center

Durante los últimos 40 años, los Data Centers se han ido convirtiendo en la columna vertebral de las organizaciones, pues el funcionamiento del 90% de ellas depende de él.

El significado de Data Center, al ser traducido del inglés, es centro de datos o centro de procesamiento de datos. Es una instalación empleada para albergar los sistemas de información y los componentes asociados a ellos como son los datos. Debido a la importancia que tienen estos datos, así como los SI, para las organizaciones, los Data Center deben ser extremadamente confiables, seguros y capaces de adaptarse al crecimiento y la reconfiguración.

Estos centros de datos variarán en tamaño y complejidad dependiendo de la magnitud de la empresa y de los datos que se manejan. A continuación se presentará la descripción de los elementos básicos de un Data Center.

2.2.7.1 Elementos

Dentro de un centro de datos, podemos definir diferentes áreas, las cuales se encuentran diferenciadas de acuerdo a las labores de los equipos que se encuentran en cada una de ellas.

Áreas de un Data Center

- Área de Distribución Principal (MDA): Área concentradora del sistema de cableado y que se encuentra dentro de la sala de cómputo.
- Área de Distribución Horizontal (HDA): Área que incluye los switches de LAN/SAN y los del hardware como teclado, video y mouse para los equipos. En casos donde el centro de datos es pequeño, suele encontrarse incorporado al MDA.
- Sala de Almacenamiento: Área en la que se albergan las piezas de reposición y cableado.
- Sala de eléctrica/mecánica: Área que alberga los servicios primarios como son los circuitos de distribución.
- Sala de telecomunicaciones: Área que mantiene lo equipos que abastecen los datos locales, video y voz necesario para las oficinas de soporte de las operaciones del centro de datos y otras áreas de trabajo.
- Centro de operaciones: Centro de monitoreo del centro de datos. Son centros en el cual se encuentran los técnicos que monitorean el funcionamiento de las redes.
- Sala de entrada: Sala que delimita con los equipos. Interface entre el proveedor de acceso y el cableado estructurado del centro de datos.
- Área de distribución de los equipos (EDA): Racks y gabinetes que contienen los módulos de computación y almacenamiento.
- Sala de cómputo: Espacio donde se encuentran los equipos de datos, telecomunicaciones y cableado.

- Área de distribución zonal (ZDA): Área donde se albergan sólo los equipos pasivos. Se utiliza en caso de salas de cómputo amplias y debe tener una distancia determinada al HDA.

Elementos físicos de un Data Center

- Servidores dedicados: Los servidores dedicados son aquellas computadoras designada para satisfacer determinadas necesidades de los sistemas o de los datos del negocio.
- Cableado: El cableado es el elementos más importante de un Data Center, porque es a través de él que se transmite la energía que permitirá el funcionamiento de los distintos dispositivos tecnológicos así como la comunicación entre diferentes medios.
- Climatización: Es también un elemento sumamente importante pues, con el paso de los años, se ha buscado disminuir el tamaño de los dispositivos electrónicos, lo cual ha concentrado mayor potencia en un espacio más pequeño. Considerando que en una sala de cómputo se contarán con muchos dispositivos electrónicos ubicados cerca uno del otro, es importante ventilar la zona de manera que no se produzca una sobre carga por el calor, lo cual no solo afectaría a los equipos, sino que podría producir un accidente.
- Energía*:* La electricidad es la parte más importante de un Data Center. Una interrupción en el fluido de energía, aunque sea por una fracción de segundo podría ocasionar una falla en el servicio y por lo tanto en el funcionamiento de la empresa. La energía es uno de los elementos que se necesita con disponibilidad del 100% para el funcionamiento de un Data Center, por lo cual se debe hacer todo lo posible para garantizar un suministro confiable e ininterrumpido de energía.
- UPS: De las abreviaturas Uninterrupted Power Supplies, es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía. Permite mantener el centro funcionando durante un período de tiempo determinado en caso de ocurrir un problema con el servicio de energía externa.
- Seguridad: La seguridad es un elemento fundamental en un Data Center, no solo haciendo referencia a la seguridad de acceso físico que se debe tener, brindada por elementos como los sistemas biométricos de acceso a las áreas

críticas o un sistema integrado de cámaras, sino también a controles ambientales que aseguren el buen estado de los equipos del centro de datos.

- PUD: Se refiere al tablero para la distribución de energía confiable y de alto rendimiento. Las PUD se encuentran normalmente equipadas con sistemas de monitoreo de energía, los cuales permiten al usuario monitorear el consumo y la calidad de energía, así como gestionar y planear nuevas necesidades de energía.

Ilustración 9: Elementos físicos que conforman un Data Center. [ADC, 2005]

- Pasillos fríos y pasillos calientes: La instalación de los sistemas en pasillos fríos y calientes responde a la necesidad de proporcionar una refrigeración más precisa y eficiente así como a la reducción de consumo energético. Todos los servidores y equipos de los Data Center están diseñados de manera que los ventiladores con los que se cuentan aspiren aire por la parte delantera y lo expulse por la parte trasera. La primera y la segunda fila de racks que contienen los servidores se colocan de manera que las partes frontales de ambas coincidan en un pasillo, por el cual se expulsará aire frío que enfriará la parte frontal de los servidores (pasillo frio). Si se incorpora otra fila, esta deberá ser colocada de forma que la parte trasera coincida en un pasillo con la parte trasera de la fila anterior, de manera que ambas líneas de rack expulsen el aire ya caliente al mismo pasillo (pasillo caliente)

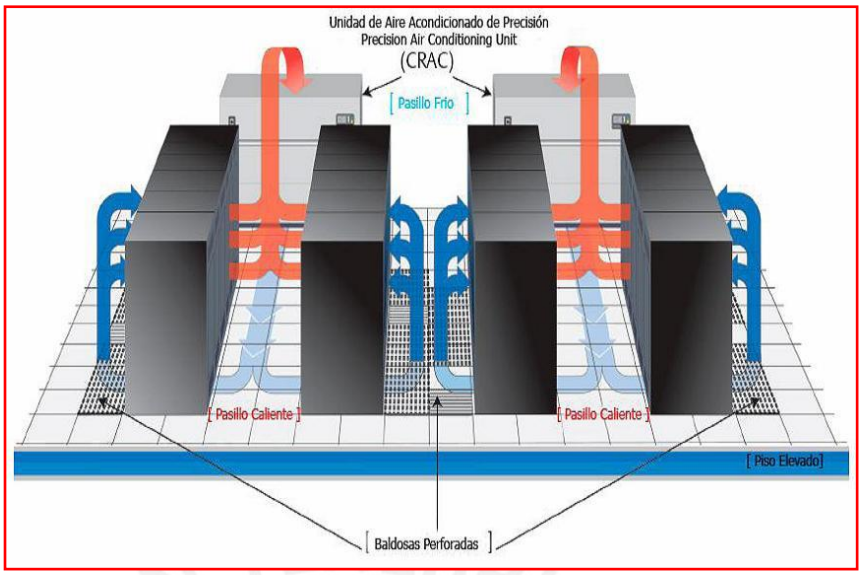

Ilustración 10: Representación de los pasillos fríos y calientes.

2.2.7.2 Características

A continuación se detallarán las características lógicas, físicas, electrónicas, ambientales y de diseño más importantes de un centro de datos.

2.2.7.2.1 Redundancia y disponibilidad

La expectativa de un centro de datos es que cuente con una disponibilidad del 100% sin embargo, todos los centros de datos, sin importar cuan cuidadosamente hayan sido planificados, construidos y manejados, sufrirán de un período de tiempo de indisponibilidad, bien sea intencional o no intencional.
La redundancia es una de las formas de reducir la indisponibilidad, pues no se cuenta con un solo elemento que provee servicios, por ejemplo eléctricos, sino que se contará con alguna medida que permitirá que, de fallar un servicio, el otro pueda asumir el trabajo y así el negocio no sienta el efecto de la falla.

2.2.7.2.2 Fiabilidad

La característica de fiabilidad está estrechamente relacionada con la redundancia y disponibilidad, pues un centro de datos debe ser diseñado de manera que se crea en el hecho de que no se aceptarán fallas durante todo el proceso de su funcionamiento. Uno de los mecanismos que permitirán confiar en el funcionamiento constante de un Data Center será la redundancia.

2.2.7.2.3 Manejabilidad

La manejabilidad nos indica la facilidad para el acceso, localización y reconfiguración de los elementos y características de los Data Center. Es necesario que, durante el diseño de éste, se busque como características la fiabilidad, flexibilidad y la integración de actualizaciones y modificaciones.

2.2.7.2.4 Espacio

Es uno de los elementos más valiosos para el diseño, pues se necesita asegurar que se cuenta con el espacio suficiente y que sea utilizado de la forma correcta. De la misma, para el cálculo del espacio se deberá considerar la posibilidad de la expansión del Data Center, considerando amplias áreas de espacio flexible libre para que se pueda reasignar a una función en particular.

2.2.7.2.5 Distribución

Es recomendable que se plantee la distribución de acuerdo a la realidad actual del centro de datos así como a los objetivos de expansión de la empresa, permitiendo, por ejemplo, reasignar de forma fácil el espacio, administrar los cables para que no superen las distancias recomendadas de tendido, entre otros.

2.2.7.2.6 Administración de cables

El significado de administración de los cables en el Data Center se refiere a la necesidad de tener un servicio de cableado confiable y flexible, de manera que puedan conectarse aplicaciones nuevas sencillamente. Para lograr un sistema cableado confiable, hay ciertos principios fundamentales:

- Se utilizan racks comunes en toda la distribución principal así como en la horizontal, simplificando el montaje de rack.
- Se instalan administradores de cables vertical y horizontal
- Se instalan trayectorias para cables.
- Los cables UTP y coaxiales se separan de la fibra óptica para evitar aplastarla, de la misma forma, los cables eléctrico van en bandejas y la fibra en canales montados en bandejas.

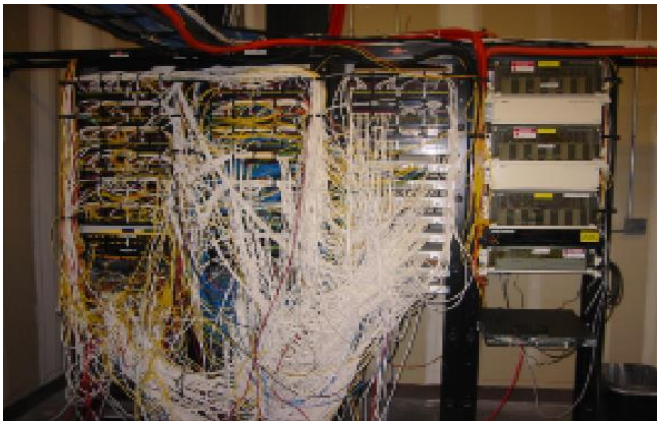

Ilustración 11: Cableado que no ha sido administrado y de difícil comprensión.

2.2.7.2.7 Edificio

Los edificios en los que se establecerá el Data Center pueden ser de dos tipos de acuerdo a las necesidades y solvencia de la empresa. Muchas de ellas cuentan con el dinero adecuado para construir el centro de datos a su medida, con las características que necesita para manejar su negocio, mientras otras adecuan edificios para esta actividad.

La medida más adecuada para la construcción de un edificio para el Data Center, es que éste cuente con el espacio suficiente para colocar, de manera ordenada y definiendo en zonas, todos los equipos necesarios. De la misma forma, es importante definir su ubicación, que no solo van de la mano con consideraciones de tipo estratégico y económico, sino que debe precisar seguridad de la zona frente a riesgos impredecibles de la naturaleza, siendo la sala que alberga los equipos que precisan de mayores cuidados como la existencia de falso piso, falso techo, insonorización, climatización y suministro de energía.

2.2.7.2.8 Falso piso

Constituido por baldosas independientes y movibles en madera o metal recubiertas por un revestimiento plástico que deben reposar sobre soportes de altura regulable que reposan en el pavimento. La altura del falso piso debe encontrarse entre los 0.05 y 0.075 m, pudiendo modificar la altura de acuerdo a las necesidades. El falso piso debe ser robusto e indeformable, resistente a la humedad, a la corrosión y a las cargas mal repartidas, debe asegurar el aislamiento de cargas estáticas y la protección de las personas.

Para el acceso y movimiento de materiales a la zona, los accesos a la sala deben estar equipados de una rampa de desnivel variable, rampa recubierta de goma estriada anti derrapante.

2.2.7.2.9 Ruido

Se debe considerar la posibilidad de altos niveles de ruido en el entorno de trabajo que puedan llegar a perturbar o producir molestias de salud a los trabajadores, por lo cual es preciso adoptar medidas oportunidad de insonorización.
El objetivo de la insonorización es eliminar al máximo las vibraciones sonoras en el interior del local del Data Center y al mismo tiempo evitar su propagación al exterior.
Las medidas más comúnmente adoptadas son la insonorización del techo, suelo y paredes es con materiales como el corcho aglomerado, que reducirá las ondas que vienen o van al exterior, así como la insonorización de las máquinas por medio de carcasas de insonorización o bloques anti vibraciones.

2.2.7.2.10 Paredes

Las paredes deben ser pintadas con pintura ignífuga, cuya misión será retardar la acción destructora en caso de incendio, formando un aislamiento multicelular al reaccionar con la presencia de llamas.
Los tipos de pintura ignífuga pueden ser:

- Extintoras: En contacto con el fuego emiten gases extintores
- Intumescente: Al entrar en contacto con las llamas se hincha, retardando el efecto de incendio.
- Mixtas: Realizarán la labor de las dos anteriores de forma simultánea, se hinchará desprendiendo gases extintores.

Ilustración 12: Falso piso

2.2.7.2.11 Ubicación de gabinetes

Los gabinetes deben ser ubicados de manera que el aire acondicionado oriente los flujos para realizar un intercambio adecuado de calor. Los patrones recomendables para la orientación son en bloques y conformando figuras geométricas, permitiendo extraer el calor generado por los equipos.

2.2.7.2.12 Temperatura

La temperatura es un factor importantísimo considerando que los equipos estarán en trabajo constante y por lo tanto generando calor constantemente. Los problemas principales derivados de la elevación de la temperatura son el apagado de los equipos por recalentamiento así como el estrés en los componentes por cambios de temperatura.

La temperatura promedio establecida es entre los 22°C y 24°C

2.2.7.2.13 Humedad

La humedad también es un factor importante pues puede producir deterioro en los equipos. Cuando los niveles de humedad son muy altos producirá corrosión, condensación y hongos, mientras que si es muy baja podría generar electricidad estática.

2.2.8 Tier

Tier es una clasificación y estándar de funcionamiento que se otorga a los Data Center basado en los niveles de disponibilidad, continuidad y capacidad que puedan brindar, permitiendo que se puedan realizar comparaciones en base al funcionamiento, capacidades y costos entre diferentes tipos de infraestructuras.

Los Tier fueron definidos por The Uptime Institude, un consorcio de empresas que ayudan a sus miembros a evitar tiempos caídos, optimizar la inversión de infraestructura del Data Center y asegurar el funcionamiento continuo de las instalaciones.

Conforme más alto es el Tier, mayor es la confiabilidad en el Data Center.

	Tier I	Tier II	Tier III	Tier IV
Downtime anual	28.8 hrs	22.0 hrs	1.6 hrs	0.8 hrs
Disponibilidad	99.671%	99.741%	99.982%	99.995%

Tabla 1: Tabla comparativa de Tier de acuerdo a tiempo de caída y disponibilidad.

2.2.8.1 Tier I: Infraestructura básica

Un Data Center con Tier I no contará con la capacidad de redundancia de los componentes, provocando que con la falla de un único componente o distribución impacte en el funcionamiento de todo el sistema de cómputo.

Esta infraestructura puede considerarse adecuada y aplicable a negocios pequeños, en la que se ejecuten únicamente procesos internos de la organización.

2.2.8.2 Tier II: Infraestructura de componentes redundantes

Los Data Centers que encajan en esta clasificación sí cuentan con componentes redundantes pero limitados. La redundancia se dará en equipos críticos como fuentes de poder, procesadores, UPS, generadores, circuitos eléctricos, entre otros.

Esta infraestructura es aplicable a pequeños negocios, donde no se ofrecen servicios “online” o “real-time”.

2.2.8.3 Tier III: Infraestructura con mantenimiento simultáneo

El Tier III describe a Data Centers que cuentan con todos sus componentes redundantes y vías de distribución también redundantes, siendo una de ellas activa y la otra pasiva. Los componentes de esta infraestructura pueden ser removidos durante un evento planeado sin generar interrupciones en el sistema, sin embargo es susceptible a caídas durante actividades no planeadas.

Buscando establecer servicio constante de distribución de poder entre el UPS y los equipos de cómputo, Tier III requiere que existan dos fuentes de poder funcionando simultáneamente, característica que no puede ser adquirida en nuestro país debido a determinaciones legales establecidas que indican que una

misma área física no se puede contar con el servicio de dos proveedores diferentes de energía.

De la misma forma, esta categoría de Tier recalca la existencia de elementos importantes en lo que se refiere a las características físicas del centro de datos, indicando que los muros exteriores no deben tener acceso por ventanas, que debe existir seguridad perimetral, entre otros.

Esta infraestructura es adecuada para compañías que dan soporte 24/7, como centros de servicios e información.

2.2.8.4 Tier IV: Infraestructura tolerante a fallas

Un Data Center con Tier IV cuenta con todos sus componentes redundantes, incluyendo las vías de distribución quienes están activas simultáneamente. En este caso, los componentes podrán ser removidos durante un evento planeado o no planeado (alarmas de incendio, supresor de incendios, entre otros) sin generar interrupciones en el sistema.

Esta clasificación es adecuada para las compañías con presencia en el mercado internacional, que brindan servicios 24x365, compañías basadas en el comercio electrónico, transacciones Online y entidades financieras. Sin embargo, como mencioné anteriormente, esta clasificación no puede ser alcanzada en nuestro país debido a limitaciones legales.

En el anexo B podremos apreciar el cuadro comparativo de la clasificación TIER en el cual se señalan todos los factores que permiten calificar la seguridad de un Data Center.

2.2.9 Seguridad en Data Center

La seguridad debe garantizar que tanto los equipos como la información que conforman la infraestructura del Data Center brinden el suficiente grado de confidencialidad, integridad y disponibilidad necesaria para el uso adecuado del mismo.

Los Data Center son el depósito de la información de una empresa, por lo tanto debe ser protegido contra daño, destrucción y robo. Se debe hacer lo posible para aislar las condiciones ambientales de la sala de cómputo y eso se logra con una

estructura fuerte y con los elementos necesarios para evitar o disminuir los efectos de un desastre.

Los mecanismos básicos para proteger los activos de información son los controles de acceso lógico[13] a ellos. Los encargados de seguridad de información deben lograr el control de los accesos por medio de identificación, autenticación y registro de usuarios, con el fin de evitar el acceso y la modificación no autorizada de datos valiosos para la empresa así como la restricción del uso de ciertas funcionalidades de los sistemas de control.

Al igual que los accesos lógicos, los accesos físicos son otro medio de riesgo para la integridad del Data Center. Entre los riesgos existentes podemos mencionar las entradas físicas no autorizadas a la sala de cómputo, daño o robo de los equipos, reproducción de los datos sensibles, entre otros. Es por ello que se debe controlar el acceso al edificio así como a las diferentes áreas de éste.

Algunos de los controles de acceso físico más utilizados son:

- Cerraduras con pestillo, combinación con teclados numéricos o con tarjetas magnéticas.
- Controles biométricos[14] para activar las cerraduras.
- Bitácora o registros manuales de ingresos.
- Tarjetas con fotografía, fotocheck.
- Circuitos cerrados de televisión ubicados en puntos estratégicos.
- Puertas de tipo esclusas [15]

[13] [Tupia,2011] Alcanzar y operar los SI y los datos involucrados.

[14] Técnica basada en características o rasgos únicos que se utilizan para reconocer al usuario que desea tener acceso, por medio de sus características físicas.

[15] Una puerta es abierta tras el cierre de las puertas anteriores a ella.

Ilustración 13: Conjunto de mecanismos de seguridad de acceso físico,

Las exposiciones medioambientales y catástrofes naturales son fenómenos impredecibles pero que pueden generar riesgos en el funcionamiento de nuestro Data Center. Fenómenos como movimientos sísmicos, inundaciones, tormentas, huracanes, erupciones volcánicas, entre otros afectan principalmente a la continuidad de las funciones realizadas por el Data Center.

Los principales controles deben asegurar y vigilar las instalaciones físicas del Data Center, así como los suministros de energía para ,de esta forma, poder determinar el grado de las amenazas ambientales y desastres naturales y poder establecer los planes y medidas de emergencia que serán tomadas al ocurrir estos.

Los principales mecanismos de seguridad ambiental son:

- Las alarmas son un mecanismo que provee cierto grado de seguridad contra desastres y amenazas en general, desde incendios hasta el ingreso de delincuentes, es por ello que la presencia de un panel de control de alarmas es básico para cualquier fin.
- Los detectores de agua, inundaciones o humedad deben encontrarse de forma obligatoria en las salas de cómputo y servidores, ubicados normalmente en el falso piso. Su labor será la de producir una señal audible que permita activar planes de emergencia previamente establecidos de acuerdo a la magnitud y tipo de circunstancia.
- El detector de humo también es un elemento importante pues detecta la presencia de partículas de humo y emite una alarma que permitirá detectar el inicio de un incendio.
- La presencia de extintores manuales de incendio y alarmas también manuales son muy importantes. Deben ser colocados en zonas estratégicas cercanas a

los puntos con más riesgo de generación de incendio y deben ser repartidos a lo largo de las instalaciones.

- Los sistemas de supresión de incendios son un mecanismo que incluye todas las alarmas y mecanismos anteriormente especificados para evitar un incendio. Sin embargo, cuenta con un mecanismo que permite no solo informar del inicio de un incendio, sino brindar la solución a él por medio de la supresión de fuego. La aplicación del sistema de supresión de incendios en un Data Center necesitará de elementos más complejos pues no puede ser utilizado con agua ya que esto provocaría el daño de los activos. Por eso, deberá contar con un sistema de gas adecuado de acuerdo a las características establecidas. Estas opciones son: Sistema de gas Halón, Sistema FM-200TM, Sistema de Argón y Nitrógeno, Sistema basado en Dióxido de Carbono.

Ilustración 14: Mecanismos de seguridad medio ambiental.

Al igual que los elementos mencionados anteriormente, se deben contar con otros mecanismos que permitan la seguridad del Data Center, como:

- Protectores de voltaje: dispositivos que protegen a los equipos de cambios que puedan producirse en el voltaje.
- UPS: Regula la energía de manera que haya consistencia eléctrica en los equipos durante un periodo de tiempo limitado.

2.2.10 Formas de administración

2.2.10.1 Servicio de hosting y housing

2.2.10.1.1 Hosting

Realizando la traducción del término del inglés, puede entenderse el hosting como alojamiento. Es el servicio que busca brindar a usuarios de Internet un mecanismo de almacenamiento de distintos tipos de información (por ejemplo imágenes, videos, documentos y aplicaciones) y que éstos puedan ser accedidos vía Web. Existen, principalmente, dos tipos de alojamiento:

- Hosting dedicado: es aquél en la que la empresa brinda un conjunto de servidores para prestar servicio a la información del cliente, asegurándole que no comparte los recursos del servidor con otros clientes y que tiene control total sobre el servidor,
- Hosting virtual: conocido también como cloud hosting es una mezcla entre hosting compartido y hosting dedicado. Consiste en un servidor físico dividido en diferentes servidores virtuales, los cuales pueden ser vistos como servidores dedicados pues su funcionamiento será de acuerdo a las necesidades del usuario y eliminando las limitaciones físicas para el crecimiento en tiempo real, lo cual lo hace una solución extremadamente flexible.

Ilustración 15: Hosting.

2.2.10.1.2 Housing

Consiste en la venta o alquiler de un espacio físico en un centro de datos, en el cual el cliente colocará su propia sala de cómputo. El proveedor es el responsable de abastecer de servicios de electricidad, conexión a Internet, mantenimiento, entre otros. La infraestructura de TI es elegida completamente por el cliente, pero muchas veces es el mismo proveedor quien da las sugerencias de adquisición y realiza la venta.

Ilustración 16: Housing.

2.3 Estado del Arte

En la actualidad se realizan con mucha frecuencia las auditorías a Data Center debido a la alta importancia y cuidado que se debe tener con ellos por el manejo de información y sistemas core de los negocios.

A continuación se describirá los puntos tratados en una auditoría de Data Center.

2.3.1 Definición de los objetivos de la auditoría

El primer paso a realizar es la definición de los objetivos de la auditoría. En la mayoría de casos estos coinciden, sin embargo, la definición de éstos dependerá del motivo por el cual ha sido solicitada la auditoría.

Los principales objetivos son:

- Determinar si se han implementado controles proporcionales a los recursos de información que se manejan así como a su nivel de importancia.
- Evaluar las condiciones de los equipos del Data Center.

2.3.2 Seguridad física de la consola de sistema.

Se intenta verificar los parámetros físicos que permiten o prohíben el acceso a la consola del servidor y de las estaciones clientes.

Si alguien lograra acceder a la consola del servidor o de la estación cliente podría existir la posibilidad de obtener accesos no autorizados al sistema y podría generar cambios en la configuración de seguridad, dando accesos no autorizados a otros usuarios o a él mismo.

2.3.3 Continuidad de negocios y planes de contingencia.

Se busca comprobar que hay planes desarrollados para facilitar la continuidad de servicios de control de acceso.

En caso de ocurrir un evento inesperado, como por ejemplo la falla en el servicio de electricidad, deberían existir planes que eviten que el sistema sea impactado, en el aspecto de seguridad, por ese evento. Es decir, que no exista la posibilidad de que, al producirse un evento inesperado, los controles de acceso puedan quedar abiertos a todos los usuarios, poniendo en riesgo la integridad de la información y de los sistemas del Data Center.

2.3.4 Modificación del sistema de gestión de cambios.

Se debe confirmar que los cambios en el sistema se realizan siguiendo una guía de procedimientos de cambio, para así verificar que en el proceso no se hayan dejado vulnerabilidades que puedan ser explotadas por otras personas. De la misma forma, las modificaciones que no cuentan con un proceso detallado de cómo hacerlo, lo cual podría afectar a otros sistemas con los que interactúe.

2.3.5 Solicitud de respuesta ante alarmas.

Se verifica que las alarmas generadas al detectar un riesgo sean reconocidas y respondidas.

Las alarmas son controles que al descubrir un error en la seguridad o en el funcionamiento de un sistema se activan, avisando del inconveniente a los

usuarios y permitiendo tomar medidas correctivas. En el caso de no ser reconocidas es muy probable que la persona encargada no se dé cuenta de ellas y por lo tanto se genere un margen de tiempo en el cual la vulnerabilidad se encuentra abierta. De la misma forma, se debe asegurar que cuando una alarma empieza a dar aviso se le debe dar respuesta inmediata para no afectar la seguridad.

2.3.6 Procesos de modificación y eliminación de accesos.

Se busca asegurar que los accesos serán modificados o eliminados de acuerdo al cambio de labor que tenga un usuario del sistema. Así, si un empleado deja de trabajar en la empresa, su acceso debería ser eliminado, mientras que un empleado que cambia de labor, debería tener acceso a los datos necesarios para la nueva labor y perder los accesos a los datos que ya no necesitará.

2.3.7 Programa de concientización de seguridad.

Este objeto de auditoría es fundamental para el funcionamiento de cualquier empresa. Los empleados que laboran en ella deben conocer las políticas y procesos de seguridad aplicados por la compañía, de manera que puedan razonarlos y conocer cuáles son las acciones que están permitidas y cuáles las que no.

2.3.8 Seguridad perimetral

El acceso al Data Center es de tanta importancia como el acceso a los sistemas e información.

No solo se debe controlas el acceso a la puerta donde se encuentra el Data Center, también debe ser controlado el acceso al edificio donde se encuentra, pues de tenerse un acceso no controlado cualquier persona malintencionada podría entrar y llevarse alguno de los servidores o componentes importantes del Data Center.

Para el control de los accesos a la sala de cómputo se verifica la existencia de alguna técnica o dispositivo colocado en las entradas que permita verificar la identidad de quien está ingresando, reduciendo así la probabilidad de ingreso de una persona no autorizada. De la misma forma, contar con un plan de contingencia

en el caso del fallo de alguno de estos mecanismos, pues en su gran mayoría se utilizan dispositivos eléctricos que están sujetos a eventos imprevistos.

2.3.9 Revisión de antecedentes

Este aspecto es muy importante a considerar, pues son los trabajadores del Data Center quienes monitorearán su funcionamiento y estarán en contacto directo con él. Por esta razón, se debe hacer una revisión de antecedentes penales tanto como policiales a cada una de las personas que se pretende contratar para el trabajo en el Data Center.

2.3.10 Autorización de documentos

El objetivo de este control es verificar que cada persona de la organización que labore en el centro de datos cuenta con un documento de autorización que indique las áreas a las que tiene acceso, el motivo por el cual tiene los accesos y que debe estar firmada por su supervisor. Esto se realiza con el fin de asegurar que los accesos sean únicamente los necesarios de acuerdo a la labor del empleado.

2.3.11 Notificación de ingreso

Todo Data Center debe contar con un sistema de vigilancia que permita monitorear todas las áreas de manera simultánea. Sea por un mecanismo de cámaras o por señales de alarmas, se debe conocer el movimiento que se produce en cada una de las salas y espacios libres, permitiendo detectar acciones incorrectas o ingresos forzosos por parte de terceros.

2.3.12 Movimientos sísmicos

Por ser un fenómeno físico, no puede realizarse una detección anticipada, sin embargo las medidas que se deben tomar son muy importantes pues el desastre no puede ser predicho.

Es importante verificar que la zona en la que se ha construido o instalado el Data Center no sea una zona altamente riesgosa en lo que respecta a los movimientos sísmicos. El Data Center debe estar construido en un área en la que se conoce las características del suelo y en las que se conoce que son seguras.

2.3.13 Agua y vías de aniego

El Data Center debe contar con la estructura adecuada que permita que en caso de una inundación los cables y equipos no sean afectados por el agua. Una de las soluciones posibles es la existencia de falsos pisos, que mantengan los cables y equipos en un espacio suficientemente elevado como para evitar el contacto del agua con ellos. De la misma forma se debe contar con un detector de agua que informe sobre la aparición de ésta y bombas que se activen con la alarma y puedan apoyar en retirar el agua de la zona.

Otros mecanismos también son la utilización de material aislante para la fabricación de cables y equipos, siendo ésta una medida sumamente importante.

2.3.14 Recuperación ante desastres.

El Data Center debe contar con un plan de recuperación de desastres que permita que en caso de un desastre que supere los controles establecidos el negocio no se vea afectado.

Una de las medidas que puede ser tomada para evitar estas circunstancias es el contrato con proveedores que brinden “sites” ubicados en otros lugares del país y que de dejar de funcionar el principal pueden aportar apoyo para no afectar la continuidad del negocio.

Los contratos con los proveedores podrían darse en las opciones de redundancia denominadas:

- Hot sites: Se cuenta con un servidor capaz de imitar el funcionamiento del servidor principal en caso que este falle. Este servidor deberá ser un duplicado exacto del servidor original y la arquitectura también deberá ser una copia exacta de la arquitectura manejada en el Data Center original.
- Warm sites: Es muy similar a un Hot site, cuenta con la misma arquitectura e infraestructura que el Data Center, pero el backup de información no será realizado de forma tan constante como en el hot site.
- Cold sites: En este caso, el servidor no está configurado como el servidor principal y solo sería útil para tomar medidas en las aplicaciones principales del negocio.

Todos los objetos mencionados anteriormente forman parte de la lista de puntos claves en la auditoría de Data Center.

2.4 Discusión sobre el estado del arte

Al realizar la revisión del estado del arte podemos observar que no existe ninguna guía estándar para el desarrollo de una auditoría en Data Center de manera que puedan cubrirse todos los aspectos necesarios.

Los puntos tratados son de suma importancia, sin embargo, hay muchos vacíos que no son considerados y que pueden ser motivos y puntos de inestabilidad e inseguridad para el manejo de la información.

El marco COBIT, con sus nuevas modificaciones nos permitirá incluir en la metodología temas relacionados con riesgos e inversiones que podrán brindarnos una mirada más amplia al entorno y que a su vez nos guiarán en la consideración de nuevos puntos de evaluación.

De la misma forma, contar con el estándar y clasificación TIER nos permitirá tener en medidas exactas los puntos críticos y que son necesarios evaluar en los Data Center.

Con este proyecto, se logrará establecer un conjunto de procesos que guíen al auditor en la realización de una auditoría con base en marcos y estándares internacionales y que estén adaptados a la realidad actual de nuestro país y de la tecnología.

CAPÍTULO 3: PROCEDIMIENTOS GENERALES DE AUDITORÍA

3.1 Introducción

En este capítulo se desarrollarán los mecanismos para establecer aspectos clave en la auditoría como son el alcance, el objetivo general y los objetivos específicos que harán las veces de criterios.

Una vez determinados estos elementos del proceso de auditoría, se indicará una serie de lineamientos que pueden fungir de criterios para la auditoría del Data Center de acuerdo al estándar y clasificación internacional TIER, la norma ISO 27002 [ISO, 2005a], COBIT 5.0 [ISACA, 2012] y algunos estándares de la norma NIST lo cuál asegurará que se evaluarán los elementos necesarios para asegurar la seguridad física y medio ambiental del Data Center.

3.2 Mecanismos para determinar el alcance de la auditoría

La determinación del alcance de la auditoría es el primer paso cuando se ha decidido dar inicio a la misma.

La definición del alcance permitirá conocer:

- ¿Cuáles son los factores que serán considerados en la evaluación?
- ¿Hasta qué punto se profundizarán cada uno de los factores?
- ¿Qué elementos del escenario organizacional estarán involucrados?

De igual manera, el alcance permitirá aclarar al auditado cuáles son los límites de la evaluación, de manera que los puntos a evaluarse sean los más críticos y que brinden una mejor visión de la realidad.

Para la definición del alcance de la auditoría es necesario conocer la realidad del Data Center. Con realidad se hace referencia a la naturaleza de éste, si brinda servicios de Housing, servicios de Hosting o ambos, así como saber si se busca evaluar un Data Center tercerizado o si es propio.

Es también importante conocer cuáles son los elementos de auditoría física y medio ambiental que pueden ser auditados, motivo por el cual, a continuación se detallarán los aspectos físicos y medio ambientales que pueden ser auditados.

3.2.1 Elementos auditables de seguridad física

Los elementos de seguridad física que pueden ser auditados son aquellos relacionados con el cuidado físico del Data Center, para su funcionamiento continuo así como para protegerlo de incidentes o personas malintencionadas.

3.2.1.1 Grado de obsolencia

La obsolencia en los equipos puede es un factor que puede ser muy perjudicial para la continuidad de servicios que ofrezca el Data Center, pues el desgaste de los equipos podría ocasionar problemas técnicos que afecten o indispongan el servicio. Es importante recalcar dos términos relacionados con este punto de análisis:

- Obsolencia técnica: Se refiere al tiempo excedido por el equipo de acuerdo al tiempo de vida determinado en la fabricación del mismo o de acuerdo a prácticas internacionales.
- Obsolencia por su uso: El desgaste del equipo debido al tiempo que ha sido utilizado

3.2.1.2 Ubicación del Data Center

De acuerdo a buenas prácticas de seguridad de información, la ubicación del Data Center principal, tanto como del alterno, deben encontrarse alejados en un rango de al menos 4 Km. El objetivo de las buenas prácticas en la ubicación se da principalmente para evitar que en un evento no previsto, como puede ser un incendio o terremoto, se vean comprometidas tanto el área administrativa así como el Data Center, generando una pérdida total para la organización.

Dentro de este punto, es importante considerar que el Data Center debe ubicarse en una zona donde se haya realizado previamente un análisis y que no sea riesgosa con respecto a desastres naturales, vibraciones, entre otros.

3.2.1.3 Puertas de acceso

Las puertas deben ser de un material resistente a golpes y maltratos y además contar con algún mecanismo de seguridad de acceso, de manera que para que ésta sea abierta deba verificarse que quien desea ingresar cuenta con los permisos necesarios para hacerlo, evitando el paso de personas mal intencionadas. De la misma forma, debe haber una sola forma de acceso al Data Center, evitando colocar medios de acceso sensibles como las ventanas.

3.2.1.4 Cableado

En lo que respecta al cableado, debe contarse con una administración correcta de los mismos, que facilite la realización de modificaciones o ampliaciones en el Data Center. Para lograrlo se pueden usar canaletas, gabinetes y etiquetas.

3.2.1.5 Falso piso

La existencia de un falso piso busca proteger tanto a los equipos y como al cableado de incidentes que podría producir una inundación o fuga de agua en el edificio.

3.2.1.6 Documentación de procedimientos de asignación

Se debe guardar un registro físico o virtual de las asignaciones de permisos como de los dispositivos de seguridad asignados a los empleados, de manera que se pueda tener control sobre los mismos. Dentro de los dispositivos de seguridad para empleados o visitantes (proveedores, reguladores, auditores, clientes, etc.) están las tarjetas de identidad, llaves tipo tokens, contraseñas y demás

3.2.1.7 Dispositivos biométricos

Por medio de los dispositivos biométricos se controlará el ingreso y salida de las personas, asegurando que no ingresen extraños y con ello brindando mayor seguridad. Estos dispositivos deben ser capaces, también, de registrar los intentos positivos y fallidos de ingreso.

3.2.1.8 Señalización

Tantos los ingresos como salidas deben estar señalizados, así como las áreas de alto voltaje o que cuentan con algún riesgo. Con esto no solo se busca cumplir con las regulaciones dadas por Defensa Civil así como por el Ministerio de trabajo, sino también asegurar la salud y bienestar del personal de la organización.

3.2.1.9 Procedimientos de emergencia

Deben documentarse los procedimientos de acción y salida en caso de una emergencia y se debe contar con capacitaciones constantes a los empleados involucrados con el Data Center para poder en práctica los procedimientos.

3.2.1.10 Sistema de vigilancia

Se debe contar con un mecanismo de vigilancia permanente que permita controlar y conocer las acciones que se realizan alrededor y dentro del Data Center. Con ello se busca controlar las acciones que puedan ser perjudiciales para el mismo.

3.2.1.11 Sistema de red independiente

Es recomendable poseer un segmento de red totalmente independiente al del resto de la empresa para el uso exclusivo del Data Center. Con esto se busca evitar problemas que puedan producirse en la red debido a sobrecargas de trabajo, ingreso de virus que busquen apoderarse de información importante, entre otros, que provengan de alguna otra área de la empresa.

3.2.1.12 Desplazamiento libre

Los pasillos y accesos del Data Center (de todas las salas que lo conformen) deben encontrarse libres para facilitar el desplazamiento del personal responsable, la salida del Data Center y para la instalación de nuevos equipos cuando sea necesario.

3.2.1.13 Programa de mantenimiento correctivo

Se debe contar con un programa que permita un control constante del estado y posibles inconvenientes que puedan producirse en los equipos del Data Center, tanto de los funcionales así como de los equipos de respaldo.

3.2.2 Elementos auditables de seguridad medio ambiental

Por su parte, en este aspecto encontramos:

3.2.2.1 Humedad

3.2.2.1.1 Sensores de aniego

Estos sensores son colocados en el piso con el objetivo de poder detectar de forma temprana las inundaciones que puedan ocurrir en las instalaciones y que pueden afectar al Data Center.

3.2.2.2 Temperatura

3.2.2.2.1 Sistema de extinción de incendios

Se debe contar con sistemas de extinción que permitan resolver de manera rápida la ocurrencia de un incendio dentro del local del Data Center. Este sistema de extinción debe utilizar una tecnología acorde con la realidad del Data Center como son los materiales y el personal que trabaja en él.

3.2.2.2.2 Detectores de humo

Los detectores de humo deben ser enlazados con el sistema de supresión de incendios, de manera que cuando éste detecte la presencia de partículas de humo se inicie el proceso de supresión de incendios inmediatamente.

3.2.2.2.3 Detectores de humedad

Estos dispositivos apoyarán en la detección del nivel de humedad con el que cuenta el Data Center. El factor humedad puede ser muy perjudicial para el funcionamiento del Data Center pues de tener valores muy elevados puede degradar el material de los equipos y de tener valores muy bajos producir energía estática.

3.2.2.2.4 Refrigeración

Contar con equipos de aire acondicionado que permitan controlar la temperatura y humedad dentro de la sala de servidores así como en las otras salas del Data Center.

3.2.2.2.5 Pintura anti fuego

Contar con pintura anti fuego en las paredes permitirá disminuir y retrasar los efectos que se generarían de producirse un incendio en el Data Center. Éste podrá controlar o disminuir el fuego, de acuerdo a sus características.

3.2.2.3 Suministro eléctrico

3.2.2.3.1 Fluido eléctrico de respaldo

Contar con un suministro de electricidad de respaldo, como son los grupos electrógenos, para asegurar la continuidad del negocio y el bienestar del personal que se encuentre dentro del Data Center frente a un corte eléctrico.

3.2.2.3.2 UPS

Se debe contar con equipos UPS con la capacidad suficiente para permitir la autonomía necesaria para el encendido del grupo electrónico.

3.2.2.4 Polvo

3.2.2.4.1 Sensores de polvo

Estos sensores permitirán determinar cuándo los equipos están siendo invadidos por el polvo, de manera que se pueda tomar acciones y evitar que éste pueda deteriorar los equipos.

3.2.2.5 Magnetismo

3.2.2.5.1 Adecuada ubicación de cables

La adecuada ubicación y distribución de los cables eléctricos como de red ayudaran a evitar la interferencia que podría producirse entre ellos, generando pérdida de datos, interferencia en la comunicación o errores en la transmisión.

Una vez definidas las necesidades de auditoría del cliente y revisando los factores que pueden ser auditados en lo que respecta a la seguridad física y medio ambiental de un Data Center, se podrá establecer los límites de la auditoría a realizar y con ella detallar el alcance y limitaciones que ésta tendrá.

Con esto, se podrá proceder a establecer el objetivo general de la auditoría y con él los objetivos específicos que finalmente serán vistos como resultados de la misma.

3.3 Mecanismos para definir el objetivo general

Para empezar con la descripción de los mecanismos para la definición del objetivo general, debemos, en primer lugar, entender lo que es el objetivo general.

El objetivo general se refiere al propósito principal y general del proyecto[16]. En este caso, se expresará a grandes rasgos, la situación o resultado que se desea alcanzar con la verificación de los criterios[17].

Va depender del tipo de empresa, como se mencionó anteriormente en el tema de hosting y housing, que se está auditando y de las características del Data Center con el que se cuenta.

Para poder determinar de manera correcta y precisa el objetivo general que tendrá la auditoría se deben hacer dos pasos principales.

3.3.1 Entrevista con el cliente

En lo que respecta a la entrevista con el cliente, se deberá conversar y conocer al área involucrada en la auditoría, tanto a quienes solicitan la realización de la misma como a las áreas intermedias que se encontrarán involucradas en la evaluación.

Siendo el Data Center el objeto de auditoría, algunas de las áreas que podrían estar involucradas en la evaluación son las siguientes:

- Gerencia General
- Área de control interno
- Área de auditoría interna
- Intendencia
- Infraestructura
- Seguridad Integral
- Contraloría (En caso de ser empresa del estado)

La entrevista con estas áreas permitirá conocer cuáles son las incertidumbres que buscan cubrir con el resultado que se obtenga de la auditoría, los puntos en los que se encuentran involucradas las diferentes áreas para el funcionamiento y

[16] [RAE,2012]
[17] [ISO, 2012]

administración del Data Center y el motivo por el que creen se debe realizar una evaluación.

3.3.2 Revisión documentaria

La revisión documentaria se refiere a la recopilación y análisis de toda la documentación que maneja la empresa y que involucra la administración del Data Center.

Los documentos nos servirán para conocer las características que debe cumplir el Data Center de acuerdo a leyes, regulaciones o políticas de la empresa y que al mismo tiempo nos permitirán poder ir avanzando en el establecimiento de criterios a evaluar.

Entre los documentos a los cuáles se debe pedir acceso y revisar tenemos:

- Contratos con clientes y proveedores.
- Leyes y Regulaciones del Estado
- Políticas y procedimientos internos
- Informes de auditoría de Data Center anteriores

De la misma forma, es importante considerar que de acuerdo a los procedimientos que serán descritos en capítulos posteriores, el objetivo general podrá estar relacionado principalmente a tres frentes:

Verificar el cumplimiento de Tier I o II: El estándar y clasificación internacional Tier, permitirá que se verifique el cumplimiento de normas internacionales de seguridad tanto física como medio ambiental en el Data Center que se desea auditar. Permitiendo clasificarla, de acuerdo a sus características, en Tier I, Tier II o, en ciertos casos, en ninguno de ellos.

Verificar la seguridad física del Data Center: Mediante la evaluación de diferentes criterios se podrá evaluar el nivel de seguridad física con el que cuenta el Data Center, evaluando los equipos, los accesos y la administración del espacio, para así obtener como resultado los puntos débiles del mismo y permitiendo darse cuenta de ellos para tomar las medidas adecuadas.

Verificar la seguridad medio ambiental del Data Center: Mediante la evaluación de seguridad medio ambiental se busca verificar que el Data Center cuente con las

medidas adecuadas para que pueda contrarrestar la presencia de incidentes medio ambientales como son los incendios, exceso de humedad, inundaciones, desastres naturales, etc.

Como se indica en los tres puntos detallados anteriormente, el objetivo general podrá ser específico o amplio de acuerdo a las necesidades de la empresa, pero deberá detallarse de la forma adecuada ya que lo que se indique en éste será lo que debe dar como resultado la auditoría.

3.4 Procedimientos para establecer los criterios

Una vez establecidos el alcance de la auditoría que se realizará así como el objetivo que se busca cumplir con ésta, se podrá empezar con el establecimiento de los criterios que se tomarán en cuenta y evaluarán durante el desarrollo de la auditoría y con los cuáles se dará el resultado de la evaluación al cliente.

Para dar inicio al establecimiento de criterios será necesario tomar en cuenta la revisión de los documentos que el cliente nos haga llegar. Esta documentación fue previamente revisada para la definición del objetivo general, sin embargo con ella se puede obtener, también, los criterios necesarios a cumplir por el Data Center de acuerdo a políticas y procedimientos internos, de acuerdo a contratos establecidos con los proveedores y cliente, leyes y regulaciones nacionales y también por auditorías previamente realizadas.

Para el establecimiento de criterios se deberá armar un cuadro de doble entrada en el cuál —de acuerdo a las necesidades y objetivos de la auditoría— se irán detallando los puntos que serán evaluados relacionándolos con el marco de control, clasificación o ISO en el cuál se especifica su utilidad y aplicación.

Para dar inicio a la elaboración del cuadro de criterios se debe tener en claro cuáles son los marcos de control, clasificaciones y normas que se utilizarán de acuerdo al objetivo y alcance que se haya establecido de la auditoría. Una vez definidos éstos se debe proceder con el estudio detallado de cada uno de los documentos con el objetivo de poder distinguir entre los criterios que serán evaluados y aquellos que no

lo serán distinguiendo aquellos que pertenecen al análisis medio ambiental o físico del Data Center.

En el anexo B del presente documento se detalla un conjunto de cuadros de las características de funcionamiento, capacidad, seguridad y costo de un Data Center de acuerdo a la clasificación y estándar internacional TIER, el marco COBIT 5.0 y la norma ISO/IEC 27002.

3.5 Declaración de aplicabilidad

Todos los criterios mostrados han sido extraídos y plasmados de manera que se puedan identificar los puntos de atención al momento de la auditoría. Sin embargo, es importante tomar en cuenta que los criterios a tomarse en cuenta para la auditoría que se vaya a realizar dependen no solo de los criterios mostrados, sino también de la intención del cliente con la auditoría y de los resultados que quiera obtener con la misma.

En ahí donde debemos distinguir la declaración de aplicabilidad. El cliente, un vez revisados los criterios y conociendo los puntos que pueden evaluarse deberá distinguir cuáles de éstos son los adecuado de acuerdo a sus expectativas y a los objetivos que haya trazado para la auditoría. Así, un cliente puede pedir una evaluación para el cumplimiento de la ISO 27002, mientras otro busca que otro quiere evaluar cuáles son sus puntos débiles para poder clasificar su Data Center con alguno de los niveles de TIER.

CAPÍTULO 4: PROCEDIMIENTOS DE LEVANTAMIENTO DE INFORMACIÓN

4.1 Introducción

En este capítulo se detallarán de forma clara y precisa los procedimientos que deben seguirse para el desarrollo de la auditoría física y medioambiental de un Data Center.

Se procederá a la descripción de los procedimientos para el levantamiento de las evidencias, la documentación de los hallazgos y finalmente la documentación de las conclusiones de la auditoría.

4.2 Procedimientos para el levantamiento de evidencias

El levantamiento de información depende totalmente de la realidad de la empresa que se esté auditando, de esta manera, el levantamiento de información buscará obtener toda la información necesaria para evaluar los criterios actuales.

De acuerdo a los criterios que hayan sido elegidos para dar inicio a la auditoría, según TIER, COBIT 5.0 o la norma 27002, será necesario evaluar los controles relacionados a ellos y con ello proceder con el levantamiento de información. Para poder realizar el levantamiento de información será necesario.

4.2.1 Determinar los controles existentes

La empresa a auditar cuenta con controles de seguridad física y ambiental establecidos al inicio de su operación o durante el desarrollo de ésta. Los controles fueron establecidos con el fin de colaborar en el cumplimiento de ciertos objetivos de seguridad, sin embargo, se debe poder determinar también, mediante pruebas de ensayo, qué tan eficientes y efectivos está siendo la aplicación de estos controles y conocer con ellos cuáles son las prioridades de la organización respecto a la protección de la información y, también, como conocer cuáles son los puntos que consideran más críticos e importantes entre todos sus procesos.

Luego de la correcta revisión de controles se debe proceder a clasificarlos:

- Controles no existentes: Son aquellos controles cuya necesidad y aplicación es implícita, pero que sin embargo, al analizar los controles existentes no han sido identificados.
- Controles efectivos: Son aquellos controles que según las pruebas de ensayo se han aplicado de forma correcta, impidiendo la aparición de riesgos.
- Controles no efectivos: Son aquellos controles que han sido aplicados, pero que sin embargo no están cumpliendo correctamente su función.
- Controles mejorables: Son aquellos controles que cumplen su función como protectores a riesgos pero que, sin embargo, pueden ser mejorados.

4.2.2 Analizar cada control existente

Luego de haber identificado cuáles son los controles con los que cuenta actualmente el Data Center se debe proceder a analizar cada uno para probar:

4.2.2.1 Controles con un plan de implementación

Los controles deben encontrarse definidos en los documentos de seguridad de información, con las especificaciones exactas de cada una, el riesgo que se está evitando con él y, claro está, el detalle de los pasos que se seguirán para poder implementarlo dentro de la organización.

Este plan de implementación debe indicar de forma detallada cada uno de los pasos que deben realizarse, desde la preparación del ambiente para que se encuentre apto para la aplicación del control, los procedimientos que se seguirán para poder lograr una aplicación correcta y finalmente los mecanismos de supervisión y mejora de estos controles.

4.2.2.2 Plan de mantenimiento preventivo y correctivo

Los controles son planteados de acuerdo a la realidad de la organización, de la misma forma, con el cambio de ésta, los controles también deben cambiar y de acuerdo a los nuevos parámetros adaptarse a la nueva realidad.

Dentro de los mantenimientos que son necesarios realizar para los controles podemos distinguir dos tipos: preventivos y correctivos.

Los mantenimientos preventivos son aquellos que deberán ser planificados y realizados de manera constante y periódica a los controles, con el fin de conocer su estado y poder hacer los cambios y configuraciones necesarias antes de que pueda producirse un problema con el mismo.

Los mantenimientos correctivos son aquellos que tendrán que realizarse una vez detectado que el control no está cumpliendo con los objetivos que tenía establecido, de esta manera, se procederá a realizar las correcciones y a ponerlo nuevamente en funcionamiento.

Es importante recalcar que para poder hacer la detección, a tiempo, de la falla en los controles se deberá contar con un conjunto de planes de pruebas, los cuáles deben estar formados por pruebas simples que permitan la inmediata detención de la inutilidad del control y por pruebas complejas que permitan determinar los puntos internos del control que no están funcionando.

4.2.2.3 Dependencia de un proveedor

Muchos de los controles que la organización establecerá dependerán parcialmente o en su totalidad de elementos o servicios brindados por proveedores. Es por ello que es importante conocer los niveles de servicio que han sido establecidos con los proveedores y verificar que de acuerdo a esos niveles de servicio se han establecido controles eficientes que aseguran un correcto nivel de protección de seguridad física y ambiental.

4.2.3 Analizar la gestión de incidentes y problemas

Un incidente se refiere a alguna interrupción no planeada en un servicio de TI. De la misma forma, también se califica como incidente la reducción de la calidad de un servicio o el fallo de un elemento de configuración que impacta en el funcionamiento del servicio.

La gestión de incidentes tiene como misión restaurar el servicio interrumpido de la manera más rápida posible. Para poder gestionar correctamente se debe contar con un proceso bien establecido, empezando por el registro de las incidencias por parte de los usuarios, la priorización y categorización de la incidencia, la solución y el cierre de la misma.

Por otro lado, un problema es la causa de la ocurrencia frecuente de incidentes sobre el mismo servicio. Normalmente la causa del problema registrado no es conocida y debe ser investigada para proceder con las acciones de corrección. La gestión de problemas busca reducir el impacto y frecuencia en la que ocurren las incidencias que lo generan. Al igual que la gestión de incidentes, la gestión de problemas requiere un proceso bien definido que vaya desde la identificación de la causa del problema, la implementación de la solución y finalmente el seguimiento para comprobar que la solución resolvió de manera correcta el problema.[18]

Por lo anteriormente indicado, un análisis de los incidentes tanto como de los problemas relacionados a los controles de seguridad del Data Center objeto de auditoría, servirá como herramienta de medición de su respectiva efectividad. Así, al analizar tanto frecuencia como impacto en la continuidad de dichos incidentes, se podrá calificar a cada control como:

- Efectivo: El control será efectivo si no es necesario tomar ninguna medida para asegurar que cumpla con su funcionamiento.
- Inefectivo: El control será inefectivo cuando la protección que brinda es mucho menor al objetivo de seguridad que tenía encomendado.
- Con oportunidad de mejora: El control mejorable es aquel que puede ser modificado o implementado de maneras diferentes con el fin de lograr que brinde mayor seguridad. Muchas veces esta mejora estará ligada a otros procesos o servicios de la organización, pero que son necesarios analizar si se quiere lograr la seguridad óptima.

4.2.4 Verificar las auditorías anteriores y documentos relacionados

Como se comentó en apartados anteriores, las auditorías previamente ejecutadas son un punto de partida para los subsiguientes ejercicios de auditoría. Sin embargo, es importante mencionar que los controles que se evaluarán, así como su priorización, dependerán considerablemente de los criterios de la auditoría actual; de allí la necesidad del auditor de seleccionar adecuadamente las auditorías anteriores que le puedan ser útiles para verificar dichos criterios.

[18] [ITGI,2003]

Los informes de auditorías anteriores nos indicarán cuáles fueron los puntos débiles de la organización en ese momento, permitiendo que se preste la atención adecuada en lo que debió ser la implementación de soluciones a esos puntos críticos, siempre y cuando correspondan a los criterios de auditoría actual (posterior).

Al igual que las auditorias previas, la revisión de documentos y regulaciones que la empresa debe cumplir —sea por un acuerdo con el cliente o por normativa del estado— permitirá que se pueda evaluar su cumplimiento y con ello, la obtención de evidencias sobre la realidad actual de la empresa.

Ejemplo:

Analizando los controles existentes, el cliente ha pedido evaluar el control:

TIER I – II: Verificar la utilización de los supresores de incendio más adecuados a la realidad y distribución del Data Center.

Para ello:

1. *Luego de la verificación del control, este ha sido clasificado como "Control no efectivo" ya que, a pesar de encontrarse implementado en el Data Center, por medio de extintores de CO2 distribuidos adecuadamente, no se está considerando la presencia constante de personal de monitoreo del Data Center, los cuales no solo se verían afectados por el incendio que pueda producirse, sino que su vida correrá peligro debido al componente de los extintores, que si bien ayudarán a disuadir el fuego, también reducirán las partículas de Oxígeno de la habitación y con ello podrían producir que las personas se asfixien.*
2. *En las auditorías anteriores no se consideraba este control, debido a que no se contaba con personas encargadas del monitoreo dentro del Data Center; sin embargo, por cambios en los procedimientos y alcances de la empresa, esta necesidad hará que sean tomados de ahora en adelante.*

4.3 Procedimiento de documentación de hallazgos

Como fue indicado capítulos más arriba, un hallazgo es al resultado de la comparación y evaluación de las evidencias contra los criterios que hayan sido determinados de acuerdo a los objetivos de la auditoría, pudiendo así establecer si fue o no conforme con los criterios establecidos.

En este caso, la documentación de hallazgos consistirá en indicar en documentos perdurables, que sirvan de evidencias para el cliente como para el auditor, la realidad encontrada al evaluar la existencia o no de los criterios y el cumplimiento de los objetivos de estos criterios dentro del Data Center, con el objetivo de poseer evidencias que sean útiles para justificar los resultados a los que llegue el auditor y al mismo tiempo para servir de guía de mejora al cliente evaluado.

Los hallazgos encontrados durante la auditoría podrán ser clasificados, en tres grupos diferentes, de acuerdo al cumplimiento del criterio relacionado a la evaluación y a las características de este criterio con respecto a la realidad (auditada). Estos tres grupos serán:

1. No hay hallazgo: Este escenario surge cuando el cumplimiento del criterio relacionado es del 100%, es decir:
   a. Existe un control para el criterio del aspecto auditado en el Data Center, existiendo además la evidencia sustentatoria correspondiente.
   b. Adicionalmente la disponibilidad del control es la adecuada.
   c. Está dimensionado infraestructuralmente de forma correcta, contando con el número suficiente y necesario de componentes tecnológicos de apoyo.
2. No conformidad: Un hallazgo será clasificado como una no conformidad[19] cuando el criterio evaluado no ha sido cumplido en su totalidad.
3. Insuficiente: Un hallazgo será clasificado como insuficiente cuando existe un control relacionado a un criterio específico, pero sin embargo

[19] [ISO, 2002]

a. El control carece de eficiencia o disponibilidad a un nivel menor que podría afectar la continuidad del negocio del poseedor del Data Center.
b. No está dimensionado infraestructuralmente de forma correcta, en el número suficiente y necesario.

Una vez clasificados los hallazgos en los tres grupos, será necesario clasificar la evidencia que se encuentre en los grupos “No conformidad” e “Insuficiente” de acuerdo a la criticidad, para demostrar la importancia del levantamiento de los hallazgos correspondientes. Como parte de la tabulación de los hallazgos, se podrá proceder al detalle de éstos indicando las diferencias existentes entre el criterio y las evidencias que los generaron.

El documento de hallazgos será la guía que permita al cliente identificar las desviaciones de los objetivos de control que inicialmente estableció y por otro lado, planificar las actividades de carácter correctivo que se consideren convenientes para subsanarlas.

Ejemplo:

Criterio: Según TIER I – II. Verificar la utilización de los supresores de incendio más adecuados a la realidad y distribución del Data Center.

Evidencia: Se cuenta con un sistema de supresión de incendios basado en extintores de CO2 distribuidos en la totalidad del área del Centro de cómputo, con cantidad suficiente y adecuada para disuadir un incendio de magnitud mediana. El personal que se encuentra constantemente dentro del centro de cómputo, realizando las labores de monitoreo y control no cuentan con mecanismos de protección a los gases que emiten los extintores, poniendo en peligro su vida.

Hallazgo: Se cuenta con el mecanismo de supresión de incendios; sin embargo, este no tiene la implementación adecuada del control de acuerdo a la realidad del Data Center auditado, debido a que no cuenta con un mecanismo que proteja la vida de las personas que laboran en la zona crítica.

Ante esta situación clasificaremos el hallazgo como “No conformidad” debido a que el control se encuentra implementado, sin embargo no en su totalidad, ya que no cubre el aspecto de protección a la vida.

Con esta clasificación procedemos a determinar la criticidad, que en este caso será Alta debido a que la vida del personal podría estar corriendo peligro.

4.4 Procedimiento para la documentación de las conclusiones y recomendaciones

Luego de establecer los objetivos de la auditoría y haber evaluado la realidad física y medio ambiental del Data Center de acuerdo a un conjunto de criterios fijados a partir de la aplicación de normas y estándares internacionales de seguridad de información (TIER, ISO, COBIT), se da por concluido el proceso de evaluación también conocido como auditoría de campo. Sin embargo, queda aún pendiente uno de los aspectos más importantes del proceso de auditoría: la documentación de conclusiones y recomendaciones.

Las conclusiones representan el resultado de la evaluación realizada; sin embargo, éstas deben poseer el detalle adecuado para servir como guía al cliente, de los controles pendientes de mejora en el Data Center.

Los hallazgos son la base del detalle de estas conclusiones. De acuerdo al grupo al que hayan pertenecido —según la clasificación mencionada en el apartado anterior— se deberá enunciar cada conclusión de acuerdo al siguiente tenor:

- El criterio sí se cumple: En este caso, no existe diferencia entre el criterio y la evidencia encontrada, por lo cual se deberá indicar comparativamente:
  - Norma o estándar internacional (apartado en particular de alguna de ellas) involucrado en el criterio.
  - El criterio mismo.
  - Y el control que está cumpliendo —en la realidad del Data Center— tanto con la norma como con el criterio de la auditoría.
- El criterio no se cumple: En el caso de los criterios que no son cumplidos, se deberá clasificar el impacto de cada uno los hallazgos distinguiendo aquellos que corresponden a la seguridad física y aquellos que lo hacen para seguridad medio ambiental.

- El criterio es insuficiente: Al igual que en el caso de criterios no cumplidos, se deberá clasificar cada hallazgo de acuerdo al impacto que tenga en la seguridad, indicando los motivos por los cuáles no ha sido cumplido.

Este detalle servirá como guía para el cliente, permitiéndole conocer los puntos que se han auditado y el nivel de cumplimiento que el Data Center evaluado tiene con respecto a los criterios seleccionados.

Por otro lado, así como se debe documentar las conclusiones, una de las labores de la auditoría es brindar al cliente las recomendaciones adecuadas que le permitan solucionar los problemas encontrados.

El primer punto a tratarse como recomendación será el conjunto de planes necesarios para la implementación de los controles con los que no se cuenta; de esta manera se podrá llenar los vacíos de seguridad física y medio ambiental para el Data Center, asegurando un mejor desempeño y mayor continuidad. Igualmente, será necesario recomendar el conjunto de planes para mejorar aquellos controles que han sido clasificados como insuficientes, permitiendo que —una vez aplicada la mejora— pueda cumplir de manera eficiente su objetivo.

Conociendo lo necesario para brindar una recomendación que pueda ser útil para el cliente, se deberá proceder al detalle de los planes mencionados siguiendo una estructura que facilite el entendimiento y reconocimiento tanto de los objetivos del plan y las pautas de implementación por ejecutarse.

La estructura para proceder al detalle de los planes de implementación es:

- Objetivo general: En este punto se busca explicar de manera amplia, pero clara, al cliente lo que se logrará una vez cubierto este control.
- Objetivos específicos: Se al detalle de los riesgos que podrán ser cubiertos una vez implementado el control.
- Resultados esperados: Es el conjunto de documentos que podrán obtener con la implantación del control, sea documentación importante para la empresa, como manuales para la mejora y control continuo.
- Alcance y limitaciones: En este punto del documento será necesario detallar los activos que involucrará el establecimiento de los nuevos controles a implantarse

o los controles a mejorarse, si serán o no tercerizados, los elementos que implica el monitoreo, entre otros.

- Calendarización: Será necesaria la presentación de un Gantt en el cuál se detalle los pasos necesarios para poder implementar correctamente el control, empezando por el acondicionamiento necesario para la implantación, la implantación en sí y el monitoreo inicial y continuo.

Una vez detallados esos puntos el cliente será capaz de conocer los pasos necesarios para implantar o mejorar los controles que han sido detectados como ausentes o defectuosos por la auditoría y con ello tendrá una mejor visión del balance inversión/ventajas que se obtendrán.

Ejemplo:

Conclusión 1: La vida del personal que trabaja en el Data Center es uno de los aspectos que abarca el cumplimiento de la normativa relacionada con la seguridad física y medio ambiental. De acuerdo a lo examinado, se cuenta con los mecanismos de protección contra incendios que asegurarán la protección de los equipos; sin embargo no se está considerando la salud del personal que se encuentra dentro del centro de cómputo, poniendo en riesgo su integridad y la del área. Con estos datos, ´podemos concluir que hace falta realizar un análisis de las necesidades que se tienen considerando que la realidad actual de la empresa tiene diferencias notables con respecto a aquella en la cual se está trabajando ahora.

En la actualidad, han surgido una gran variedad de tecnologías que permiten el control de los incendios, como por ejemplo los sistemas FM-200TM los cuales no solo son muy eficientes para la supresión de incendios, sino que además permite apagar el incendio protegiendo la salud del empleado que labora en dicho ambiente. De la misma forma, la tecnología de pintura anti incendios permite que una vez detectado el incendio, la pintura emane partículas que permitirán controlar el incendio.

CAPÍTULO 5: PRUEBA DE LOS PROCESOS

5.1 Introducción

En el presente capítulo se documentará la aplicación de los procedimientos descritos en los capítulos anteriores, generando pruebas de la utilidad y veracidad en la utilización de los mismos.

Las pruebas se realizarán en una empresa del estado, cuyo objetivo es la evaluación del Data Center con el que cuentan actualmente para evaluar que tan óptimos son los controles de seguridad física y ambiental con.

5.2 Alcance de las pruebas

Las pruebas realizadas se desarrollan evaluando la seguridad física y medio ambiental que posee el Data Center, teniendo como guía para el análisis:

- La clasificación y estándar internacional TIER
- Marco de control COBIT 5
- La ISO/IEC 27002 de Seguridad de Información

De la misma forma, es importante aclarar que para materias del presente análisis no se ha considerado la realización del análisis de SW de los CCTV.

5.3 Objetivos de las pruebas

El objetivo de las pruebas realizadas es el análisis de la infraestructura actual del Data Center para evaluar la idoneidad de la seguridad física y ambiental en él.

5.4 Ejecución de la auditoría de prueba

5.4.1 Seguridad perimetral

5.4.1.1 Objetivo

Revisión de las instalaciones físicas para verificar la existencia de controles de acceso perimetral al área donde se ubica el Data Center.

5.4.1.2 Criterios

Los criterios a evaluarse son:

- COBIT 5
  - APO01.02, APO12.05, APO13.01: Verificar si se cuenta con un plan de seguridad física y ambiental establecido, comunicado y conocido a través de la empresa.
  - DSS05.05: Verificar la existencia de mecanismos de autorización y restricción de acceso a los locales del Data Center.
  - DSS05.07: Verificar la existencia de herramientas de detección de intrusos para controlar el acceso no autorizado al Data Center.
- ISO27001
  - 9.1.1: Verificar la existencia de barreras físicas que dificulten el acceso al edificio del Data Center.
  - 9.1.1: Verificar la existencia de mecanismos de contingencia cuando la barrera física principal no funcione.
  - 9.1.3: Verificar la existencia de un circuito de cámaras de seguridad que se encuentren monitoreadas 24/7.
  - 9.1.4: Verificar la existencia de puertas y ventanas con marcos adecuado para evitar forcejeos y lunas con sistema de resistencia a rupturas.
  - 9.1.4: Verificar mecanismos adecuados de articulación de puertas y ventanas
  - 9.1.4: Verificar la existencia de sensores de ruptura de vidrios para emitir alarmas que permitan detectar el motivo de la ruptura y actuar de acuerdo a la situación.
- TIER
  - I-II: Verificar la existencia de mecanismos de control de acceso al centro de datos por medio de controles eléctrico o biométricos

- I-II: Verificar que dentro de la sala principal del Data Center no existan ventanas ni otros mecanismos de acceso diferentes al de la puerta con controles.

5.4.1.3 Evidencias

Se realizó una visita ocular al local actual en el cual se encuentra ubicado el Data Center. El objetivo de esta visita es poder comprobar cuál es el estado actual de los controles perimetrales de la zona.

A continuación se presenta la descripción de la realidad actual de algunos de los aspectos básicos del Data Center.

Ingreso al Data Center

En la zona de ingreso al Data Center podemos observar que se cuenta con puerta y marcos de madera delgada, pintados de color verde (color característico de la institución).

La puerta anteriormente descrita cuenta con una chapa simple en forma de perilla y sin ninguna protección adicional que se encuentre visible. Al costado izquierdo de la puerta, podemos observar la presencia de una ventana corrediza con un sistema simple de apertura (seguro en la parte superior), la cual se encuentra rota, permitiendo la visibilidad de los elementos contenidos dentro del Data Center así como la facilidad para acceder a la manija de la puerta y el seguro de la misma ventana.

Una vez en el interior de la facilidad, la mampara que alberga a los servidores en uso puede ser apreciada en la siguiente foto:

Sala de Servidores

Una vez en el interior de la facilidad, la mampara que alberga en su interior a los servidores es de vidrio con aluminio y contiene pegado en el vidrio la señalética de acceso restringido

Al lado de la mampara podemos observar sillas que llevan encima teclados y pantallas que al parecer no son utilizados. De la misma forma, podemos observar que alrededor de la puerta se encuentran CPU's desconectados y apilados que parecen en desuso. El piso es de lozas blancas y de material cerámico.

En la parte interna de la Sala de Servidores, en la pared izquierda se observa una ventana corrediza a pocos centímetros del techo de la facilidad. Esta ventana no cuenta con medidas de seguridad para su apertura.

5.4.1.4 Hallazgos

A partir de la inspección visual se puede indicar lo siguiente:

1. El Data Center se encuentra ubicado en las mismas instalaciones en las cuáles se encuentran las oficinas administrativas de la empresa. De acuerdo al estándar TIER y las buenas prácticas de seguridad, el Data Center principal, así como el centro alterno deben estar ubicados a un rango mínimo de 4Km a los alrededores de las oficinas principales.
2. De acuerdo a las descripciones anteriormente mostradas, el acceso a la locación no tiene las características adecuadas para un Data Center, las características mostradas son las de puertas típicas de una puerta común de madera o tripley.
3. Junto a la puerta de acceso está dispuesta una ventana corrediza, la cual se encuentra rota formando una ranura que facilita el acceso al interior del Data Center.
4. La cerradura y chapa de la entrada principal tienen características de cerraduras de puertas típicas de interiores de casas u oficinas, sin ningún mecanismo particular de seguridad.
5. El ingreso a la sala de servidores es a través de una mampara corrediza de aluminio con vidrio y con una cerradura convencional. No existe ningún mecanismo de control de acceso físico.

A continuación se muestra una tabla con el detalle de las vulnerabilidades que han sido halladas y las respectivas amenazas y riesgos que conlleva el no corregir las mismas.

Aspecto	Vulnerabilidad	Amenaza	Riesgo	Impacto
Seguridad perimetral	Material de la puerta de ingreso principal	Personas no autorizadas tienen acceso a los activos de información.	Acceso no autorizado y pérdida o daño total o parcial de activos de información	Medio - Alto
	Cerradura de la puerta de ingreso principal			
	Ruptura de la ventana contigua a la puerta principal			
	Material de la puerta de ingreso a la sala de servidores			
	Ventana no clausurada en la parte trasera, a espaldas de los servidores			

Tabla 2: Análisis de riesgos – Seguridad perimetral.

5.4.2 Disposición de equipos

5.4.2.1 Objetivo

Verificar la existencia de controles que permitan que la infraestructura del Data Center cuente con los elementos necesarios que aseguren su disponibilidad constante y que los equipos se encuentren adecuadamente ubicados y ordenados.

5.4.2.2 Criterios

Los criterios son:

- COBIT 5
  - APO03.01: Verificar la correcta definición de objetivos de la seguridad de información para el funcionamiento del Data Center.
  - APO13.02: Verificar la existencia de un inventario de los dispositivos con los que se cuenta.
  - BAI03: Verificar la existencia de soluciones de seguridad que sean probados y aprobados.
  - BAI06.02: Verificar la existencia de medidas que controles el mantenimiento de los equipos sin comprometer la seguridad de información.
  - DSS05.06: Verificar la existencia de garantías que aseguren y protejan la seguridad física y ambiental del Data Center.

- ISO27001
  - 9.1.3: Verificar la existencia de un inventario de cuartos del Data Center y el contenido de cada uno de ellos.
  - 9.2.3: Verificar una administración adecuada de cables que permita el cambio o movilización de los mismos de forma ordenada y sencilla.
  - 9.2.3: Verificar la utilización de canaletas adecuadas que protejan y organicen el recorrido de los cables.
- TIER:
  - I-II: Verificar una adecuada distribución del cableado eléctrico y de red dentro del Data Center.
  - I-II: Verificar que los cables se encuentren adecuadamente etiquetados para facilitar la manipulación y cambio de los mismos.
  - I-II: Verificar el nivel de interferencia y ruido que se producen entre los diferentes cables con los que cuenta el Data Center.

5.4.2.3 Evidencias

A continuación se detallan las características observadas al ingresar a la Sala de Servidores

Racks

Los racks observados contienen los servidores del Data Center, los cuales no se encuentran colocados correctamente generando riesgo de caídas o golpes. Igualmente, los racks no se encuentran dispuestos de forma adecuada en el área total de la sala de servidores, dificultando el control de temperatura y ventilación de la misma.
Se observa una gran cantidad de polvo y suciedad en el interior de los racks y sobre los servidores, lo cual evidencia una falta de cuidado y limpieza en la zona.

Cableado

No existe un orden que permita hacer el seguimiento visual de un extremo a otro del cable y éstos se encuentran sucios y maltratados. Igualmente, pude observar que los cables de datos y los cables eléctricos transitan por la misma zona sin ninguna medida de cuidado y sin un mantenimiento adecuado ya que se encuentran en mal estado (sucios y rotos).

Falso piso y cielo raso

No se observa la construcción de un falso piso y falso techo que proteja los equipos.

Conexiones eléctricas

Se cuenta con conectores eléctricos simples, sin supresor de picos ni ningún mecanismo de regulación de energía.

Los conectores se encuentran ubicados a menos de un metro de distancia del suelo y el cableado del mismo va al ras del suelo.

Otros

Las pantallas y teclados de control de los servidores se encuentran a disposición de las personas que ingresen. No cuentan con protección de acceso a ellos.

Se observa la presencia de una escalera en la mitad del Centro de Datos. De la misma forma, se presentan mochilas y bolsas en el interior de la Sala de Servidores.

Adicionalmente a los puntos anteriormente descritos, se analizó la capacidad de los equipos de electricidad con los que cuenta el Data Center, obteniendo como resultado que éstos no cuentan con la potencia necesaria para soportar los equipos del mismo.

5.4.2.4 Hallazgos

A partir de la evidencia que se ha documentado mediante fotografías, podemos indicar que:

1. El cableado está siendo remodelado pero, como se puede apreciar, no guarda una disposición ordenada por la parte de atrás de cada uno de los racks que contienen los servidores. Situación que repite por el techo y por el piso.
2. No se cuenta con canaletas que permitan el flujo adecuados de los cables, permitiendo ordenar la distribución de éstos y protegiéndolos.
3. Los cables no se encuentran etiquetados, haciendo más complicada la manipulación y cambio de los mismos.

4. Los cables de energía y los de datos se encuentran mezclados unos con otros, pudiendo producirse interferencia entre la comunicación y cortos circuitos.
5. Las tomas eléctricas no se encuentran protegidas por ningún mecanismo que evite problemas de cortos circuitos por sobrecargas o inundaciones.
6. Como se puede observar en la imagen superior, existe una escalera que apoyada a la pared de esa zona apuntando hacia un falso techo inexistente.
7. No se observa la presencia de infraestructura de falso piso y falso techo.

Luego de determinar la realidad del Data Center se obtiene como el conjunto de vulnerabilidades detalladas a continuación.

Aspecto	Vulnerabilidad	Amenaza	Riesgo	Impacto
Disposición de equipos	Sistema de falso techo inexistente	Daño físico de los equipos	Pérdida de la continuidad de negocios (y de TI)	Alto
	Sistema de falso piso inexistente			
	Cableado carente de orden y señalización.			
	Cableado eléctrico y de datos no distinguidos.			
	Cableado no protegido.			
	Tomas eléctricas sin protección.			
	Suciedad en los equipos electrónicos			
	Capacidad de los equipos UPS (de Uninterruptible Power Supply)	No contar con suficiente potencia eléctrica más que para poder apagar correctamente los equipos	Ante la ausencia de grupos electrógenos como controles compensatorios, Pérdida de la continuidad de negocios (y de TI)	Alto

Tabla 3: Análisis de riesgos - Disposición de equipos.

5.4.3 Seguridad ambiental

5.4.3.1 Objetivo

Verificar la existencia de controles de seguridad ambiental en el Data Center, con el fin de prevenir desastres medio ambientales que pudieran ocurrir.

5.4.3.2 Criterios

Los criterios son:

- COBIT 5
  - DSS01.04: Verificar el cumplimiento de requisitos de gestión ambiental.

- ISO27001
  - 9.1.3: Verificar el nivel de protección de los equipos de aire acondicionado.
  - 9.1.3: Verificar el nivel de protección de los sensores de humedad y humo.
  - 9.1.4: Verificar la existencia de un centro de control de sensores que sea constantemente monitoreado.
  - 9.1.4: Verificar la existencia de sensores de humedad que emitan alertas cuando el nivel ascienda o descienda considerablemente para producir daño a los equipos.
  - 9.1.4: Verificar la existencia de un sistema de ventilación adecuado de acuerdo al tamaño, capacidad y distribución de las habitaciones del Data Center.
  - 9.1.4: Verificar la existencia de sensores de aniego que emitan alarmas cuando se detecta la presencia de agua en el cuarto del Data Center.
  - 9.1.4: Verificar la existencia de mecanismos de desfogue de agua para poder eliminar de la manera más rápida posible las consecuencias que podría producir una inundación.
  - 9.1.4: Verificar la existencia de sensores de humo que emitan alarmas con la mínima presencia de humo.
  - 9.1.4: Verificar la existencia y utilización de extintores y sistemas de supresión de incendios.
  - 9.1.4: Verificar la correcta selección de extintores y supresores de incendios de acuerdo a la realidad del Data Center.
- TIER
  - I-II: Verificar la existencia de fuentes redundantes de enfriamiento y reserva de energía.
  - I-II: Verificar la existencia de un panel de alarmas que permita mantener supervisados los sensores y alarmas del Data Center, evitando que se produzcan activaciones innecesarias.
  - I-II: Verificar la existencia de alarmas de aniego enlazadas con mecanismos de desfogue de agua.
  - I-II: Verificar la instalación adecuada de los equipo de acuerdo a los niveles de enfriamiento existentes en las salas.
  - I-II: Verificar que no se cuente con material inflamable dentro de la sala principal del Data Center.

5.4.3.3 Evidencias

Durante la visita no se encontró evidencia de existencia de sensores de humo, humedad y aniego. El único mecanismo con el que se cuenta es de extintores de CO2 fuera de la sala de servidores.

No existe un control o sensor de polvo que prevenga la cantidad de éste en el interior de la sala y en los alrededores de los equipos.

Para el caso de inundaciones, no se halló evidencia de un sistema de desfogue de agua ni de protección de los equipos electrónicos frente a este factor ambiental.

5.4.3.4 Hallazgos

De acuerdo a la ausencia de controles y mecanismos de protección que se han indicado en las evidencias, los hallazgos son:

1. Los equipos se encuentran rodeados de polvo.
2. Existen extintores manuales de incendio a la entrada de la sala de servidores y al exterior.
3. No se identificaron mayores controles ambientales.

Con estos se realizó el análisis de vulnerabilidades obteniendo:

Aspecto	Vulnerabilidad	Amenaza	Riesgo	Impacto
Seguridad ambiental	Suciedad en los equipos electrónicos	Daño físico de los equipos	Pérdia de la continuidad de negocios (y de TI)	Alto
	Ausencia de instalaciones de aire acondicionado adecuadas.			
	Ausencia de detectores de humo al interior de la sala de servidores.			
	Ausencia de detectores de humedad al interior de la sala de servidores.			
	Ausencia de detectores de aniego al interior de la sala de servidores.			
	Ausencia de sistema de desfogue de agua.			

Tabla 4: Análisis de riesgos - Seguridad Ambiental.

5.5 Conclusiones y recomendaciones

De acuerdo a las evidencias y hallazgos que se han obtenido en la realización de las pruebas, se ha presentado el análisis de los riesgos a los que se está expuesto

debido a las falencias de seguridad física y ambiental. No se cuenta con mecanismos de seguridad de accesos ni con sensores que aseguren que el Data Center pueda funcionar de manera continua frente a eventos ambientales inesperados y frente a personas malintencionadas.

De acuerdo a las condiciones actuales del Data Center, y considerando que el objetivo es lograr que el Data Center cumpla con su función como tal y se asegure su disponibilidad 24/7, se presentan dos alternativas que el cliente podría considerar:

Alternativa 1: adquirir equipos y construir un nuevo Data Center para que soporte los servicios.

Esta alternativa incluye:

- Implementación de una nueva infraestructura civil para albergar al Data Center considerando buenas prácticas internacionales relativas a la construcción. En lo referente a las características en la escala de Tiers, podría considerarse una calificación igual a Tier II.
- Adquirir los equipos suficientes y necesarios para dar soporte a los servicios críticos.

Para la actividad relacionada con la implementación de una nueva infraestructura civil, se deben considerar ciertos aspectos que podrían influir considerablemente en los costos de esta alternativa.

A continuación se presentan los aspectos necesarios a considerar:

1) Características básicas sobre la ubicación del Local: De acuerdo a las buenas practicas que se indican para las instalaciones del tipo Data Center, se deben incluir en él las áreas que fueron explicadas en este mismo documento en capítulos anteriores, como son:
    - Área de Distribución Principal (MDA)
    - Área de Distribución Horizontal (HDA)
    - Sala de Almacenamiento
    - Sala de eléctrica/mecánica
    - Sala de telecomunicaciones

- Centro de operaciones
- Sala de entrada
- Área de distribución de los equipos (EDA)
- Sala de cómputo
- Área de distribución zonal (ZDA)

De la misma forma, relacionada a la ubicación del Data Center éste debe estar convenientemente resguardado y su identificación no debe ser obvia desde el exterior, siendo necesaria una señalización adecuada en la parte interna que permita su reconocimiento por parte del personal autorizado. De la misma forma, se debe asegurar que se encuentre alejado de fuentes de vibración por su cercanía a pistas o calles.

2) Equipos de alojamiento – Racks: Los componentes de alojamiento deben cumplir por lo menos con las siguientes especificaciones:

Componente Alojamiento	Full Rack compartido de 19'' con llaves individuales
Cantidad	Depende de los servidores por alojar
Disponibilidad de acceso	7 días por 24 horas (aunque depende del horario del cliente) Se extiende a la modalidad 24/7/365 sobre todo para casos de desastre.
Altura	42 U/R (Unidades de rack) Altura máxima 2.4m, preferiblemente 2.1m
Ancho	Rango [450mm, 600 mm]
Profundidad	Rango [0.9 m, 1.1 m.]
Toma de Corrientes	Series de conectores hembra multipropósito pertenece a un circuito independiente conectados a tableros eléctricos diferentes
Regletas	Al menos una de 20Amp/120V
Sistemas de soporte de tecnología	Suficiente tiempo de respaldo para que se encienda el generador que brinde respaldo entre 5 a 30 minutos (en baterías). El cuarto de UPS y Baterías debe contar con un aire acondicionado de precisión (PAC)

Tabla 5: Requerimiento mínimo de los equipos racks.

3) Aspectos de seguridad física y ambiental: Es necesario establecer un conjunto mínimo de normas de control físico y ambiental en el interior y exterior del Data Center, que aseguren que el acceso a la locación como a los equipos sea restringido únicamente para personal autorizado y que a su vez proteja éstos de peligros ambientales como son la humedad, temperatura, presencia de polvo, etc.

A continuación se muestra un cuadro resumen de los principales aspectos de seguridad física y ambiental que deben considerarse:

Seguridad ambiental	Seguridad de acceso físico
Equipo de aire acondicionado para el control de la temperatura y humedad relativa, dependiendo de la cantidad de equipos por alojarse en la facilidad.	Contar con un sistema de control de ingreso al Data Center mediante un mecanismo que responda a las políticas de seguridad del cliente.
Suministro de fluido eléctrico de respaldo ante un corte del mismo mediante el uso grupos electrógenos.	Presencia de puertas de acceso que se mantienen cerradas en todo momento. Debe poder demostrarse que dichas puertas son capaces de soportar ataque físico.
Equipos UPS con una capacidad instalada que permite la autonomía necesaria hasta el encendido del grupo electrógeno.	Mantener un registro detallado de acceso al Data Center por personal autorizado.
Deben documentarse claramente los procedimientos de salida en caso de emergencia, que incluyan su distribución entre todo el personal involucrado.	Contar con un mecanismo de vigilancia permanente —normalmente con la presencia de cámaras de video o CCTV—en las áreas de acceso al Data Center.
Sistema de detección y extinción de incendios FM 200 en caso la facilidad aloje 10 a más componentes de alojamiento o racks.	Dispositivos de control de acceso (biométricos, digitales, etc.) con registros de todos los accesos (positivos y fallidos). Deben documentarse los procedimientos de asignación de tarjetas de identidad, llaves tipo tokens, contraseñas y demás para uso permanente y temporal (visitas, proveedores, entes reguladores, clientes, etc.); igualmente, debe documentarse el proceso de visitas.
Sensores de aniego para la detección temprana de inundaciones.	
Sensores de humo, polvo y aumento de temperatura si las condiciones de los dispositivos de alojamiento de servidores lo requiera.	

Tabla 6: Tabla resumen de los controles físicos y ambientales recomendados

4) Acondicionamiento de la infraestructura civil: Algunos de los trabajos que será necesario realizar son:
   - Suministro y pintado con pintura anti fuego de preferencia importado y acabado a 2 manos, comúnmente en color blanco.
   - Suministro e instalación de baldosas como piso técnico del Data Center.
- Cableado con materiales y accesorios completos para el aterramiento del piso técnico nuevo con conductores fijados a los parantes.

5) Piso técnico: Algunos detalles que serán necesarios para el piso técnico son:

- La altura del piso técnico no debe ser menor de 28cm y se debe realizar una nivelación del piso para evitar la acumulación de polvo que pueda perjudicar el funcionamiento de los equipos.
- La resistencia mínima de la baldosa debe ser de 2 000 Kg/m2 (carga uniforme) y 450 Kg/500mm (carga concentrada).
- Resistencia eléctrica de 1 x 100 000 Ω según norma NFPA 99 cap. 3.
- Deben contar con aislamiento térmico y eléctrico.
- Se instalará rejillas metálicas de ventilación o baldosas con perforaciones lo que permitirá un flujo de aire adecuado de acuerdo al concepto de pasillos calientes y pasillo fríos.
- Se realizará las perforaciones necesarias para el ingreso de cables del cableado estructurado y cableado eléctrico a instalarse, buscando no dañar dichos cables.
- Se debe considerar una ventosa doble para manipulación de las baldosas del piso técnico.

6) Suministro y montaje de aire acondicionado: Los trabajos a realizarse en este punto son:
   - Suministro e instalación del sistema de alimentación eléctrico para la unidad de aire acondicionado.
   - Suministro e instalación del sistema de alimentación de agua para el aire.
   - Montaje de unidad de aire acondicionado.
   - Instalación de sistema y panel de control y mando.

7) Instalación de cableado estructurado: Todos los elementos del cableado estructurado deben garantizar la compatibilidad entre ellos, para lo cual será necesario que todos sean de la misma tecnología.

   El diseño que se realice dependerá de la cantidad máxima de gabinetes que se tendrá, dato que será brindado por el cliente y considerado en el diseño la ventilación adecuada de los equipos.

   El diseño debe considerar:
   - Garantizar el flujo del aire por debajo del piso técnico, considerando el criterio de pasillos calientes y fríos.

- Fácil acceso a los gabinetes para futuras instalaciones y/o mantenimientos.
- Pasillos libres para el tránsito del personal, ingreso y/o retiro de equipamiento.
- Distribución adecuada del sistema de cableado estructurado y su canalización.
- Todos los bienes materiales instalados serán nuevos y de primer uso, de reconocida calidad y vigencia, tanto en el mercado nacional como internacional y compatibles a los pre existentes donde se requiera.

8) Controles de temperatura: La nueva infraestructura debe contar con controles de protección contra incendios, garantizando que la edificación cuente con mecanismos que eviten el sobrecalentamiento de los equipos y los ambientes. Como parte de los controles de este tipo debe considerarse:
   - Ausencia de equipos tales como cafeteras, calentadores, etc.
   - Señalética adecuada para indicar la imposibilidad de hacer fuego dentro de las locaciones.
   - El suministro de papel en el aula de informática debe estar en armarios de metal.
   - Debe contarse con detectores de humo, fuego y/o polvo claramente identificados en zonas estratégicas. Esta información debe ser visible a través de planos.
   - Las alarmas de sonido deben estar conectadas a la consola de seguridad integral y/o la central de monitoreo.
   - Los extintores deben ser fácilmente accesibles, bien marcados y convenientemente probados por los proveedores en un lapso semestral.
   - El personal debe recibir capacitación anual en los pasos a seguir en caso de incendio, la formación debe cumplir con los requisitos del código local y los registros deben mantenerse.

9) Controles de aniego: Estos controles tienen por finalidad la protección contra el daño del agua asociado con la liberación accidental de agua en un centro de cómputo. Se debe contar con mecanismos de detección de fugas y filtraciones de agua así como los mecanismos para contrarrestarlos.

10) Controles de suministro eléctrico: Estos controles buscan la protección ante cualquier interrupción del suministro normal de energía. Debe existir documentación explicativa de la manera en que el flujo se despliega a través del Data Center y todos los suministros de energía de respaldo disponibles en caso de fallo de alimentación.

    Se debe tener claramente documentado el programa de mantenimiento preventivo de los generadores y los sistemas de UPS, documentando las tareas de mantenimiento preventivo hecho por los proveedores respectivos. De la misma forma, se deben contar con procedimientos escritos para cambiar al modo de energía de respaldo, debiendo estar todo el personal entrenado para ejecutar tales procedimientos.

Alternativa 2: Tercerizar todos los servicios (críticos y no críticos) de tal forma que un proveedor externo atienda el Data Center.

Para esta alternativa se deben contemplar los mismos aspectos que en el caso de la alternativa anterior, considerando las recomendaciones como exigencias que se le deben imponer al proveedor

En función a la clasificación TIER se deberá solicitar como mínimo la clasificación TIER II, garantizando la continuidad del servicio.

Adicionalmente, es necesario exigir al proveedor: Contar con infraestructura de clase mundial.

- Contar con infraestructura de clase mundial.
- Tener experiencia en soluciones de housing / hosting de aplicaciones y la provisión de los servicios relacionados.
- Disponibilidad de acuerdo a las necesidades del cliente, que en este caso sería de 24/7.
- Contar con profesionales altamente experimentados y especializados.

Es importante aclarar que se deberá exigir al proveedor que brinde las facilidades para la realización de auditorías contratadas por el cliente y que le aseguren al cliente que se está cumpliendo con lo establecido en el contrato.

CAPÍTULO 6: CONCLUSIONES Y RECOMENDACIONES

6.1 Introducción

En el presente capítulo, se detallarán las conclusiones y recomendaciones a las que se ha podido llegar luego de la aplicación, paso por paso, de los procedimientos que se detallan en este documento.

6.2 Conclusiones

Los procedimientos detallados en este documento tienen como fin guiar los pasos que un auditor debe realizar para lograr un resultado adecuado en una auditoría física y medio ambiental de un Data Center.

Una vez realizadas las pruebas y con los resultados que se indican en el apartado anterior podemos concluir que los procedimientos han podido ser correctamente aplicados en la auditoría a un Data Center real, permitiendo obtener los resultados adecuados que demuestren la efectividad o deficiencia de los controles que se hayan implantado y que perjudican la seguridad y continuidad de operación.

De la misma forma, se ha podido comprobar que estos mismos procedimientos pueden ser extensibles a nivel de otros marcos y normas como, por ejemplo, la ISO 27001 de seguridad de información, permitiendo ampliar la gama de criterios posibles de auditar.

Finalmente, se puede concluir que el presente proyecto ha sido exitoso debido al conocimiento que se ha adquirido durante el período de enseñanza universitaria que se ha cursado hasta el momento, permitiendo profundizar temas relacionados a las tecnologías y seguridad de información.

6.3 Recomendaciones

Se recomienda que pueda complementarse el presente proyecto profundizando en temas directamente relacionados a él como son la auditoría de desastres naturales en un Data Center, sobre todo considerando la ubicación geográfica de nuestro país y todos los desastres que podrían azotarnos en cualquier momento.

De la misma forma, los mecanismos de continuidad de negocio y la auditoría de accesos lógicos podrían complementar este proyecto y lograr un nivel de seguridad mucho mayor.

REFERENCIAS

ADC TELECOMMUNICATION

2005 *Cómo diseñar un centro de datos óptimo.* Minnesota, USA

2006 TIA-942. Minnesota, USA

COX, Barry

2003 *Auditing your Data Center Access Control System: An independent Auditors Perspective*. EE.UU.

DELOITTE GLOBAL SERVICES LIMITED

2011 *Gobierno de TI.* UK. Consulta: 05 de abril del 2012 <http://www.deloitte.com/view/es_PE/pe/servicios/consultoria/tecnologia de-la-informacion/gobierno-de-ti/index.htm>

DIRECCIÓN GENERAL DE ELECTRICIDAD DEL MINISTERIO DE ENERGÍA Y MINAS

2009 *Ley de concesiones eléctricas y reglamento. Decreto Ley N° 25844, Decreto Supremo N°009-93-EM*. Lima, Perú.

GREMBERGEN, Win Van; DE HAES, Steven.

2010 *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value.* NY, USA. Springer Science + Business Media.

IBM International Technical Support Organization – Redbooks

2010 *IBM b-type Data Center Networking: Design and Best Practices Introduction.* Second Edition. USA

2011 *IBM Data Center Networking: Planning for Virtualization and Cloud Computing.* First Edition. USA

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

2012 *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*. Illinois, USA

2012 *COBIT 5.0 for Information Security.* Illinois, USA

INTERNATIONAL STANDART ORGANIZATION

2002 *ISO/IEC 19011:2002 Guidelines for quality and/or environmental management systems auditing.* EE.UU.

2005a *ISO/IEC 27002:2005 Information technology - Security techniques – Code of practice for information security management*. EE.UU.

2005b *ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements.* EE.UU.

2011a *ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for information security management systems auditing*. EE.UU.

2011b *ISO/IEC 27007:2011 Information technology – Security techniques – Guidelines for auditors on security controls*. EE.UU.

IT GOVERNANCE INSTITUTE

2003 *Board Briefing on IT Governance*. Illinois, USA

LEGISLATIVE AUDIT DIVISION

2006 *Data Center Review.* Montana, USA.

NETWORK SYSTEM ARCHITECTS, INC.

2003 *Planning a Data Center*. Denver. EE.UU.

NORTON, Peter

2006 *Introduction to computers.* Sexta edición. New York, EE.UU. McGraw-Hill Technology Education.

PIATTINI, Mario G.; DEL PESO, Emilio

2001 *Auditoría Informática: Un enfoque práctico*. 2da Edición. México D.F:
Alfaomega grupo editor S.A.

REAL ACADEMIA DE LA LENGUA ESPAÑOLA

2012 *RAE.* Madrid. Consulta: 07 de setiembre del 2012 http://www.rae.es/rae.html

SECRÉTARIAT DU CONSEIL DU TRÉSOR DU CANADA

2009 *Business Case Guide*. Canada.

THE UPTIME INSTITUTE, INC.

2008 *Industry Standard Tier Classifications Define Site Infraestructure Performance*. Santa Fe.

2010 *Data Center Site Infrastructure. Tier Standard: Operational Sustainability.* Nueva York, USA.

TUPIA ANTICONA, Manuel Francisco

2011 *Principios de auditoría y control de sistemas de información.* Segunda Edición. Lima: Tupia Consultores y Auditores S.A.C.