UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS GEOLOGÍA Y CIVIL

ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE SISTEMAS

"PROCEDIMIENTOS PARA LA AUDITORÍA EN SEGURIDAD FÍSICA DEL DATA CENTER DE LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA"

TESIS PRESENTADO POR:

HUERTA ARANDA MELISSA

Para optar el título profesional de
INGENIERO DE SISTEMAS

ASESOR: ING. ELINAR CARRILLO RIVEROS

AYACUCHO-PERÚ

2015

"PROCEDIMIENTOS PARA LA AUDITORÍA EN SEGURIDAD FÍSICA DEL DATA CENTER DE LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA"

RECOMENDADO : 09 DE SETIEMBRE DEL 2015

APROBADO : 05 DE NOVIEMBRE DEL 2015

MSc. Ing. Carlos A. PRADO PRADO
(Presidente)

Ing. Karel PERALTA SOTOMAYOR
(Miembro)

Ing. Manuel A. LAGOS BARZOLA
(Miembro)

Ing. Elinar CARRILLO RIVEROS
(Miembro)

Ing. Floro N. YANGALI GUERRA
(Secretario Docente)

Según el acuerdo constatado en el Acta, levantada el 05 de noviembre del 2015, en la Sustentación de Tesis Profesional presentado por la Bachiller en Ingeniería de Sistemas Srta. Melissa HUERTA ARANDA, con el Trabajo Titulado "PROCEDIMIENTOS PARA LA AUDITORÍA EN SEGURIDAD FÍSICA DEL DATA CENTER DE LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA", fue calificado con la nota de DIECISÉIS (16) por lo que se da la respectiva APROBACIÓN.

MSc. Ing. Carlos A. PRADO PRADO
(Presidente)

Ing. Karel PERALTA SOTOMAYOR
(Miembro)

Ing. Manuel A. LAGOS BARZOLA
(Miembro)

Ing. Elinar CARRILLO RIVEROS
(Miembro)

Ing. Floro N. YANGALI GUERRA
(Secretario Docente)

DEDICATORIA

A Dios por ser el centro de mi vida y por encaminarme en la verdadera felicidad y porque con su gracia me impulsa día a día a trabajar en el desarrollo de una sociedad más justa, humana y fraterna.

A la Virgen María, por ser mi mamita del cielo a quien amo tanto.

A mis padres y hermanos que con su entrega generosa y amor profundo, han fortalecido en mí el anhelo de servir y amar.

AGRADECIMIENTO

A mis papás y a mi hermana Suyana, por su apoyo y su entrega sin límites.

A mis amigas: hna. Silvia y Daysi, por sus consejos su amistad verdadera y por recordarme que estoy hecha para "cosas grandes".

Al Movimiento de Vida Cristiana de Ayacucho, por ser mi familia espiritual y un medio para mi formación personal.

A la Ing. Elinar, por la paciencia y dedicación brindadas para orientarme a realizar un buen trabajo.

A los trabajadores de la sub gerencia de sistemas de la Municipalidad de Huamanga por dedicarme su tiempo y espacio para concluir con mi trabajo de investigación.

CONTENIDO

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

CAPITULO IV

RESULTADOS DE LA INVESTIGACIÓN

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Los Data Center se han convertido en la actualidad en los lugares más utilizados para el almacenamiento de información importante, por lo que el cumplimiento de medidas de seguridad que aseguren la permanencia y buen estado de los datos es fundamental.

La Municipalidad Provincial de Huamanga cuenta con un Data Center, la información que almacena y se maneja en ella es de vital importancia para su funcionamiento, motivo por el cual su cuidado es una tarea imprescindible.

Existen diversos ámbitos del Data Center de la Municipalidad que requieren ser analizados, no obstante, en el siguiente trabajo, vamos a ver lo concerniente a la seguridad física; es importante que los Data Centers estén preparados para resistir tanto catástrofes naturales como cualquier incidente que pueda afectar sus instalaciones y/o conectividad.

Por lo mencionado anteriormente, en la presente tesis se desarrolla una propuesta de procedimientos para la realización de una auditoría en seguridad física al Data Center de la Municipalidad Provincial de Huamanga, basados en estándares internacionales como el TIER I, en la normativa peruana NTP ISO/IEC 17799 y el marco de control COBIT5.0; con la intención de evaluar la infraestructura del Data Center y verificar la disposición de su seguridad física.

PALABRAS CLAVES

Auditoría en seguridad física, Data Center, TIER.

INTRODUCCIÓN

La auditoría de un Data Center en seguridad física es una tarea importante, que verifica el correcto funcionamiento de los equipos y el cumplimiento de las medidas necesarias para que, por ningún motivo, se interrumpan los procesos que son ejecutados en su interior.

La presente investigación brinda una herramienta de apoyo para la realización de una auditoría en seguridad física del Data Center de la Municipalidad Provincial de Huamanga, mediante procedimientos de auditoría.

Se muestra la realización de un procedimiento de auditoría para evaluar la seguridad física en el Data Center de la Municipalidad, utilizando como criterios de evaluación a los objetivos de control detallados en cada uno de los procesos de COBIT 5.0, que tienen relación directa con la seguridad física, a uno de los dominios de la norma peruana NTP-ISO/IEC 17799, y a los requerimientos de la clasificación y estándar internacional TIER. Con estos procedimientos se permiten recoger, agrupar y evaluar evidencias para determinar si las instalaciones del Data Center salvaguarda la información que procesa, y utiliza adecuadamente sus recursos.

En el capítulo I se describe la situación problemática que dio inicio a la investigación, se plantea el problema de la investigación, así como los objetivos y la justificación.

En el capítulo II se presenta el marco teórico de los principales conceptos, tales como auditoría, Data Center, seguridad física, y otros relacionados a ellos, también se fundamenta el marco teórico de los estándares utilizados, así como los principales antecedentes de la investigación en curso.

En el capítulo III se desarrolla la metodología de la investigación, donde se contempla el tipo, nivel y diseño de la investigación; las técnicas, herramientas e instrumentos usados para la implementación del presente trabajo de investigación.

En el capítulo IV se propone el diseño de un procedimiento de auditoría para la seguridad física, utilizando como criterios de evaluación a COBIT 5.0, a la clasificación y estándar internacional TIER y a la norma NTP-ISO/IEC 17799. En este capítulo también se realiza la aplicación de los procedimientos de auditoría en seguridad física, en las instalaciones del Data Center de la Municipalidad Provincial de Huamanga. Se evalúan los resultados arrojados y se emiten recomendaciones pertinentes.

En el capítulo V se presentan las conclusiones y recomendaciones de la investigación en general.

CAPÍTULO I

PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 DIAGNÓSTICO Y ENUNCIADO DEL PROBLEMA

La Municipalidad Provincial de Huamanga (MPH) es un gobierno local que brinda servicios públicos, comprometidos con la transparencia, responsabilidad e identidad cultural de la sociedad local; siendo una institución importante para la ciudad de Huamanga sus sistemas y Centro de Procesamiento de Datos necesitan someterse a una evaluación técnica objetiva, para conocer el nivel de seguridad *alcanzado* por sus actividades de control.

Actualmente el Data Center de la Municipalidad Provincial de Huamanga, es administrado por la Sub Gerencia de Sistemas y Tecnologías.

Las instalaciones del Data Center de la Municipalidad fueron diseñadas en base a un proyecto, en cuya documentación no están contemplados estándares internacionales de seguridad, pero si algunos lineamientos generales; la infraestructura de éste centro está ubicado en el sótano del local central y tiene hasta la fecha una antigüedad de dos años.

Para muchos la seguridad sigue siendo el área principal a auditar, cada día es mayor la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, el impacto de los fallos, los accesos no autorizados, la revelación de la información, y otras incidencias, cada vez van en aumento; de ahí la necesidad de protecciones adecuadas que se evalúan o recomiendan en una auditoría de seguridad (Piattini y Del Peso, 2001).

No existen informes ni registros que contemplen tareas de auditoría informática realizados al Data Center de la Municipalidad, y menos en lo concerniente a la seguridad física, poniéndolo de este modo como un punto olvidado e ignorado y un blanco fácil de ataques, de pérdidas o de daños irreversibles; por tal motivo es necesario realizar un diagnóstico y calificación de sus niveles de seguridad, utilizando la auditoría como una herramienta de evaluación. Como punto central nos enfocaremos en la seguridad física del Data Center.

Se tomará en cuenta la seguridad física porque la infraestructura física es la columna vertebral sobre la que se sustenta toda la operación de un Data Center y por ende de una organización, cualquier falla relacionada con su seguridad física podría generar dificultades en la disponibilidad de la información y en el buen desempeño de toda la institución.

La Municipalidad no contempla un presupuesto económico destinado a la realización de las tareas de auditoría en seguridad física, el personal que labora en dicha institución no tiene conocimiento de los medios o procesos para realizarlo, por esta razón se propone brindar una opción para evaluar y calificar la seguridad física de su Data Center, emitiendo un informe que muestre el cumplimiento de las mejores prácticas derivados de normas y estándares internacionales, y dar a conocer las vulnerabilidades de seguridad física de sus instalaciones, derivándolo en recomendaciones, acciones o cambios en sus políticas de seguridad.

1.2 DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN

PROBLEMA GENERAL

¿Cómo realizar una auditoría de seguridad física del Data Center de la Municipalidad Provincial de Huamanga, 2014?

PROBLEMA ESPECÍFICO

1. ¿Qué activos están involucrados en la seguridad física del Data Center de la Municipalidad Provincial de Huamanga?
2. ¿Cuáles son los riesgos comunes que atentan contra la seguridad física del Data Center de la Municipalidad Provincial de Huamanga?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Implementar un procedimiento de auditoría en seguridad física del Data Center de la Municipalidad Provincial de Huamanga de la ciudad de Ayacucho, 2014. Mediante la clasificación y estándar internacional TIER, marco de control COBIT 5.0 y la norma técnica peruana NTP-ISO/IEC 17799.

OBJETIVOS ESPECÍFICO

a. Identificar los activos involucrados en la seguridad física del Data Center de la Municipalidad Provincial de Huamanga.
b. Identificar los riesgos comunes en seguridad física del Data Center de la Municipalidad Provincial de Huamanga.

1.4 JUSTIFICACIÓN Y DELIMITACIÓN DE LA INVESTIGACIÓN

1.4.1 JUSTIFICACIÓN

Los Data Center son instalaciones donde se concentran una gran cantidad de recursos que tienen como principal misión procesar uno de los bienes más valiosos e irremplazables que tiene una organización, que es su información. La seguridad física en un Data Center asegura la disponibilidad de los procesos y de los servicios de Tecnología de Información (TI). En tal virtud, surge la necesidad de verificar que las instalaciones físicas en un Data Center sean adecuadas para el buen funcionamiento de los equipos que garanticen ésta disponibilidad.

Para verificar si un Data Center tiene un buen funcionamiento que evite interrupciones en sus servicios por el descuido en el mantenimiento, por una inadecuada ubicación de los equipos o elementos, o por cualquier

evento no programado, se hace ineludible contar con mecanismos de control en seguridad física y una herramienta para realizar ésta actividad de control es la auditoría en seguridad física.

La presente investigación tiene la intención de brindar una guía para la realización de una auditoría en seguridad física, que ayude a un auditor en la realización de una evaluación bien cimentada, que colabore con la institución u organización auditada en la prevención de eventualidades no deseadas, en la definición de las futuras líneas de actuación y en la eliminación de algunos riesgos más críticos, teniendo como referencia el Data Center de la Municipalidad Provincial de Huamanga.

La propuesta de la investigación se basa en marcos de control reconocidos internacionalmente, COBIT 5.0, la clasificación y estándar TIER y la norma técnica peruana NTP-ISO/IEC 17799; cuyos procesos e indicadores garantizan una evaluación certera y objetiva.

La Municipalidad se beneficiaría del presente trabajo, pues al verificar la capacidad y el cumplimiento de las medidas de seguridad física de su Data Center, se podría llegar a rectificaciones posteriores en sus políticas de seguridad, así como en sus controles que sean críticos y les ocasionen problemas.

1.4.2 DELIMITACIÓN

La demarcación espacial de la investigación será el Data Center de la Municipalidad Provincial de Huamanga, con información del año 2014.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Bustos, Chávez, Gonzáles, Millán y Gómez (2009), en su tesina, "Metodología para evaluar y calificar la seguridad física de un centro de procesamiento de datos", concluyen que la metodología propuesta y basadas en las mejores prácticas de las normas y estándares internacionales como la I ISO/IEC -171999 y el COBIT, evalúa y califica la seguridad física de un centro de datos, determinando su nivel de seguridad, permitiéndole actuar ante las amenazas y vulnerabilidades de manera eficiente, oportuna y eficaz, y disminuyendo la materialización de las riesgos.

Rubio (2012), en su tesis, "Análisis y Diseño de un Data Center en base a los estándares ANSI/EIA/TIA 606, 607 y 942 para el edificio de la Dirección Provincial de Salud de Pichincha", concluye que el diseño del Centro de Datas propuesto para la Dirección Provincial de Salud de Pichincha cumple can los estándares ANSI/EIA/TIA 606, 607 y 942, proporcionándale instalaciones bien equipadas, con un buen rendimiento y considerando factores importantes que involucran la seguridad, el control de incendios, el plan de contingencia, consumo reducido de potencia y un operador que se encargue de la administración y monitoreo del mismo.

Nogueira (2013), en su tesis, "Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER", concluye que el desarrollo de los procedimientas tienen como fin guiar los pasos que un auditor debe realizar para lagrar un resultado adecuado en una auditoría física y

medio ambiental de un Data Center; los procedimientos han sido aplicados correctamente en la auditoría a un Data Center real. De la misma forma ha podido comprobar que estos mismos procedimientos pueden ser extensibles a nivel de otros marcos y normas.

Llerena (2013), con su tesis de master, "Formulación de una guía de auditoria para la infraestructura física de los centros de datos de las entidades públicas del ecuador basado en marcos de referencia de TI", concluye que es necesario realizar Auditorías a los Centros de Datos de las entidades públicas del Ecuador, y evidencia que una auditoría contribuyen a mantener una adecuada infraestructura física de un Centro de Datos y ayuda a que los activos estén protegidos contra los riesgos causados por amenazas físicas; concluye además que para la realización de ésta guía de auditoría se ha utilizado varios estándares de TI y las normas de control Interno de la Contraloría General del Ecuador.

2.2 MARCO TEÓRICO

2.2.1 AUDITORÍA EN SEGURIDAD FÍSICA

Toda y cualquier auditoría, es una actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar (Ramirez y Álvarez, 2003).

Para muchos la seguridad sigue siendo el área principal a auditar, lo cierto es que cada día es mayor la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la revelación de la información, y otras incidencias, es mucho mayor que hace unos años; de ahí la necesidad de protecciones adecuadas que se evalúan o recomiendan en una auditoría de seguridad (Piattini y Del Peso, 2001).

La auditoria de la seguridad física, es un medio que permite la evaluación de las protecciones físicas de datos, programas, equipos

instalaciones, redes y soportes, e incluidas también a las personas. (Piattini y Del Peso, 2001)

"La auditoría de la seguridad física analiza todos los procesos referentes a la protección de los componentes hardware, dispositivos, instalaciones y entornos de los distintos sistemas informáticos. Los auditores deberán analizar la correcta protección y actualización de estos componentes, además de la protección de datos que forman parte del sistema" (Chicano, 2015)

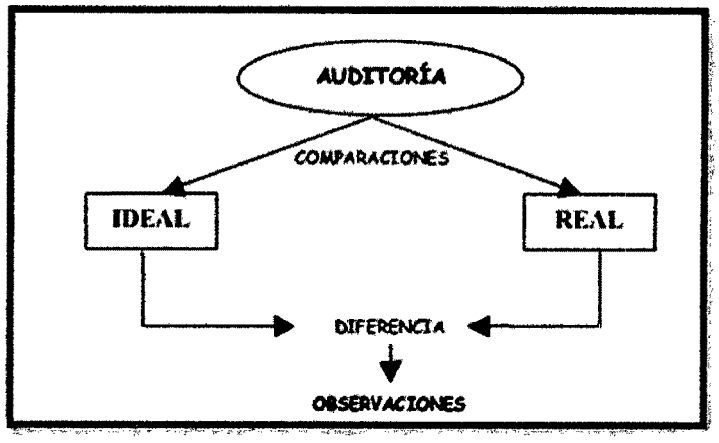


Figura N° 2.1: Esquema del concepto clásico de auditoría(Ramirez y Álvarez, 2003)

2.2.1.1 AUDITORÍA A UN DATA CENTER

El Data Center es el centro neurálgico de toda empresa y, por tanto, su seguridad y disponibilidad son esenciales. Un fallo en su infraestructura puede acarrear graves consecuencias. Para garantizar su operatividad, determinar su nivel de fiabilidad y seguridad es indispensable realizar auditorías que permitan conocer con exactitud el "estado de salud" de su infraestructura, que identifiquen los posibles riesgos, las carencias o debilidades, así como los problemas de capacidad. A través de una auditoria se identifican oportunidades para mejorar la disponibilidad y la eficiencia, se analiza la situación del Data Center en relación con la normativa aplicable y se definen las mejores prácticas (Compañía TRC, s.f.)

Por su parte Galán (1996) recomienda que al realizar una auditoría en un Data Center se debe verificar que sus instalaciones físicas sean adecuadas, que cumplan con los requisitos mínimos para permitir el adecuado funcionamiento de los equipos.

Piattini y Del Peso (2001) señalan a continuación algunas fuentes que deben estar accesibles en todo Data Center al realizar una auditoría:

- Políticas, normas y planes sobre seguridad.
- Auditorías anteriores, generales y parciales, referentes a la seguridad física a cualquier otro tipo de auditoría que, de una u otra manera, esté relacionada con la seguridad física.
- Contratos de seguros de proveedores y de mantenimiento.
- Entrevistas con el personal de seguridad.
- Actas e informes de técnicos y consultores (que diagnostiquen el estado físico del edificio, estado de operatividad de los sistemas de seguridad y alarma, agencias de seguridad que proporcionan a los vigilantes jurados, bomberos, etc).
- Plan de contingencia y valoración de la pruebas.
- Informes sobre accesos y visitas.
- Informes sobre pruebas de evacuación ante diferentes tipos de amenaza: incendio, catástrofe natural, terrorismo, etc.
- Informes sobre evacuaciones reales.
- Política de personal. Revisión de antecedentes personales y laborales, procedimientos de cancelación de contratos y despidos, rotación en el trabajo, planificación y distribución de tareas, contratos fijos y temporales.

2.2.1.2 CONCEPTOS PARA LA REALIZACIÓN DE LOS PROCEDIMIENTO DE AUDITORÍA

Para realizar una auditoría, según Delgado (1998) "el auditor deberá establecer procedimientos que le permitan sustentar su evaluación en técnicas apropiadas que faciliten la obtención de juicios objetivos resultantes de cada una de las pruebas que se realicen".

La opinión profesional, elemento esencial de la auditoría, se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma. Con los procedimientos se pretende garantizar que se toman en consideración todos los aspectos, áreas, elementos, operaciones, circunstancias, etc, que sean significativas (Piattini y Del Peso, 2001).

La norma internacional ISO 19011:2011 proporciona directrices sobre la auditoría a sistemas de gestión (por ejemplo: sistema de gestión de calidad, sistema de gestión financiero, sistema de gestión ambiental, *etc), directrices* que ayudarán al desarrollo del presente trabajo de investigación, de cuales se tomaron algunos conceptos:

A. **Plan de auditoría;** descripción de las actividades y de los detalles acordados de una auditoría
B. **Alcance de la auditoría;** es la extensión y límites de una auditoría. El alance de la auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el periodo de tiempo cubierto.
C. **Objetivos de auditoría;** definen lo que se debe lograr en la auditoría. Estos objetivos pueden estar en consideración a lo siguiente: prioridades de la gerencia, intenciones comerciales y de otros negocios, características de procesos, productos y proyectos y cualquier cambio en estos, resultados de auditorías

previas, necesidad de evaluación de proveedor, nivel de madurez del sistema de gestión a ser auditado.

D. **Criterio de Auditoría;** es un conjunto de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la evidencia de auditoría.

E. **Evidencia de auditoría;** comprende registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.

F. **Hallazgos de Auditoría;** son los resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría. Los hallazgos de auditoría pueden indicar tanto conformidad o no conformidad con los criterios de auditoría como oportunidades de mejora. Si los criterios de auditoría son legales, se utilizan a menudo los términos "cumple" o "no cumple" en un hallazgo de auditoría.

G. **Conclusiones de la auditoría** es el resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.

2.2.1.3 ACTIVOS

ISACA (2011) conceptualiza que es un "activo"; "un recurso o bien económico propiedad de una empresa, con el cual se obtienen beneficios. Los activos de las empresas varían de acuerdo con la naturaleza de la actividad desarrollada."

Para Areitio (2008) un activo es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección. Posibles activos a identificar son: Activos de TIC (hardware, software, información), personal (empleados, invitados, usuarios de empresas de externalización), entorno (edificio, instalaciones), actividades (operaciones).

Según Bustos et. al. (2009) un activo es un "recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos"

"Los activos también son fundamentales para lograr los objetivos definidos por la organización y requieren de una especial protección: cualquier amenaza que pueda afectar a un activo puede poner en peligro la actividad de la organización y su servicio al cliente" (Chicano, 2015)

Para Tupia (2010) un activo "es un elemento impreso o digital que contenga información, así como todo sistema - conformado por software, hardware y su documentación pertinente - que cree, maneje y procese información para una organización; también se puede incluir a la infraestructura tecnológica donde se desenvuelven dichos sistemas".

Según el estándar ISO/IEC 27005:2008, los activos de información se clasifican en las siguientes categorías:

- Activos de Información (datos, manuales de usuario, etc)
- Documentos de papel (licencias, contratos, etc)
- Activos de Software (aplicaciones, software de sistemas, etc)
- Activos físicos (computadoras, medios magnéticos, equipos, etc)
- Personal
- Servicios

Figura Nº 2.2: Clasificación general de los activos (Consultora ISOTools Excellence, 2013)

2.2.1.4 RIESGO

Según Guagalango y Moscoso (2011) un riesgo es "estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización".

Según Chaparro, Perez y Tenjo (2010) "el riesgo se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños."

Para Piattini y Del Peso (2001) el riesgo es "la probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad. Ejemplo: los datos estadísticos de cada evento de una base de datos de incidentes".

"El riesgo es la probabilidad de que una amenaza explote una vulnerabilidad. En los sistemas de la información se pueden asumir riesgos si el coste de la pérdida es bajo, pero existen entornos en los que el riesgo es muy alto y se han de implantar medidas para mitigarlo" (Cilleros, 2012).

Aguilera (2010), afirma:

> No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma. Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:
>
> - Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el perjuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría de la reparación del daño.
> - Aplicar medidas para disminuirlo o anularlo
> - Transferirlo (por ejemplo, contratando un seguro).

Para identificar los posibles riesgos dentro de un Data Center es necesario realizar un análisis de riesgo.

2.2.1.4.1 ANÁLISIS DE RIESGO

El análisis de riesgo, es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir.

Dais-ujat (2006) "El análisis de riesgo puede ser considerado como, la identificación, el análisis, la evaluación, el control y la minimización de las pérdidas asociadas con eventos de riesgo, es una revisión constante y permanente debido a que se trata de un proceso continuo"

El análisis de riesgos introduce un enfoque riguroso y consecuente para la investigación de los factores que contribuyen a los riesgos. En general implica la evaluación del impacto que una violación de la seguridad tendría en la empresa; señala los riesgos existentes, identificando las amenazas y la determinación de la vulnerabilidad a dichas amenazas. (De Pablos, López-Hermoso, Martín-Romo, Medina, Montero y Nájera, 2006)

Existen varias guías y metodologías que buscan hacer más objetivo el Análisis de Riesgos, entre los cuales constan Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), ISO 27005,

Octave (Metodología de Análisis y Gestión de Riesgos Operationally Critical Threat, Asset, and Vulnerability Evaluation), entre otras.

Chamorro (2013), en base a las metodologías mencionadas, plantea una forma práctica de realizar un análisis de riesgo, por lo que se definen las siguientes actividades o fases principales:

1. Identificación de Activos

Se identifican los activos que se encuentran dentro del alcance definido. Los activos de información son muy amplios por lo cual comprender que es un activo de información es fundamental para realizar el correcto análisis de riesgo.

2. Tasación de Activos

La tasación de activos se realiza bajo la afectación que produce la falla o pérdida de un activo en términos de confidencialidad, integridad y disponibilidad. Una práctica comúnmente utilizada al momento de realizar la tasación de activos es plateando la pregunta ¿Cómo una falla o pérdida en un activo específico afecta a la confidencialidad, la integridad y la disponibilidad?, para esto se debe puede hacer uso de la escala de Likert:

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

Tabla N° 2.1: Escala de Likert (Chamorro, 2013)

Identificación de Amenazas y Vulnerabilidades

La identificación de amenazas y vulnerabilidades se realiza en función de la naturaleza del activo, y se los clasifica según sea el caso en varios grupos de acuerdo a su origen, su naturaleza, entre otras.

3. Cálculo de Amenazas y vulnerabilidades.

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

4. Análisis del riesgo y su evaluación.

El análisis de riesgo ayuda a identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y de la probabilidad de ocurrencia de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Riesgo= Probabilidad x Impacto

Los niveles de riesgo calculados sirven para poder priorizar e identificar los más problemáticos.

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

2.2.1.4.2 VULNERABILIDAD

Mantino (2013) define la vulnerabilidad como "grado de resistencia y/o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro".

Piattini y Del Peso (2001) conceptualiza a la vulnerabilidad como la situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático.

Por su parte Aguilera (2010) define como la probabilidad que existe de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las mismas amenazas. Por ejemplo, los datos son

vulnerables a la acción del hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgo hay que tener en cuenta la vulnerabilidad de cada activo.

"Una vulnerabilidad, por sí misma, no causa daño alguno; es, simplemente, una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo. Las vulnerabilidades pueden ser permanentes, a no ser que se produzcan cambios en el activo, de forma que lo haga insensible a la vulnerabilidad" (Areitio, 2008)

2.2.1.4.3 AMENAZA

Según Piattini y Del Peso (2001) una amenaza es una(s) persona(s) o cosa(s) vista(s) como posible fuente de peligro o catástrofe. Ejemplos: inundación, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.

"Son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañándolo y no permitiendo que brinde soporte a algún proceso, perjudicando directamente la consecución de los objetivos de negocio" (Tupia, 2010).

Guagalango y Moscoso (2011) "una amenaza es cualquier cosa que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de nuestros activos".

Una amenaza necesita explotar una vulnerabilidad del activo para producir un daño. El daño causado por una amenaza puede ser temporal o permanente y se puede asociar con una escala de severidad como otros fenómenos. Entre las características más relevantes de una amenaza se encuentra las siguientes: El origen (puede ser interno o externo), la motivación (como son las ventajas competitivas, los beneficios económicos, etc), la frecuencia o periodicidad de los ataques, la severidad (dependiendo de si es o

irreversible). Al tratar las amenazas, se deben considerar los de tipo medioambientales y también culturales (Areitio, 2008)

Según Del Peso E., Ramos, Del Peso M. y Del Peso M. (2011) "las amenazas pueden ser muy diversas: sabotaje, vandalismo, terrorismo accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores, negligencias, huelgas, epidemias o intoxicaciones".

Mantino (2013) enumera distintas amenazas físicas con relación a la seguridad física:

- Desastres naturales, incendios accidentales, tormentas e inundaciones.
- Amenazas ocasionadas por el hombre.
- Disturbios, sabotajes internos y externos deliberados.

Para Aguilera (2010) las amenazas físicas pueden ser desde cortes eléctricos, fallos del hardware o riesgos ambientales; y menciona dos tipos de amenazas a nivel físico:

- **De interrupción**, el objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.
- **Accidentales**; accidentes meteorológicas, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

2.2.1.4.4 IMPACTO

Areitio (2008) "el impacto es la consecuencia de la materialización de una amenaza sobre un activo".

Es la magnitud del daño que provoca un ataque exitoso. Dependiendo de los daños causados y los activos afectados, el impacto será mayor o menor (Chicano, 2015)

Aguilera (2010) un impacto es la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad o dicho de otra manera, el daño causado.

2.2.2 DATA CENTER

"El Centro de Procesamiento de Datos (CPD) es un cuarto, espacio físico o ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. Se le conoce también como centro de cálculo en España, centro de cómputo en Iberoamérica, o centro de datos (data center). En dicho espacio se encuentran los equipos de una red, además de los servidores" (Gómez, 2011)

Según Bustos et. al. (2009), "es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico".

Para Rytoft (2013), los centros de datos se pueden definir como tres infraestructuras paralelas: TI, electricidad y refrigeración. Las tres infraestructuras tienen que ser perfectamente compatibles y estar armonizadas y optimizadas para lograr el funcionamiento perfecto de una instalación crítica. Esta infraestructura es donde se instalan las funciones principales de los centros de datos y donde se entregan los servicios de TI.

Según Taborda, Escobar y Torres (2011) "Un Data Center o centro de datos si lo traducimos literalmente es una instalación especializada para brindar facilidades desde hospedaje web de páginas webs estáticas hasta hospedaje de aplicaciones y diversos servicios de comunicaciones".

El objetivo principal de un CPD (Centro de Procesos de Datos) es proteger la integridad, confidencialidad y disponibilidad de la Información (Aguilera, 2010).

Los Data Center son creados y mantenidos por los organizaciones con objeto de tener acceso a la información necesaria para sus operaciones (Quintana, 2009).

"Prácticamente todas las compañías de tamaño mediano o grande disponen de algún tipo de CPD, mientras que las más grandes llegan a tener varios u optan por extemalizar este servicio. Entre los factores más importantes que motivan la creación de un CPD se puede destacar el garantizar la continuidad y disponibilidad del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica" (Espinosa, 2012).

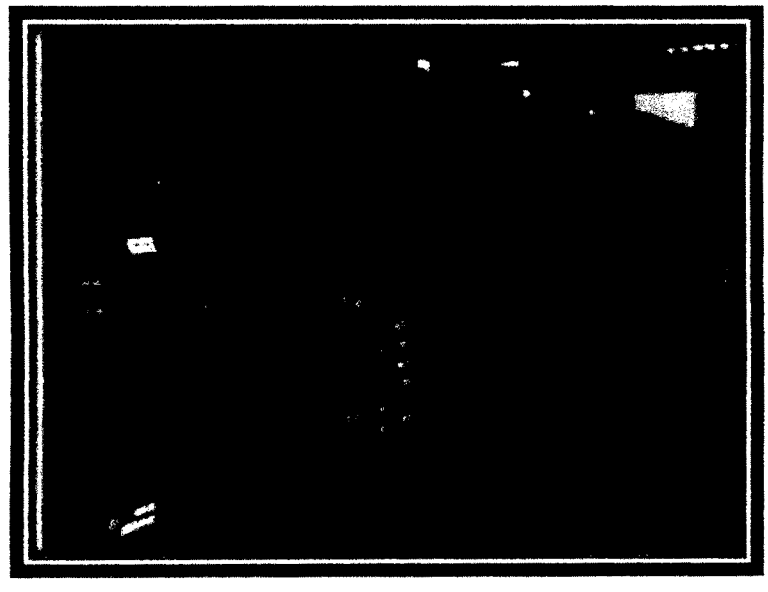


Figura N° 2.3: Centro de Procesos de Datos (Gómez, 2011)

2.2.2.1 SEGURIDAD FÍSICA EN UN DATA CENTER

Con la evolución tecnológica, el Data Center, cada día se hace más complejo, por lo que su infraestructura debe garantizar la continuidad de las operaciones. Tratándose de Data Centers, una falla puede generar parálisis en los servicios, grandes perjuicios o hasta costar la sobrevivencia de una empresa, por ello es necesaria una inversión en

una seguridad física porque es menor que el perjuicio proveniente de una falla grave causada por amenaza física o problemas relacionados a la infraestructura.

En relación seguridad físico de un Data Center (Compañía TRC, s.f.) menciona:

> La infraestructura física es la columna vertebral sobre la que se sustenta toda la operativa de un Data Center y, por tanto, del negocio de la organización. Es la base que permite que las redes de TI funcionen correctamente. Se trata de un sistema integrado de recursos en el que se incluyen los sistemas de energía, climatización, cableado, canalización, seguridad. Garantizar la seguridad de todo este conjunto integrado es un proceso complejo, ya que son muchos los factores que intervienen. Hay que tener en cuenta aspectos como la ubicación del Data Center, los elementos que lo componen, los aspectos medioambientales, los campos electromagnéticos. Asimismo, también hay que prever otras variables como incendios, inundaciones u otro tipo de catástrofes.

"La seguridad física consiste en la aplicación de barreras físicas y procedimientos de control para protección de las amenazas a los recursos, tanto del Data Center, como el resto de la empresa. Por la información que contiene, ésta es, sin dudas, la habitación más protegida de un entorno corporativo. Su estructura interior es bastante particular en comparación con otros ambientes" (Cerra, 2010).

Para Bustos et. al. (2009) la seguridad física "se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Los mecanismos de seguridad física deben

resguardar de amenazas producidas tanto por el hombre como por la naturaleza".

Mantino (2013) menciona algunas ventajas de la seguridad física:

- Disminuir siniestros.
- Trabajar mejor manteniendo la sensación de seguridad.
- Descartar falsas hipótesis si se produjeran incidentes.
- Tener los medios para luchar contra accidentes.

2.2.2.2 ELEMENTOS DE UN DATA CENTER

Para Barba y Viteri (2012), un Data Center se compone de cuatro elementos principales:

Espacio blanco: Es un espacio libre dentro del Data Center, necesarios para poder reasignar alguna función en particular; por ejemplo, un área para equipos nuevos.

Infraestructura de apoyo: Se refiere a los equipos y espacio necesarios para apoyar las funciones del Data Center como: transformadores, UPS, equipos de ventilación y aire acondicionado; panel de distribución de energía y equipos de transmisión remota.

Equipos de Soporte: Como racks o bastidores, cableado estructurado, servidores, unidades de almacenamiento y equipos de red.

Operaciones: Constituye el personal de operaciones o de soporte técnico, a quien asegura que los equipos y la infraestructura tengan el mantenimiento adecuado; estén mejorados y reparados.

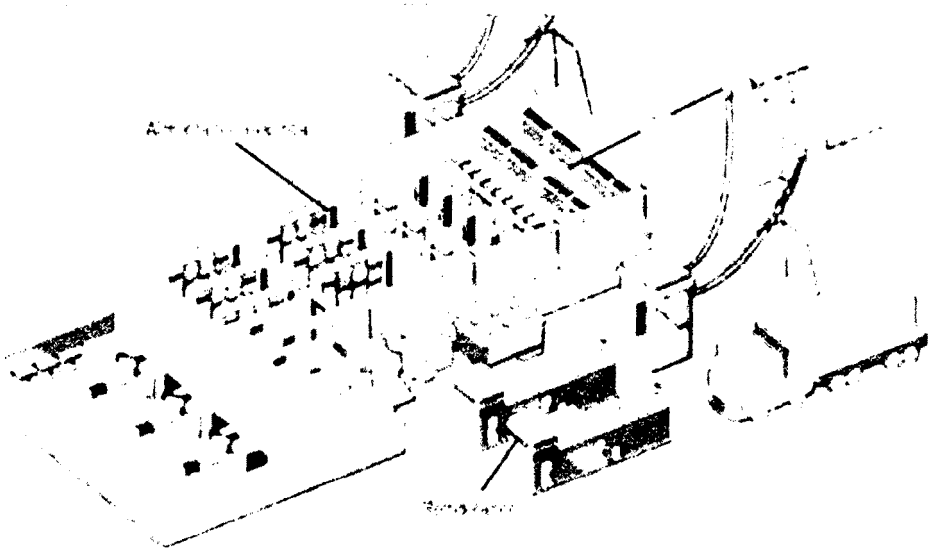


Figura N° 2.4: Configuración física de un centro de datos genérico (Rytoft, 2013)

Resumiendo lo q ue plantea Quintana (2009) y Taborda et. al. (2011) los elementos más importantes a tener en cuenta para un buen Data Centerson:

a) El espacio.
b) La ubicación geoestratégica.
c) Sistema Eléctrico (acometidas eléctricas, Sistemas de Alimentación Ininterrumpida-UPS, tablero de distribución eléctrica).
d) Sistema de refrigeración (climatización, aire acondicionado, pasillos fríos y calientes, flujos y pérdidas de aire)
e) Fluido de gases.
f) Cableado de datos: cobre, fibra, etc
g) Bandejas portacables distribuidoras.
h) Protección de contaminantes.
i) Equipos de comunicaciones en alta disponibilidad.
j) Sistemas de copias de seguridad.
k) Botón de apagado de emergencia EPO

l) Canalizaciones para proveedores de servicios de Telecomunicaciones.

m) Sistemas anti-incendio. Elementos ignífugos (en puertas y paredes)

n) Sistema de seguridad: CCTV, control accesos, detectores de movimientos, etc.

o) Pisos y techos falsos

p) Generadores y cuadros de distribución eléctrica. Depósito de combustible.

q) Instalación de alarmas, control de temperatura y humedad.

r) Sistemas para prevenir y controlar incendios e inundaciones como drenajes y extintores, puertas con protección anti-incendio.

s) Diseño hidrófugo ante recorridos de fontanería o filtraciones de agua.

t) Los pisos, paredes y techos deben estar sellados, pintados o construidos con un material que reduzca al máximo la aparición de polvo.

u) Carga del suelo: capacidad de carga suficiente para soportar tanto la carga concentrada como la carga distribuida de los equipos instalados.

v) Señalización o vías de evacuación.

Para Maldonado(2010), un Data Center debe tener los siguientes componentes:

a) Espacio Físico; es importante definir bien el espacio físico que ocupará el centro de datos. Esto generalmente implica a toda el área del centro de datos y los espacios asociados como cuartos de bodega, cuartos eléctricos, etc.

b) Piso Falso; el piso falso es un sistema de reja elevado que se instala en los centros de datos, los sistemas de aire, cableado y eléctrico

son ubicados a través del espacio que queda entre el piso fijo y el piso falso, garantizando una mejor circulación del aire para el enfriamiento y climatización de la sala facilitando la manipulación de los cables y del sistema eléctrico. Sistemas de seguridad como extintores, sensores de humo pueden ser ubicados aquí. El piso falso está compuesto de un estándar, que lo ubica a 30 cm del piso. Esto puede variar dependiendo del peso y fuerza que impriman los equipos dependiendo del uso en el centro de datos.

c) **Cuarto Eléctrico;** el cuarto eléctrico tiene que ver con el suministro de la energía para todo el centro de datos, este incluye los paneles, conductores y algunos tipos de receptores.

d) **Sistemas de respaldo eléctrico;** incluye todos los responsables de suministrar el flujo eléctrico al centro de datos ante cualquier falla por cualquier razón. Este sistema incluye baterías grandes conocidas como fuentes ininterrumpidas de corriente o también conocidas como generadores eléctricos, es importante determinar también la capacidad del generador que va a operar en el centro de datos.

e) **Cableado;** el sistema de cableado es toda una estructura de cables dentro del centro de datos. Este permitirá la comunicación a través del uso de algunos tipos de conectores que enlazarán los cables y comunicarán sistemas y servidores de manera local y remota. Los usuarios simplemente deberán conectar los servidores en el sistema de cableado estructurado del centro de datos con un cable sencillo al sistema principal.

f) **Enfriamiento;** el sistema de enfriamiento tiene que ver con los dispositivos y medios a través de los cuales se logra regular la temperatura del ambiente y el control en la humedad del centro de datos. Este sistema incorpora sistemas de aire acondicionado para lograrlo. Cada armario de servidores puede poseer su propio

sistema de enfriamiento, tales como refrigeradores o sistemas basados en circulación de agua.

g) **Extintores de fuego;** este sistema incluye todos los dispositivos y substancias asociadas con la detección de humo y extinción del fuego en el centro de datos. Los más comunes son los extintores basados en rociadores de agua, supresores gaseosos de fuego y extintores de mano.

h) **Otros componentes;** adicional a estos hay diversos componentes que no caen en la categoría de ser primordiales pero que si deben ser considerados y tomados en cuenta y que son encontrados en los entornos de un centro de datos. Esto incluye por ejemplo dispositivos para detección de goteras, mitigación sísmica, controles de seguridad física como biométricos y cámaras de seguridad.

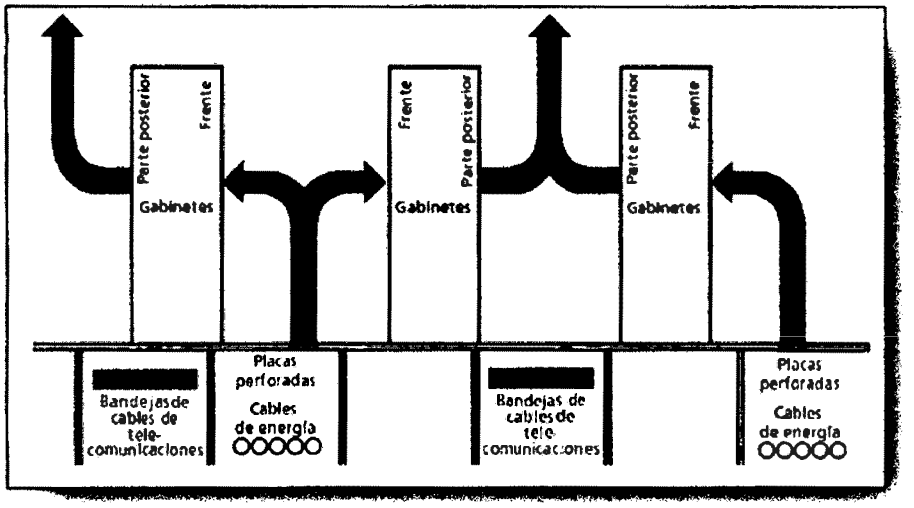


Figura N° 2.5: Configuración de los pasillos "Calientes y Fríos" (Barba y Viteri, 2012)

2.2.2.3 CARACTERÍSTICAS DE UN DATA CENTER

Los Data Center, ya sea para mantener las necesidades de una sola empresa o alojar decenas de miles de sitios de Internet de clientes, deben ser extremadamente confiables y seguros al tiempo que deben

ser capaces de adaptarse al crecimiento y la reconfiguración. Para diseñar un Data Center se deben tener en cuenta varias factares más allá del tamaña y la cantidad de equipas de datas que éste debiera albergar. Establecer el lugar físico, accesa a la energía, nivel de redundancia, cantidad de refrigeración, rigurosa seguridad y tipo de cableado son algunos de las características a considerar (Devoto, 2008).

A cantinuación Nagueira (2013) detalla las características lógicas, físicas, electrónicas, ambientales y de diseño más importantes de un centra de datos:

a) **Redundancia y disponibilidad:** La expectativa de un centro de datos es que cuente can una disponibilidad del 100% sin embarga, tados las centras de datas, sin importar cuan cuidadasamente hayan sido planificadas, construidos y manejadas, sufrirán de un período de tiempo de indispanibilidad, bien sea intencional o no intencional. La redundancia es una de las farmas de reducir la indisponibilidad, pues no se cuenta can un salo elementa que pravee servicias, por ejemplo eléctricos, sino que se contará can alguna medida que permitirá que, de fallar un servicio, el otra pueda asumir el trabaja y así el negocio no sienta el efecto de la falla.

b) **Fiabilidad:** Está estrechamente relacionada con la redundancia y dispanibilidad, pues un centra de datos debe ser diseñado de manera que se crea en el hecho de que no se aceptarán fallas durante tada el praceso de su funcianamiento. Uno de los mecanismas que permitirán confiar en el funcionamiento constante de un Data Center será la redundancia.

c) **Manejabilidad:** La manejabilidad nos indica la facilidad para el accesa, localización y reconfiguración de los elementos y características de las Data Center. Es necesario que, durante el

diseño de éste, se busque como características la fiabilidad, flexibilidad y la integración de actualizaciones y modificaciones.

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

e) **Administración de cables:** 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.

f) **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.

g) **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.

h) **Ubicación de los 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.

i) **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

j) **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.

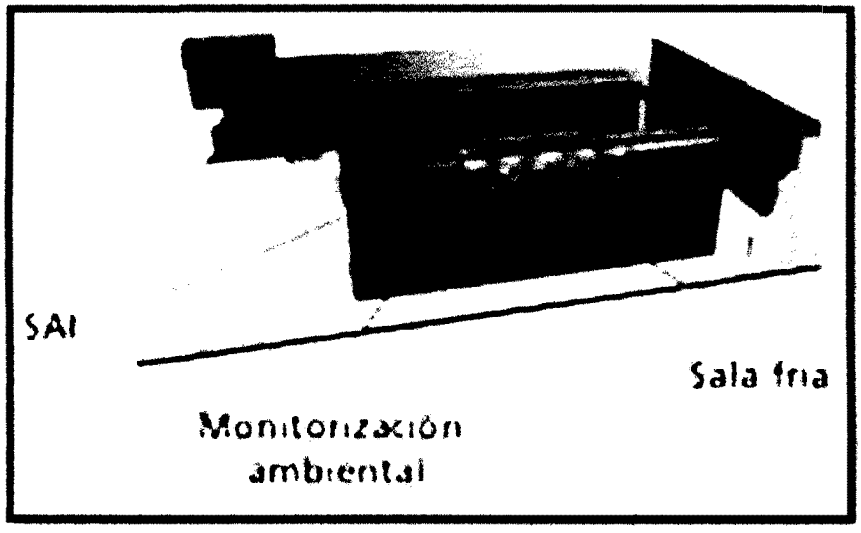


Figura N° 2.6: Esquema de un CPD con sala fría, con los sistemas de monitorización ambiental y de alimentación ininterrumpida (Aguilera, 2010)

Arizala y Ortiz (2010), resume las características de un Data Center de la siguiente manera:

a) **Conectividad en la red:** Las redes de computadoras son el mecanismo principal de conectividad en un ambiente electrónico. Al hablar de conectividad en la red, se refiere entonces al nivel de eficacia con que los dispositivos electrónicos logran empatarse dentro de la red para alcanzar su objetivo principal de compartir recursos.

b) **Seguridad física y lógica:** La capacidad de proteger físicamente los bienes y recursos es una consideración importante en la estrategia de seguridad de una organización. Ya sea porque su principal preocupación es la seguridad de su personal, la seguridad de sus datos y sistemas o la protección de su equipo clave. En cuanto a lo que tiene que ver con la seguridad lógica, se pueden mencionar la periodicidad de las actualizaciones de

los sistemas, las réplicas de disco, autenticación y autorización de cuentas, encriptación, instalación de firewalls, antivirus, etc., que dan la garantía de la fiabilidad de la información.

c) **Fiabilidad de la Información:** En informática, se refiere a la fiabilidad como la capacidad de un sistema para desempeñar y mantener sus funciones en circunstancias rutinarias, hostiles o inesperadas durante un determinado periodo de tiempo. En teoría, un producto fiable es totalmente libre de errores; en la práctica sin embargo, frecuentemente se expresa la fiabilidad de un sistema por medio de un porcentaje. Los Centros de Datos buscan reducir al mínimo los tiempos de inactividad (downtimes) y para ello se valen de recursos como la redundancia de los datos y la virtualización de la información. La *redundancia* es la propiedad que constituye un factor comunicativo estratégico que consiste en intensificar, subrayar y repetir la información contenida en el mensaje a fin de que el "ruido" no provoque una pérdida fundamental de información, esto se logra con la implementación de equipos como routers, switches, etc.

   La *virtualización* se refiere a la abstracción de los recursos de una computadora, llamada Hypervisor o VMM (Virtual Machine Monitor), la máquina virtual en general es un sistema operativo completo que corre como si estuviera instalado en una plataforma de hardware autónoma. Los ambientes virtualizados permiten a las organizaciones reducir costos operativos, consumo de energía y espacio físico.

d) **Disponibilidad permanente:** La disponibilidad y la eficiencia energética son dos de los conceptos asociados a un Centro de Datos sobre los que más se incide a la hora de establecer las prescripciones de partida para un nuevo proyecto o a la hora de valorar una instalación existente. En el origen de ambos, y en

mayor o menor grado, se encuentra la topología de diseño que, por ello, se ha convertido en una de los requerimientos principales. En cualquier caso, e independientemente del nivel de exigencia deseado, toda instalación de Centro de Datos cuenta con dos elementos mínimos: Sistema de suministro ininterrumpido y Suministro de emergencia. La colocación de UPSs y grupos electrógenos es un denominador común que constituye la base de todas las topologías.

e) **Escalabilidad de la infraestructura:** La infraestructura de un Centro de Datos debe brindar la flexibilidad necesaria que permita realizar cambios desde el diseño. El diseño de un Centro de Datos comienza por la elección de su ubicación geográfica, y requiere un balance entre diversos factores: Coste económico, infraestructuras disponibles en las cercanías, riesgo, etc., una vez seleccionada la ubicación es necesario encontrar unas dependencias adecuadas para su finalidad, ya se trate de un local de nueva construcción u otro ya existente a comprar o alquilar. Aun cuando se disponga del local adecuado, siempre es necesario algún despliegue de infraestructuras en su interior.

f) **Protección ambiental:** La tendencia de los nuevos Centros de Datos, condescendientes con el medio ambiente, es hacia los Green Data Centers (Centros de Datos Ecológicos), en los cuales la mecánica, iluminación, electricidad y sistemas de computadoras están diseñados para obtener una eficiencia de energía máxima y un mínimo impacto ambiental. La construcción y operación de estos centros incluye avances tecnológicos y estrategias, como por ejemplo el uso de materiales de construcción de bajas emisiones, reciclaje de los desperdicios, instalación de convertidores catalíticos sobre los generadores de respaldo, el uso de vehículos híbridos o eléctricos, etc.

g) **Gestión de Riesgos:** La falla de un sistema informático puede producir pérdidas en la productividad y de dinero, y en algunos casos críticos, hasta pérdidas materiales y humanas. Por esta razón es necesario evaluar los riesgos ligados al funcionamiento incorrecto (falla) de uno de los componentes de un sistema informático y anticipar los medios y medidas para evitar incidentes o para restablecer el servicio en un tiempo aceptable.

2.2.3 TIER

El TIER de un Data Center es una clasificación ideada por el Uptime Institute (organismo encargado de dar la certificación Tier) que se plasmó en el estándar ANSI/TIA-942 y que básicamente establece 4 categorías, en función del nivel de redundancia de los componentes que soportan el Data Center (Clasificación TIER en el Data Center, 2012) Bernabé y López (2012) una condición fundamental a la hora de diseñar un CPD es el que no haya puntos únicos de fallo, de forma que *siempre* haya redundancia de componentes y tener así una mayor fiabilidad, tanto en el CPD y su infraestructura, como en los servicios externos que se publican. La redundancia aumenta la tolerancia a fallos y el margen de maniobra en caso de necesidad. En la actualidad, para valorar el nivel de disponibilidad de un CPD la norma más extendida es la que se conoce como ANSI/TIA-942. El anexo informativo G de esta norma, basado en recomendaciones del Uptime Institute, establece cuatro niveles (TIERS)

Rubio (2012) nos ayuda entender un poco sobre los niveles TIER:

TIER I INFRAESTRUCTURA BÁSICA

Ningún sistema tiene redundancia, es decir tiene un solo proveedor de servicios de telecomunicaciones, un solo punto de acceso de energía eléctrica o un solo sistema de HVAC (Sistema de ventilación, calefacción y aire acondicionado).

Cumple condiciones mínimas para contrarrestar inundaciones, como por ejemplo haber instalado piso falso. Los sistemas de respaldo de energía como los UPS van por la misma instalación eléctrica que la energía principal.

Generalmente se debe cortar el servicio una vez al año por motivo de mantenimiento. También tiene sistema básico de puesta a tierra.

TIER II COMPONENTES REDUNDATES

Cuenta con un segundo punto de acceso para los servicios de telecomunicaciones, los UPS (se alimentan de un generador diesel) y un segundo sistema de HVAC. Los servicios que brinda el Data Center pueden verse interrumpidos en menor porcentaje por actividades deseadas o no deseadas; como por ejemplo: corte del suministro eléctrico o tareas de mantenimiento eléctrico o tareas de mantenimiento en el Data Center. Esta infraestructura cuenta con puertas de seguridad.

TIER III MANTENIMIENTO SIMULTÁNEO

Cuenta con redundancia de equipo y rutas redundantes para telecomunicaciones, HVAC, sistema eléctrico (varias vías de distribución; por lo general 2 proveedores de servicios). Los servicios que brinda el Data Center no se ven interrumpidos por mantenimiento, ya que se puede suspender una línea y dar el servicio por otra línea de distribución. El nivel de seguridad es mayor al contar con sistemas de CCTV, blindaje magnético en las paredes, detección de inundaciones.

TIER IV TOLERANTE A FALLAS

Cuenta con múltiples componentes y rutas de redundancia, muchas de estas siempre activas. Soporta en el peor de los casos un incidente no planificado. Se maneja una mayor protección para incidentes naturales como terremotos, huracanes o inundaciones.

Todos los equipos tienen redundancia de datos y cableado eléctrico en circuitos separados. Comprende un edificio separado (áreas aisladas) solo para el Data Center.

	TIERI	TIER II	TIER III	TIER IV
Aplicado:	A empresas pequeños,en los cuales se usa TI únicamente para procesos internos.	A empresas pequeños, en los cuales se utiliza TI limitado al horario de oficina y que no ofrecen servicios en línea a cualquier hora.	Compañías que dan soporte 24/7 como centros de servicio e información.	Compañías que brindan servicio 24x365, compañías basadas en comercio electrónico o de transacciones online, así como entidades financieras
Componentes redundantes	N	N + 1	N + 1	2(N+1)
Disponibilidad [%]	99,671	99,749	99,982	99,995
Tiempo de caída anual [horas]	28,8	22,8	1,6	0,4
Turnos del personal	Ninguno	1 turno	1 + turnos	Siempre (24 horas)
Enfriamiento Continuo	No	No	Puede ser	Si
Puntos únicos de falla	varios+error humano	varios+error humano	pocos+error humano	ninguno+error huamano
Meses para implementar	3	3-6	15-20	15-20
Año de primera implementación	1965	1970	1985	1995

Tabla N° 2.2: Cuadra descriptivo de las característicos TIER poro un Doto Center (Elaboración propio)

Para Bernobé y López (2012):

TIER I

Un CPD está definido como de nivel I (o TIER 1), si no alcanza a dispaner las companentes redundantes y puede tener una solo instalación de infraestructuras de distribución eléctrico y refrigeración. Puede carecer de suelo técnico (por donde introducir y acceder el cableado) y carecer de garantías de servicio continuo de energía ya sea mediante un generador propio o mediante uno

UPS. En todo caso, aunque alguna de la infraestructura pueda ser redundante, no se garantiza que no haya uno o varios puntos de fallos sin repuesto activo. Se asume que el sistema podrá estar en situaciones críticas al límite de su funcionamiento y podrá apagarse alguna vez y dejar de funcionar por cuestiones de mantenimiento o reparaciones.

TIER II

El siguiente nivel (tier 2), llamado de componentes redundantes implica que dispone de más capacidad para continuar funcionando aunque fallen algunos sistemas o se necesite parar alguno para sus modificación o recambio. Tiene componentes redundantes en toda la infraestructura que entran en funcionamiento al parar los primarios. Dispone de suelo técnico y sistemas de mantenimiento de la energía eléctrica, aunque el sistema de distribución eléctrica y el de refrigeración no estén duplicados. Esto puede causar una parada.

TIER III

Cuando puede realizar cualquier operación sobre cualquiera de las infraestructuras del centro de datos sin que eso signifique una caída del sistema. Este nivel se denomina de mantenimiento simultáneo. Dispone de diferentes sistemas de refrigeración, diferentes conducciones y sistemas eléctricos aunque sólo dispone de una ruta activa, lo que implica que los componentes redundantes no están en la ruta principal.

TIER IV

El nivel 4 o CPD tolerante a fallos, asegura que cualquier trabajo, sobre cualquier de los subsistemas puede realizarse sin que se interrumpa el servicio. Eso se logra gracias a la existencia distintas rutas de distribución de la energía eléctrica y frigorífica. Implica la existencia de distintas rutas de distribución activa simultánea.

Esta clasificación TIER es aplicable en forma independiente a cada subsistema de la infraestructura física de los Data Centers: Telecomunicaciones, Arquitectura, Eléctrico y Mecánico. Hay que tener en cuenta que la clasificación global del Data Center será igual a la de aquel subsistema que tenga el menor número de tier.

2.2.4 COBIT 5.0

COBIT (Control Objectives for Information and related Technology) es el marco aceptado internacionalmente como buena práctica para el control de la información, Tecnología de Información (TI) y los riesgos que conllevan.

ISACA (2012), la asociación internacional custodios del framework COBIT, nos dan a conocer todo a cerca del COBIT 5.0:

COBIT 5.0 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Ayuda también a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5.0 es genérico y útil para empresas de todos los tamaños, tanto comerciales, con o sin ánimo de lucro o del sector público.

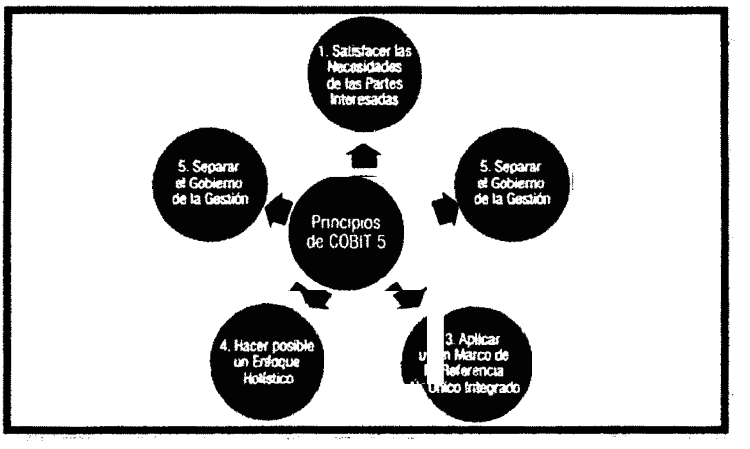


Figura N° 2.7: Principios de COBIT 5.0 (ISACA, 2012)

COBIT 5.0 se basa en cinco principios claves (figura 2.7) para el gobierno y la gestión de las TI empresariales:

- **Principio 1. Satisfacer las Necesidades de las Partes Interesadas.**
  Las empresas existen para crear valor a sus Stakeholders. Esto se logra manteniendo un balance entre los objetivos de negocio, la optimización de los riesgos que puedan existir y el uso de recursos dentro de la organización. COBIT 5.0 provee todos los procesos requeridos y otros habilitadores para dar soporte a la creación de valor a través del uso de las tecnologías de información.
- **Principio 2: Cubrir la Empresa Extremo-a-Extremo**
  COBIT 5.0 cubre todas las funciones y procesos dentro de la empresa. No solo se enfoca en la parte de TI, sino que trata a la información y a la tecnología como activos que necesitan ser tratados como otro cualquier activo dentro de la empresa.
- **Principio 3: Aplicar un Marco de Referencia único integrado**
  Hay varios estándares relacionados a las tecnologías de información y sus buenas prácticas. COBIT 5.0 se alinea con estos estándares y frameworks en un alto nivel y puede ser utilizado como un marco contenedor de todos estos.
- **Principio 4: Hacer Posible un Enfoque Holístico**
  COBIT 5.0 define un conjunto de habilitadores para dar soporte a la implementación de un gobierno y una gestión comprensiva de TI. Estos habilitadores son definidos como cualquier cosa que pueda ayudar a alcanzar los objetivos de negocio de la organización. Más adelante se definirán los siete habilitadores que propone COBIT 5.0.
- **Principio 5: Separar el Gobierno de la Gestión**
  El marco de trabajo COBIT 5.0 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

La visión de COBIT 5.0 en esta distinción clave entre gobierno y gestión es:

Gobierno: El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas.

Gestión: La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

Ciclo de Vida de COBIT 5.0

La implementación del ciclo de vida proporciona a las empresas una manera de usar COBIT para solucionar la complejidad y los desafíos que normalmente aparecen durante las implementaciones. El ciclo de vida y sus siete fases se ilustran en la Figura 2.8:

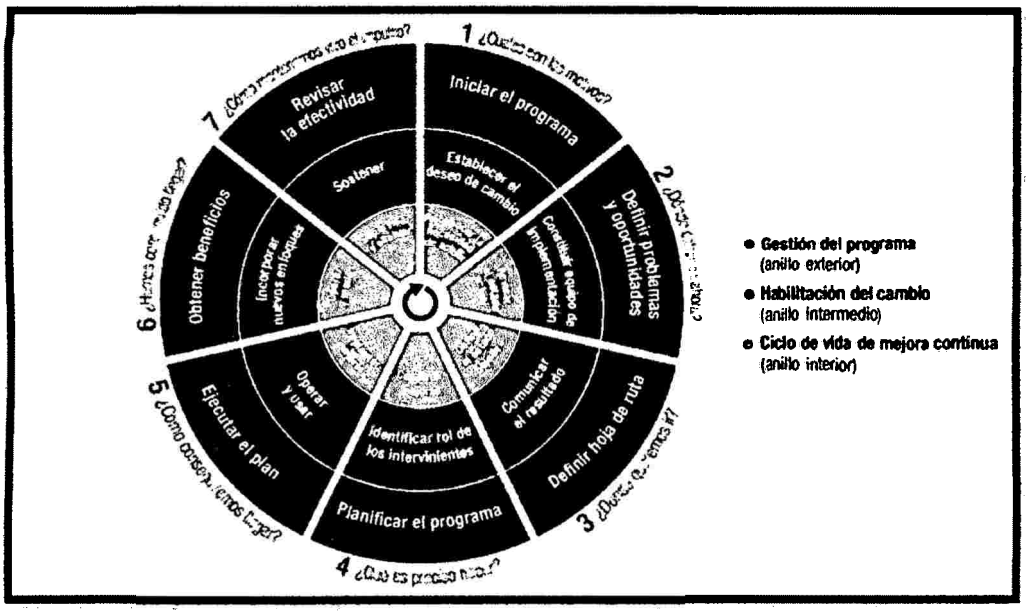


Figura N° 2.8: Ciclo de Vida de implementación de COBIT 5.0 (ISACA, 2012)

La implementación cubre:

- Posicionamiento del Gobierno de TI empresarial dentro de la organización.
- Tomar los primeros pasos hacia la mejora del Gobierno de TI

- Desafíos de la implementación y factores de éxito.
- Facilitar los cambios organizacionales y el comportamiento de los mismos.
- Implantado la Mejora Continua que incluye posibilitación del cambio y gestión del programa.
- La utilización del marco integral COBIT y sus componentes.

Facilitadores de COBIT 5.0

También se presenta el concepto de facilitadores que son factores que individual o colectivamente influyen para que algo funcione. En COBIT 5.0 son descritas 7 categorías:

1. **Principios, políticas y marcos de trabajo** son el medio para trasladar el comportamiento deseado a una guía práctica para conducir la gestión del día-a-día.

2. Procesos constituyen un conjunto organizado de prácticas y actividades.

3. Estructura organizativa

4. Cultura, ética y comportamiento como un factor de éxito de los objetivos de gobierno y gestión establecidos.

5. La Información está en todos los ámbitos de la organización. Es requerida para mantener a la organización andando y bien gestionada. Asimismo, en un nivel operacional, la información es pieza clave.

6. Servicios, infraestructura y aplicaciones dan soporte a los procesos y a las TI.

7. Personas, habilidades y competencias específicas. Son requeridas para tomar decisiones correctas y tomar acciones correctivas adecuadas.

El modelo de referencia de COBIT 5.0

COBIT 5.0 es complementado por sus procesos facilitadores que son: prácticas relacionadas de TI.

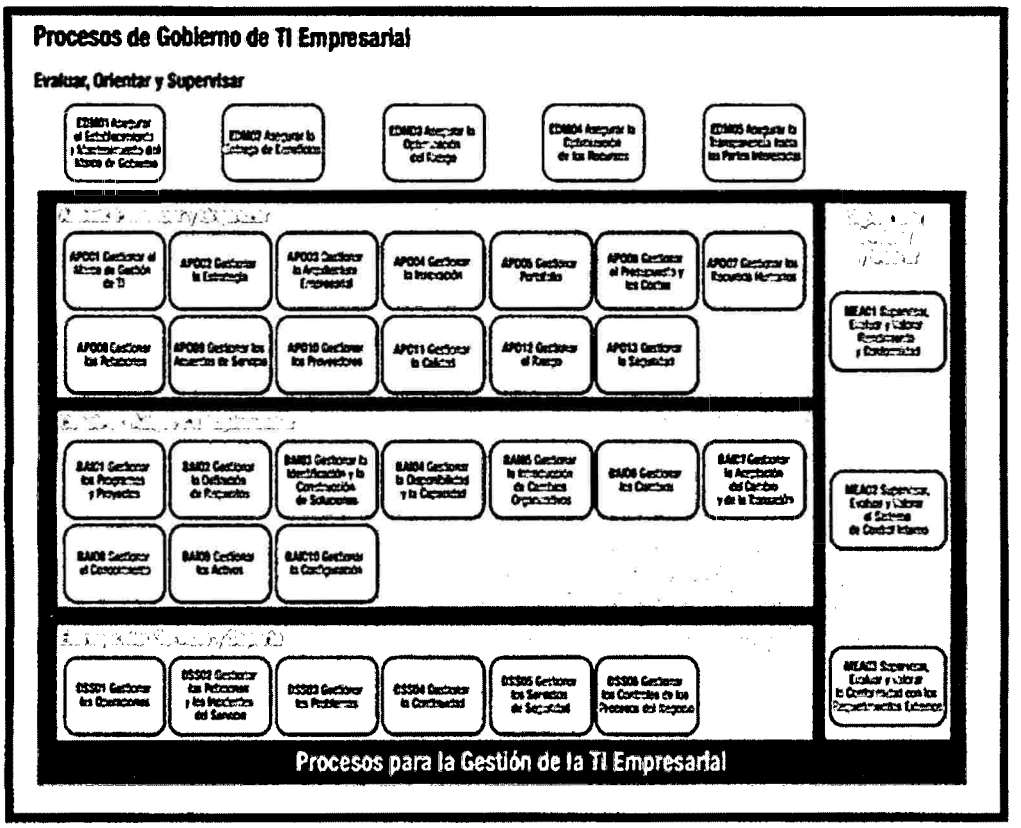


Figura N° 2.9: Modelo de Procesos COBIT 5.0 (ISACA, 2012)

El modelo de referencia de COBIT 5.0 divide a los procesos de gobierno y gestión de una empresa de TI en dos áreas principales de actividad: gobierno y gestión a su vez divididas en dominios de procesos.

- **Gobierno**; este dominio contiene cinco procesos de gobierno; en cada uno de ellos se definen prácticas de Evaluación, Dirección y Supervisión (**EDM**, siglos en inglés).
- **Gestión**; estos cuatro dominios están alineados con las áreas de responsabilidad de Planificación, Construcción, Ejecución y Supervisión (**PBRM** por sus siglos en inglés) proporcionando cobertura, de principio o fin, a toda lo TI.

2.2.5 NTP-ISO/IEC 17799

Norma Técnica Peruana elaborada por el comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos (EDI) en el año 2006, siendo oficializada al año siguiente. La NTP-ISO/IEC 17799, es una adopción de la norma ISO 17799:2005; actualmente renombrado como ISO 27002:2005. Es importante indicar que las norma ISO 27002 ha sido actualizada recientemente a la versión 27002:2013; pero los NTP (normativa vigente) aún mantienen su versión anterior (ISO 27002:2005), mientras no se actualice al equivalente a la nueva versión ISO, se puede seguir trabajando bajo la versión anterior.

La NTP 17799:2007 tiene como finalidad proporcionar una base común en el desarrollo de normas de seguridad en las organizaciones y ser una buena práctica de la gestión de la seguridad, la supervisión de su cumplimiento está a cargo de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI.

La estructura de este estándar contiene 11 cláusulas y cada una acompaña por categorías principales de seguridad que en su totalidad suman 39 categorías, que son:

1. Política de seguridad

a. Política de seguridad de la información.

2. Aspectos organizativos para la seguridad

a. Organización interna.

b. Seguridad en los accesos de terceras partes.

3. Clasificación y control de activos

a. Responsabilidad sobre los activos.

b. Clasificación de la información.

4. Seguridad en Recursos Humanos

a. Seguridad antes del empleo.

b. Durante el empleo.

c. Finalización o cambio del empleo.

5. Seguridad física y ambiental

a. Áreas seguras.

b. Seguridad de los equipos.

6. Gestión de comunicaciones y operaciones

a. Procedimientos y responsabilidades de operación.

b. Gestión de servicios externos.

c. Planificación y aceptación del sistema.

d. Protección contra software malicioso.

e. Gestión de respaldo y recuperación.

f. Gestión de seguridad en redes.

g. Utilización de los medios de información.

h. Intercambio de información.

i. Servicios de correo electrónico.

j. Monitoreo.

7. Control de accesos

a. Requisitos de negocio para el control de accesos.

b. Gestión de acceso de usuarios.

c. Responsabilidades de los usuarios.

d. Control de acceso a la red.

e. Control de acceso al sistema operativo.

f. Control de acceso a las aplicaciones y la información.

g. Informática móvil y teletrabajo.

8. Adquisición, desarrollo y mantenimiento de sistemas

a. Requisitos de seguridad de los sistemas.

b. Seguridad de las aplicaciones del sistema.

c. Controles criptográficos.

d. Seguridad de los archivos del sistema.

e. Seguridad en los procesos de desarrollo y soporte:

f. Gestión de la vulnerabilidad técnica

9. Gestión de incidentes en la Seguridad de Información

a. Reportando eventos y debilidades de la seguridad de información
b. Gestión de las mejoras e incidentes en la seguridad de información

10. Gestión de continuidad del negocio

a. Aspectos de la gestión de continuidad del negocio

11. Cumplimiento

a. Cumplimiento con los requisitos legales.
b. Revisiones de la política de seguridad y de la conformidad técnica.
c. Consideraciones sobre la auditoria de sistemas

La oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros, ha recomendado la aplicación y uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007". De conformidad con lo dispuesto por el Decreto Legislativo N° 560 - Ley del Poder Ejecutivo y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo N° 063-2007-PCM, con la finalidad de poder generar un plan de seguridad de la información en la administración pública, medida que muestra que el estado peruano tiene como consigna el introducir cada vez más la cultura de seguridad en sus empresas estatales.

CAPITULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 TIPO DE LA INVESTIGACIÓN

Para McMillan y Schumacher (2005) "La investigación aplicada se centra en un campo de práctica habitual y se preocupa por el desarrollo y la aplicación del conocimiento obtenido en la investigación sobre dicha práctica."

Según Carrasco (2009) "la investigación aplicada se distingue por tener propósitos prácticos inmediatos bien definidos, es decir, se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad. Para realizar investigaciones aplicadas es muy importante contar con el aporte de las teorías científicas, que son producidas por la investigación básica y sustantiva"

Por lo antes mencionado la presente investigación es de tipo aplicada, porque buscará contribuir con soluciones innovadoras a una organización en este caso la MPH.

3.2 NIVEL DE LA INVESTIGACIÓN

Para Bernol (2006), la investigación descriptiva es un nivel básico de investigación, el cual se convierte en la base de otros tipos de investigación; además, agregan que la mayoría de los tipos de estudios tienen, de una u otra formas, aspectos de carácter descriptivo. La investigación descriptiva se soporta principalmente en técnicas como la encuesta, la entrevista, la observación y la revisión documental. Algunos ejernplos de temas de investigación descriptiva son: estudios de carácter diagnóstico, diseño de guías, modelos, productos, prototipos, estudio de tiempos y movimientos, etc.

Debido a éste concepto, el nivel de la presente investigación es descriptiva.

3.3 DISEÑO DE LA INVESTIGACIÓN

La investigación no experimental se define como la investigación que se realiza sin manipular deliberadamente variables, no varía en forma intencional las variables independientes, lo que se hace es observar tal y como se da un fenómeno en su contexto natural para después analizarlo. (Hernández, Fernández y Baptista, 2003).

En diseños transaccionales o transversales, "se recolectan datos en un solo momento, en un tiempo único. El propósito es analizar y describir variables en un momento dado" (Hernández et. al. 2003). Debido a estas acepciones el diseño de la presente investigación es no experimental y transversal.

3.4 MÉTODO

En la presente investigación se utilizaron los siguientes métodos:

Inductivo – Deductivo. Método de inferencia, basado en reglas lógicas de deducción con el que se llega a nuevos conocimientos y predicciones relacionado con el estudio de hechos particulares.

Sintético. Este método es el que usa la síntesis (composición de un todo por la reunión de sus partes) como procedimiento ordenado para conocer la verdad de las cosas.

Analítico. Este método es el que proceso por medio del análisis, el análisis es la distinción o separación de las partes de un todo hasta llegar a conocer sus principios o elementos.

3.5 POBLACIÓN Y MUESTRA

POBLACIÓN

La población está conformada por todos los procesos de control de la seguridad física de un Data Center.

MUESTRA

Se realizó una selección por juicio de valor de los procesos de control relacionados a la seguridad física de un Data Center según TIER, Cobit 5.0, NPT-ISO/IEC 17799. En total los procesos de control seleccionados son 105.

3.6 VARIABLES E INDICADORES

DEFINICION CONCEPTUAL DE LAS VARIABLES

VARIABLE X

Auditoría en Seguridad física. Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios de auditoría, pero centrando sus análisis y revisiones en los aspecto de la seguridad física.

DIMENSIONES

Activos. Cualquier elemento o información que las entidades consideran importante o de alta validez.

Riesgo. Potencial de que una amenaza (externa o interna) explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización.

VARIABLE Y

Data Center. Es una infraestructura informática muy importante y vulnerable en toda empresa, cuya principal función consiste en albergar los recursos necesarios para la gestión, procesamiento de información, servicios de TI; es decir, equipos informáticos como racks, dispositivos de networking y almacenamiento, servidores (web, aplicaciones, base de datos) y sus áreas de soporte, todos ellos con el objetivo de mantener los servicios de continuidad operativa de una organización.

DIMENSIONES

Elementos. Se refiere a cada una de las partes o componente del que consta un Data Center.

Características. El diseño de un Data Center debe contar con ciertos rasgos o características que hagan de él una buena infraestructura que brinde las máximas garantías para la continuidad de un negocio, de sus operaciones y para la seguridad de los activos de información.

DEFINICION OPERACIONAL DE LAS VARIABLES

VARIABLE X

X. Auditoría en seguridad física

DIMENSIONES

X1.Activos

X2. Riesgo

VARIABLE Y

Y. Data Center.

DIMENSIONES

Y1. Elementos

Y2. Características

3.7 TECNICAS E INSTRUMENTOS

3.7.1 TÉCNICAS

La técnica utilizada para la investigación fue:

Análisis documental.- Es el conjunto de operaciones (unas técnicas y otras intelectuales) que se realizan para representar tanto la forma como el contenido de documentos primarios, generando de esta forma otros documentos secundarios cuyo objetivo no es otro que facilitar al usuario la identificación precisa y recuperación posterior de los documentos primarios representados, el análisis documental abarca siempre la descripción formal (externo) y la descripción del contenido (interno) del documento.

Un análisis documental se basa en libros, monografías, tesis, revistas, diarios, periódicos u otras fuentes secundarias de información.

3.7.2 INSTRUMENTOS

Ficha bibliográfica. Es un instrumento de registro, de vital importancia porque, entre otras cosas permite acceso a las fuentes consultadas por el autor del trabajo en cuestión.

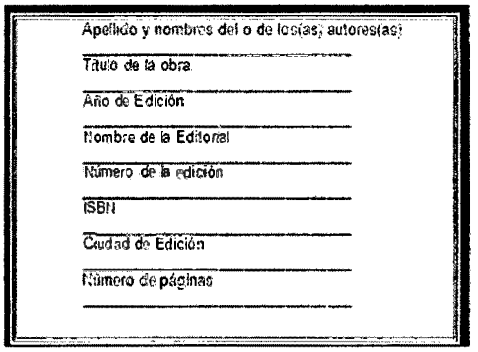


Figura N° 3.1: Formato de una ficha bibliográfica (Elaboración propia)

Reporte de página electrónica. El internet es un medio de comunicación masivo y moderno que nos auxilia en la búsqueda de datos, pero se debe poner más cuidado en la selección de la fuente a consultar, buscando que sea información confiable.

Figura N° 3.2: Dirección de un página electrónica (Elaboración propia)

Ficha hemerográfica. Este documento es una derivación de la ficha bibliográfica en la que se registra información obtenida de publicaciones periódicas (revistas, diarios).

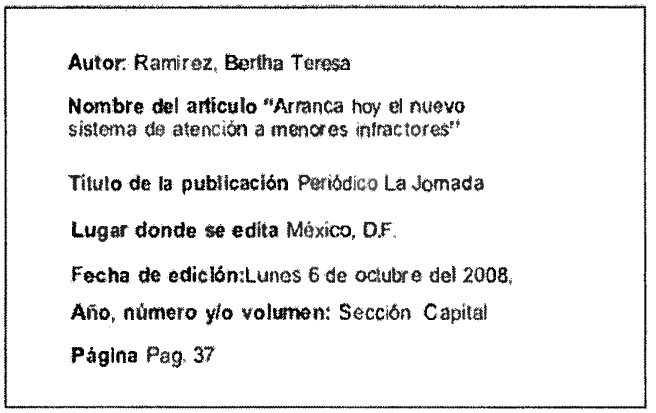


Figura N° 3.3: Dirección de un página electrónica (Elaboración propia)

Referencia. Es una cita de alguna obra donde el lector puede encontrar mayor información de la que se presenta.

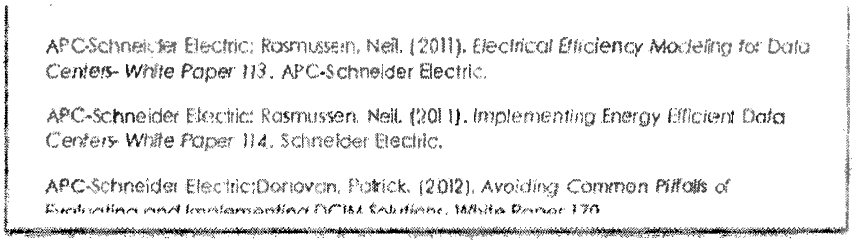


Figura N° 3.4: Referencias bibliográficas (Elaboración propia)

3.7.3 HERRAMIENTAS PARA LA ELABORACIÓN DEL PROCEDIMIENTO

La selección de la herramienta que mejor se adecúe para la elaboración de los procedimientos de la auditoría de seguridad física es una decisión importante, por ello se ha tomado en cuenta las herramientas que más se ajusten al problema de investigación, aquellas que promuevan el respeto a las normas, regulaciones y busquen el mayor beneficio para la institución a auditar.

En función a los aspectos mencionados, se seleccionó los siguientes estándares, marcos de control de TI o normas que se muestra en la tabla 3.1:

ESTÁNDARES	ELABORADO	USO
NTP-ISO/IEC 17799:2007	IDE (comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos)	Proporciona directrices para las normas de seguridad de información de una organización, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente y los riesgos de la seguridad de la información.
COBIT 5.0	ISACA	Ayuda a las organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios, la optimización de los niveles de riesgo y la utilización de los recursos.
TIER	Uptime intitute	Este sistema de clasificación indica el nivel de fiabilidad de un centro de datos asociados a cuatro niveles de disponibilidad. A mayor número en el Tier, mayor disponibilidad, y por lo tanto mayores costes asociados en su construcción y más tiempo para hacerlo.
ISO 19011:2011	ISO (International Organization for Standardization)	Norma internacional que se aplica a todas las organizaciones que requieren llevar a cabo auditorías internas o externas a sistemas de gestión o manejar un programa de auditoría.

Tabla N° 3.1: Herramienta para la elaboración de los procedimientos de auditoría en seguridad física (Elaboración propia)

CAPITULO IV

RESULTADOS DE LA INVESTIGACIÓN

4.1. PROPUESTA DE LOS PROCEDIMIENTOS DE AUDITORÍA EN SEGURIDAD FÍSICA DEL DATA CENTER DE LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA

4.1.1 DESARROLLO DEL ALCANCE DE LA AUDITORÍA

Toda evaluación que tenga el tipo de auditoría, tiene un alcance. Éste está referido a los aspectos, considerados necesarios de cubrir en dicha evaluación para lograr los objetivos de la auditoria.

En esta etapa determinamos el alcance que tendrá la auditoría, el alcance permite aclarar al auditado cuáles son las demarcaciones de la evaluación.

Como aporte, el Auditor, en base a su juicio profesional, puede ampliar y/o disminuir el alcance de la Auditoría.

Es significativo conocer cuáles son los elementos de seguridad física y los elementos ambientales que atentan contra el mismo, que pueden ser auditados, y que ayudan al control de la administración de la seguridad física en un Data Center, a continuación se detallan en las tabla 4.1 y tabla 4.2 los aspectos de seguridad física que pueden ser auditados:

ELEMENTO	DEFINICIÓN
Ubicación	Se recomienda que esté ubicado entre la primera o segunda planta del edificio, que su ubicación no esté señalizada, que no tenga ventanas etc. Es importante considerar también 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, no es recomendable ubicarla en zonas como: • En la última planta (incendios) • En el sótano o plantas bajas (inundaciones) • Cerca de áreas públicas del edificio (alto riesgo en la seguridad)
Estructura	La infraestructura del ambiente del Data Center debe tener: 1. Suelos con alta capacidad de carga. 2. Dobles suelos para evitar riesgos de electrocución y de inundación. 3. Construcción antisísmica en zonas con riesgo de terremotos. 4. Paredes con tratamiento ignífugo y antipolvo. 5. Aislamiento térmico en muros y ventanas. 6. *Falso Piso;* se recomienda que exista un falso suelo o suelo técnico por donde suele discurrir el cableado, suelo que debe ser de material ignífugo o difícilmente inflamable y guardar cierta distancia respecto del suelo real. Asimismo se recomienda limpiar debajo del mismo, que tenga detectores de humedad, un sistema de detección de incendios etc. 7. *Falso techo;* se recomienda que sea de material ignífugo o difícilmente inflamable, que tenga instalado un sistema de detección de incendios etc. 8. *Sala fría;* También denominada "pecera" y nevera es la zona más protegida de todo el centro. 9. Los pasillos y accesos del Data Center deben encontrarse libres para facilitar el desplazamiento del

	personal, para la instalación de nuevos equipos cuando sea necesario y para facilitar la salida de emergencia en caso de evacuación por incidente. 10. La iluminación es importante dentro del Data Center, ya sea para hacer trabajos dentro de él, en caso de vigilancia con las cámaras IP o CCTV y para detectar algún daño físico dentro de los equipos.
Sistema de cableado	Una correcta administración de cable, brinda un servicio que debe ser ordenado y flexible para que facilite la realización de modificaciones o ampliaciones en el Data Center. Para lograrlo se pueden usar: racks y gabinetes (brinda un amplia control de cables en dirección horizontal y vertical); un sistema de tendido de cable (usar el trayecto por debajo del falso piso para el cableado permanente, y el trayecto por encima del piso para el cableado temporal) y etiquetas. Se debe separar los cables de cruzada y datos de los de fibra, ya que la fibra es más frágil y puede sufrir daños.
Señalización	Deberán estar debidamente señalizados los ingresos como salidas, las áreas de alto voltaje o que cuentan con algún riesgo, las vías de evacuación y las salidas de emergencia (esto asegura también la salud y bienestar del personal).
Seguros por robo u otros riesgos.	La contratación de uno o varios seguros de riesgos compensará económicamente o minimizará las pérdidas por desastres ocurridos en uno organización, como pueden ser: incendios, inundaciones, robos, fallos, eléctricos, polvo en el ambiente, etc.
Control de Acceso	i. Deben haber guardias de seguridad. ii. Control de acceso perimetral y zonas interiores (es un conjunto de dispositivos que generan una detección temprana en un perímetro, es decir, una detección que da tiempo al vigilante para la toma de acciones preventivas antes de producirse un hecho delictivo o anómalo) iii. Puertas blindadas en áreas más críticas. iv. Control de acceso personal o electrónico y nuevo control en las distintas dependencias para que ninguna

	persona pueda acceder a una zona para la que no tiene permiso. v. *Alarma contra intrusos;* los sistemas de alarma para centros de datos pueden usar sensores, como las barreras de rayos láser, sensores de pisadas, sensores táctiles, sensores de vibración. Los centros de datos también pueden tener algunas áreas en las que se prefiera una alarma silenciosa en vez de una alarma sonora, para poder atrapar "in fraganti" a los intrusos. vi. *Sistema de vigilancia;* hay que evaluar la posibilidad de instalar cámaras de vigilancia, sensores de control de presencia, vigilancia en circuito cerrado de televisión. vii. *Dispositivos biométricos;* son medidas de seguridad existentes para constituir la mejor práctica en cuanto al control de acceso.
Sistema de red independiente	Un Data Center puede tener un segmento de red propio, independiente al del resto de la institución, con esto evitará problemas que puedan producirse en la red que provengan de otras áreas.

Tabla N° 4.1: Elementas a cansiderar para una adecuada seguridad física en un Data Center (Elabaración prapia)

ELEMENTO AMBIENTAL	EL IMPACTO QUE PUEDE GENERAR EN EL DATA CENTER	MEDIDAS DE SEGURIDAD
Temperatura	El excesivo calor en los equipos electrónicos reduce significativamente la vida útil de sus componentes; el excesivo frío en los equipos produce errores en su funcionamiento.	**Sensores de temperatura:** Dispositivos que detectan fallas en los equipos y disminución de la vida útil de los equipos debido a temperaturas mayores de las especificadas y/o cambios drásticos de temperatura.
Humo/ incendios	Un incendio en un Data Center puede ser producido por un simple corto circuito o ser provocado accidental o intencionalmente. También puede generarse en un ambiente vecino al Data Center. El humo puede producirse cuando existe fuego o incluso si no hay fuego, por ejemplo es posible que dispositivos emanen humo aun cuando no se ha generado llama, como el caso de un cortocircuito en donde los cables al calentarse a elevadas temperaturas comienzan a desprender humo del calentamiento del aislante. Un incendio en un Data Center ocasionaría pérdidas de los bienes y datos; además carga	**Barrera mural**: Su objetivo es impedir durante un período más o menos largo de tiempo que el incendio se propague a sus áreas colindantes. En las separaciones entre edificios, se construyen a la vez que estos y van desde los cimientos hasta sobrepasar la cubierta. Las placas cortafuegos pueden adosarse a muros y pilares de hormigón o metálicos. Están construidas con materiales ignífugos, no inflamables y de gran resistencia al calor. **Puerta cortafuegos:** Su objetivo es impedir la propagación no solo del fuego a zonas colindantes, sino también de humo y gases tóxicos y deben proteger las vías de evacuación. **Compuerta cortafuegos:** Son unos dispositivos que se colocan en las salidas de los conductos de ventilación y aire acondicionado para cerrarse de forma manual o automática en caso de incendio e impedir que el fuego, el humo y los gases se propaguen a otras secciones.

	otras omenozos derivados cama calar, humedad, humo y goses corrasivas. Por esta rozón hosto un pequeña incendia puede provacor grandes doños en los equipos informáticos. Elnfuega y el humo na solo nfectan o las estructuras físicos, equipos u otros elementos de un Dota Center, también pueden ocasionar la muerte de una persona, ya sea par inhalocián de huma o par quemaduras graves.	**Detectores de incendios:** Son unos dispositivas que se instalan normalmente en el techa a en la parte más alta de los muros de las hobitaciones, que son los puntos hacia los que se desplaza el humo, se debe evitar calocarlas en las esquinas, porque el humo llega más torde o esos zanos. **Extractor de humo:** Es uno medida de seguridad que mantiene el oire con un cierto punta de respirabilidad cuanda se ha producido un incendia. **Extictores:** En espaciai físicos dande haya equipamienta infarmático, electrónico o eléctrica están excluidas extintores por agua o espuma, y son recamendobles los de anhídrida carbónica (CO2). Las halones (hidrocorburos halagenados), como agentes extintores, se desaconsejaron en el Protacola de Montreal parque dañan la capa de ozono. **Pictura anti fuego:** Contor can pintura anti fuego en las paredes permitirá disminuir los efectos que se generarían de praducirse un incendio en el Data Center. **Nebulizador de agua:** Las pequeñas gatas que genera este aparato permiten que el agua nebulizada controle, snfaque y suprima incendios mediante: el enfriamiento tanto de la llama como de los goses generados en la combustión; el desplazamienta de oxígeno por evaparación; la otenuoción del calor radiante con las mismas

		pequeñas gotas. **Rociadores:** Son uno de los sistemas de extinción de incendios. Generalmente forman parte de un sistema contra incendio basado en una reserva de agua para el suministro del sistema y una red de tuberías de la cual son elementos terminales. Por lo general se activan al detectar los efectos de un incendio, como el aumento de temperatura asociado al fuego, o el humo generado por la combustión. - Bocas de incendio (toma de agua diseñada para proporcionar un caudal considerable en caso de incendio) equipadas situadas próximas a la entrada del Data Center.
Suministro eléctrico	La energía eléctrica es indispensable para el funcionamiento de los equipos eléctricas a electrónicos de un Data Center, pera las compañías de servicios no pueden asegurar suficiente disponibilidad como se esperaría, pues su interrupción se pueda dar en cualquier momento, ya sean por situaciones inesperadas o no programadas. La interrupción del servicio eléctrico en el Data Center, ocasiana la paralización de sus servicias; la posible presencia de otras dificultades.	**Fluido eléctrico de respaldo:** Dos o más acometidas de red eléctrica de compañías proveedoras, para evitar que un apagón producido en una de ellas pueda comprometer la seguridad de los equipos electránicos e informáticos si el tiempo de desconexión eléctrica superase la capacidad de los UPS y de los grupos electrógenos. **Suministro de Alimentación Interrumpible (UPS):** Es el sistema de alimentación ininterrumpida; cuenta con baterías que almacenan energía. Este dispositivo proporciona energía en caso de emergencia y cuando el generador eléctrico del Data Center falle o no haya energía eléctrica. **Grupos electrógenos y Generadores eléctricos:** Son utilizados

	Los sistemas de alarmas y controles de acceso perimetrales del Data Center dependen también de la energía eléctrica, por lo que su no funcionamiento también puede generar más problemas.	principalmente en aplicaciones denominadas "de emergencia", para paliar los problemas de los cortes de corriente es decir como fuente principal de corriente cuando falla la red eléctrica.
Acandicia-namienta del clima (HVAC- Heating, Ventilation and Air conditionin g)	La climatización es un proceso de tratamiento del aire para establecer las condiciones ambientales apropiadas para distintos fines, mediante el control de la temperatura, humedad, calidad y distribución del aire en un determinado ambiente. El mantenimiento preciso de las condiciones ambientales es muy importante en los espacios del Data Center porque garantizan la integridad de su información y la confiabilidad de la operación de los equipos electrónicos por mucho tiempo.	**Aire Acandicianada de Precisión:** El aire no solo es enfriado, sino también controlan otros factores, como puede ser su pureza, su limpieza. Tiene la exactitud y precisión necesarias para operar en el "modo" requerido (humidificación, enfriamiento o calefacción) y mantener el ambiente dentro de los parámetros recomendados. Cuenta también con elementos como pueden ser filtros de partículas, sensores de humedad, humidificadores y deshumidificadores, etc. **Sistema de aire refrigerado:** Entendemos por sistemas de aire refrigerado los dispositivos que producen aire frío. Estos sistemas no tratan el aire de ninguna otra manera que no sea su enfriamiento. **Sistemas de refrigeración basadas en agua helada:** Estos equipos consiguen altísimas potencias de refrigeración y son usados para Dota Center medianos/grandes y en lugares de alta concentración. **Implementar una configuración de pasillo caliente/pasillo frío:** Existe un método para favorecer la circulación de aire, es conocido como

		"pasillo caliente/pasillo frío". Los racks se disponen en filas alternas de pasillos fríos y calientes. En el pasillo frío los racks se ponen frente a frente y en los pasillos calientes dorso contra dorso. Las placas perforadas en el piso falso de los pasillos fríos permiten que llegue aire frío al frente de los equipos. Lo que realiza el aire frío es envolver el equipo y ser expulsado por la parte trasera hacia el pasillo caliente. Usar racks abiertos en lugar de gabinetes.
Calidad del aire	En el ambiente del Data center se pueden presentar químicos suspendidos en el aire, como producidos por el hidrógeno de baterías en mal estado o originadas por otras partículas, como el polvo. El no tener una adecuada calidad de aire puede praducir situaciones de riesgo para el personal o fallas en los equipos por el aumento de la electricidad estática y la obstrucción de filtros/ventiladores por la acumulación de polvo. Las partículas de polvo también son un gran enemigo de los equipos electrónicos y servidores.	**Detectores de Gases:** Dispositivos que se utiliza para obtener la pureza en el aire, para detectar y medir el monóxido de carbono, el oxígeno, el metano, el sulfuro de hidrógeno y otros gases. **Sensores de polvo:** Este dispositivo detecta las fallas en los equipos debidas al aumento de la electricidad estática y a la obstrucción de filtros/ventiladores por la acumulación de polvo.
Humedad	Un ambiente húmedo puede generar la condensación de agua sobre los componentes	**Humidificadores:** Es el dispositivo empleado para aumentar el grado de humedad del aire.

	electrónicos o mecánicas de los sistemas, generalmente debido a un mal funcionamiento del sistema de refrigeración. El agua condensada puede causar c ɔrtocircuitos en el equipamiento, teniendo camo cansecuencio el mali funcianamiento de sus circuitos e inclusa daños a sus componentes. En los dispositivos mecánicos, la humedad puede generar carrosión, afectar a los lubricantes a inclusa generar esfuerzas innecesarios par aumento de la fricción.	**Deshumidificadores:** Es el dispositivo empleado para reducir la humedad en el ambiente y consiste en una bomba de calor para proporcionor una zona fría donde condensor la humedad y una zana caliente paro recuperar la temperatura ambiental. **Sensores de humedad:** Detectan fallas en los equipos debido a la ocumuloción de electricidad estática en los puntos de baja humedaa formación de condensoción en los puntos de humedad alta.
Filtraciones de agua	El agua puede ser una amenaza para el Dota Center y se presentan par: filtraciones de tuberías que estén por encima del ambiente del Data Center, inundaciones provocodas por fuertes lluvias a aberturas de las bocas de incendios. Las daños provocadas por la presencia de fuga de agua tendrían consecuencias nefastas sobre los equipos intormáticas.	a) Disponer de bombas extractoras de aguo (en caso de ocurrir inundación). b) Cuidar que el alcantarillado cercano a la entidod se encuentra limpio, desatascado y aperativo al cien por cien. c) Verificar que las puertas y ventanas na filtron el agua. Además, las ventanas deben tener un cierre hermético. d) Los elementos del hordware deberán estar alejados de las ventanos y no apoyarse directamente en el suelo. e) Los baños y salidas de agua deben situarse o distancia de las salas que alojen hardware o contor con sistemas de desviación y absorción del ogua en cosa de escapes accidentales y roturas

		d) Sensores de aniego: Estos sensores son colocados en el piso con el objetiva de poder detectar de forma temprana las inundaciones que puedan ocurrir en las instalaciones.
Vibraclanes	Las vibraciones pueden estar originadas por múltiples motivos, incluso por algunos procedentes del interior de las propias instalaciones del Data Center o del exterior (por ejemplo transporte de vehículos pesados). Puede que existan dispositivos internos, como generadores de energía, sistemas de refrigeración o ventiladores que generen vibraciones; es necesario, además, revisar que éstos tuncionan correctamente, ya que si se encuentran en mal estado, puede que aun siendo perfeetamente eficaces, generen una cantidad de vibraciones superior a la normal; los propensos a sufrir daños ante estas acontecimientos son los equipos más sensibles e incluso pueden afectar al mismo personal que labora en el interior del Data Center.	a. Colacar los equipos sensibles a las vibraciones lo más alejado de los elementos que las provoquen. b. Los dispositivos extremadamente sensibles, como discos duros, pueden ser aislados con gomas o capas de goma espuma que amortigüen las vibraciones. c. Sensores de vibración; en Data Center con mucho tráfico, se recomienda colocar un sensor de vibración en cada rack para detectar la instalación o extracción no autorizada de equipos críticos.
Electramag netisma	Los campos electromagnéticos pueden afectar los equipos de TI interfiriendo en su	**Pararrayas:** Los sistemas ele trónicos son muy vulnerables ante una descarga de electricidad estática, por lo que parece evidente que

	funcionamiento y borrando informaciones gravadas en discos y medios magnéticos	la caída de un rayo, que podríamos decir que es la descarga de electricidad estática más potente que podemos encontrar, puede dejarlos del todo inservibles. Es imprescindible que en el propio local donde se encuentre el Data Center o en los alrededores cercanos a éste, esté instalado un pararrayos. **Sistema de conexión a tierra**: Consiste en una pieza metálica (electrodo) enterrada en suelo con resistencia y conentada a una malla. El objetivo de su instalación es: • Seguridad de las personas (garantizar la seguridad al personal durante fallas eléctricas o descargas) • Protección de las instalaciones (disminuye las tensiones de objetos metálicos que se encuentran influenciados por inducciones de objetos energizados o por estática) • Compatibilidad electromagnética (cuando se presenta las descargas atmosféricas, proporcionan un camino seguro para la corriente eléctrica del rayo, manteniendo la equipotencialidad de toda la instalación)
Magnetis-mo	La adecuada ubicación y distribución de los cables eléctricos como de red ayudarán a evitar la interferencia que podría producirse entre ellos, generando pérdida de datos, interferencia en la comunicación o errores en la transmisión.	

Tabla N° 4.2: Elementas Ambientales que pueden afectar la Seguridad Física en un Data Center (Elaboración propia)

4.1.2 DESARROLLO DEL OBJETIVO GENERAL DE LA AUDITORÍA

Conociendo el alcance de la auditoría (delimitada anteriormente) se procede a definir el objetivo de la misma. El objetivo general regula de manera holística lo que se pretende evaluar, este será complementado por los objetivos específicos denominados por la ISO 19011 como criterios de auditoría (como se verán más adelante).

La auditoría a la que va dirigido el presente trabajo de investigación es eminentemente el de verificar la seguridad física del Data Center de la Municipalidad de Huamanga.

Siendo el Data Center el objeto de auditoría, algunos factores que podrían estar involucrados en la evaluación son las siguientes:

- El mandato y el cometido de una de las tres entidades: Control Interno, Gerencia General o Controloría General de la República (si la empresa a auditar es del Estado)
- Políticas y procedimientos internos.
- Leyes y regulación interna pertinentes a la Municipalidad.
- Efectuar un seguimiento con las recomendaciones dadas en anteriores evaluaciones (auditorías pasadas)

Estos factores podrían influir en la determinación del objetivo de la auditoría.

4.1.3 PLANIFICACIÓN DE LA AUDITORÍA

En esta etapa se conoce a grandes rasgos el área a auditar (Data center de la Municipalidad) y la asignación de recursos necesarios para la ejecución de la auditoría.

4.1.3.1 CONOCIMIENTO PRELIMINAR DEL ÁREA A AUDITAR

Para conocer un poco del área a auditar podemos recurrir a diferentes fuentes de información como:

- Evaluaciones de riesgos precedentes.
- Información de auditorías previas.
- Entrevistas con los actores involucrados.

- Revisión de documentación proporcionada por la institución.

Una vez finalizada esta actividad se tendrá un conocimiento global del área a auditar, que en este caso es el Data Center de la Municipalidad. El auditor puede documentar esta actividad, realizando un registro de los aspectos más relevantes, para este registro no se plantea un formato particular, sino que será a criterio del auditor.

4.1.3.2 ANÁLISIS DE RIESGO

La realización del Análisis de Riesgos, permite identificar los principales riesgos a los que están expuestos los activos en relación directa con la seguridad física de un Data Center y permite conocer también su situación actual, por tanto para realizar el análisis de riesgo nos basados en el capítulo II, título 2.2.1.4.1 del presente trabajo de investigación:

4.1.3.2.1 IDENTIFICAR LOS ACTIVOS

Se identifican los activos físicos que se encuentran en el Data Center de la Municipalidad, dichos activos serán ubicados en la tabla "Activos físicos de un Data Center" (ver anexo A, tabla A.1).

4.1.3.2.2 REALIZAR LA TASACIÓN DE LOS ACTIVOS

La tasación de activos y la calificación se hará en términos de la "disponibilidad", dado que se evalúa la seguridad física del Data Center de la Municipalidad. El criterio de la calificación se da según la tabla A.3 (Anexo A) aplicando la pregunta ¿Cómo una pérdida o falla en un determinado activo afecta su disponibilidad? "Los valores asignados a la disponibilidad de cada uno de los activos se deducen del análisis de la importancia de dicho activo para la realización de las funciones o procesos indispensables para las actividades que realiza la entidad auditada. Este criterio se fundamenta en el análisis de impacto al negocio. Estos parámetros corresponden al criterio del auditor con la ayuda del análisis de impacto al negocio" (Llerena, 2013).

En la tasación de activos trabajaremos con la tabla A.2 (Anexo A).

4.1.3.2.3 IDENTIFICACIÓN DE LAS AMENAZAS Y VULNERABILIDADES

Se procede a identificar las amenazas y vulnerabilidades que se presenten en el Data Center de la Municipalidad mediante entrevistas u observaciones, es decir todas aquellas que pueden afectar su normal funcionamiento en relación directa con la seguridad física (para ellos nos apoyaremos en los elementos de seguridad física de la tabla 4.1 y tabla 4.2)

4.1.3.2.4 CÁLCULO DE LAS AMENAZAS Y VULNERABILIDADES

Identificadas las amenazas y vulnerabilidades en el Data Center de la Municipalidad, se procede a realizar la estimación de la probabilidad de las amenazas. Para determinar la "probabilidad de ocurrencia de una amenaza frente a una vulnerabilidad" (ver tabla A.4 del Anexo A), se debe analizar las vulnerabilidades que pueden ser explotadas por alguna de las amenazas identificadas, esta estimación se determina en base a la escala de Likert (tabla 2.1).

4.1.3.2.5 ANÁLISIS Y EVALUACIÓN DE RIESGO

En este punto se procede a valorar el riesgo; para ello haremos uso de la "Matriz de riesgo" (ver tabla A.5 del anexo A):

Los activos identificados anteriormente se colocarán en la columna "Activos". Los valores obtenidos en la tasación de cada uno de los activos en base a la importancia que representa en términos de disponibilidad, se ubicarán en la matriz de riesgos en la columna "Impacto" (consideremos que el impacto va ligado con la disponibilidad del activo). Para valorar el riesgo multiplicamos el impacto por la probabilidad. Una vez obtenido la valoración del riesgo, se identificará aquellos que tienen mayor riesgo en el Data Center, y procede a priorizarlos de mayor a menor.

Por último presentar las conclusiones del análisis de riesgo y las acciones a tomar en cuenta (ésta puede estar incluida en la etapa de la documentación de conclusiones de la auditoría).

4.1.4 DEFINICIÓN DE LOS CRITERIOS A SEGUIR EN LA AUDITORÍA

Partiendo de los objetivos y alcance previstos y considerando toda la información obtenida, se procederá a escoger los criterios que serán planteados según la norma NPT-ISO/17799:2007, el marco de control COBIT 5.0, la clasificación y estándar internacional TIER; todos éstos enfocados en los aspectos de seguridad física y así dar inicio a la elaboración del cuadro de criterios (ver el anexo B).

4.1.5 LEVANTAMIENTO Y/O RECOLECCIÓN DE EVIDENCIAS PARA LA AUDITORÍA

En esta etapa de la auditoría es preciso buscar los medios o caminos por las cuales se podrá realizar el levantamiento de evidencias. Para esta intención se tiene en cuenta los siguientes aspectos:

De acuerdo a los criterios que hayan sido elegidos para dar inicio a la auditoría, según TIER, COBIT 5.0 o la norma 17799, será necesario evaluar los controles relacionados a ellos y con ello proceder con el levantamiento de evidencias.

Una vez seleccionados los controles a evaluar se procede a la recolección y evaluación de evidencias, para lo cual será necesaria la clasificación de los controles:

CONTROLES	
No existentes	**Existentes**
Son necesarios aplicarlos pero al realizar la auditoria podrían no ser identificados.	Son identificados al momento de realizar la auditoria y requieren ser evaluados para verificar si cumplen con su funcionamiento.

Tabla N° 4.3: Clasificación de los controles (Elaboración Propia)

El auditor puede hacer uso de alguna de las siguientes técnicas para evaluar los controles existentes.

- Observación
- Indagación: entrevistas las cuales deben tener una naturaleza de descubrimiento no de acusatoria), cuestionarios.

- Inspección
- Investigación analítica: Evaluar tendencias.
- Conciliación; contrastar la información con personas o documentos, como pueden ser:

  ✓ Sistema de gestión de incidentes y problemas (es una herramienta importante, pues maneja los eventos que se dan en el día a día en la institución, es el activo más cercano y constante que dará información certera y directa de cómo reacciona toda la infraestructura del Data Center ante los incidentes o problemas que pudiera ocasionarse en el flujo normal de las actividades de la Municipalidad)

  ✓ 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)

  ✓ 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, unos serán planificados y realizados constantemente y otros serán para realizar correcciones)

  ✓ Dependencia de proveedores (si estos controles dependen los servicios brindados por proveedores, es importante conocer los niveles de servicio que han sido establecidos y verificar que aseguran un correcto nivel de protección de seguridad física)

  ✓ Los reportes de auditorías pasadas en relación a seguridad física.

  ✓ Revisión de documentos acerca de la seguridad física.

Al realizar la recopilación de información para la evidencia tener en cuenta:

- Depurar toda la información recopilada que no es de nuestro interés.
- Calificación de la persona que suministra la información o evidencia, que tenga un buen entendimiento del área técnica que está en revisión, de lo contrario la información recopilado puede ser no confiable.
- Objetividad de lo evidencio: lo evidencia se debe entender sin ningún tipo de explicación o interpretación.
- Todo lo información obtenida debe ser manejado de formo confidencial y ética.

4.1.6 DOCUMENTACIÓN DE HALLAZGO

Los hallazgos de auditoría examinan los resultados de lo evaluación de la recopilación de las evidencias de lo auditoría frente a los criterios de auditoria.

Las evidencias a buscar poro lo obtención de los hallazgos deben ser objetivas, los cuales corresponden ser evaluados siguiendo los criterios de auditoría definidos precedentemente.

Figura N° 4.1: Ilustración de un hallazgo (Elaboración Propio)

Como resultado de lo evaluación de las evidencias, se podría encontrar los siguientes escenarios:

1. **No tiene evidencia:** Se presenta cuando el auditor no pudo obtener una manera de relacionar un criterio con la respectiva evidencia a pesar de haberse aplicado los mecanismos de levantamiento necesarios.
2. **Se tiene evidencia:** Es este caso el auditor cuenta con la evidencia necesaria y razonable para relacionarlo con un criterio. Los hallazgos de auditoría obtenidos en este caso pueden indicar tanto:
   a. **Cumple el criterio:** Cuando el criterio en su totalidad, es atendido por controles o procesos los cuales pueden ser corroborados por las evidencias respectivas.
   b. **Cumple parciamente el criterio:** Cuando las evidencias nos permiten determinar que el criterio está siendo asistido no en su totalidad, sino en un porcentaje que será dispuesto a juicio del auditor.
   c. **No cumple con el criterio** Cuando las evidencias obtenidas revelan que el criterio evaluado no se está insertado en su totalidad.

Para documentar un hallazgo se puede tener en cuenta la relación de la evidencia, el criterio, el hallazgo, y las recomendaciones. El documentar un hallazgo nos permite planificar las actividades de carácter correctivo que se consideren convenientes para subsanarlas.

4.1.7 DOCUMENTACIÓN DE LAS CONCLUSIONES Y RECOMENDACIONES

La última etapa para la culminación con el informe de auditoría son los resultados, para ello se documentan las conclusiones y las recomendaciones generales, y éstas deben:

- Incluir comentarios positivos y constructivos.
- Cubrir no solamente las no conformidades a partir de los hallazgos, sino también las oportunidades que se puedan presentar como un medio de mejora y cambio de acciones.

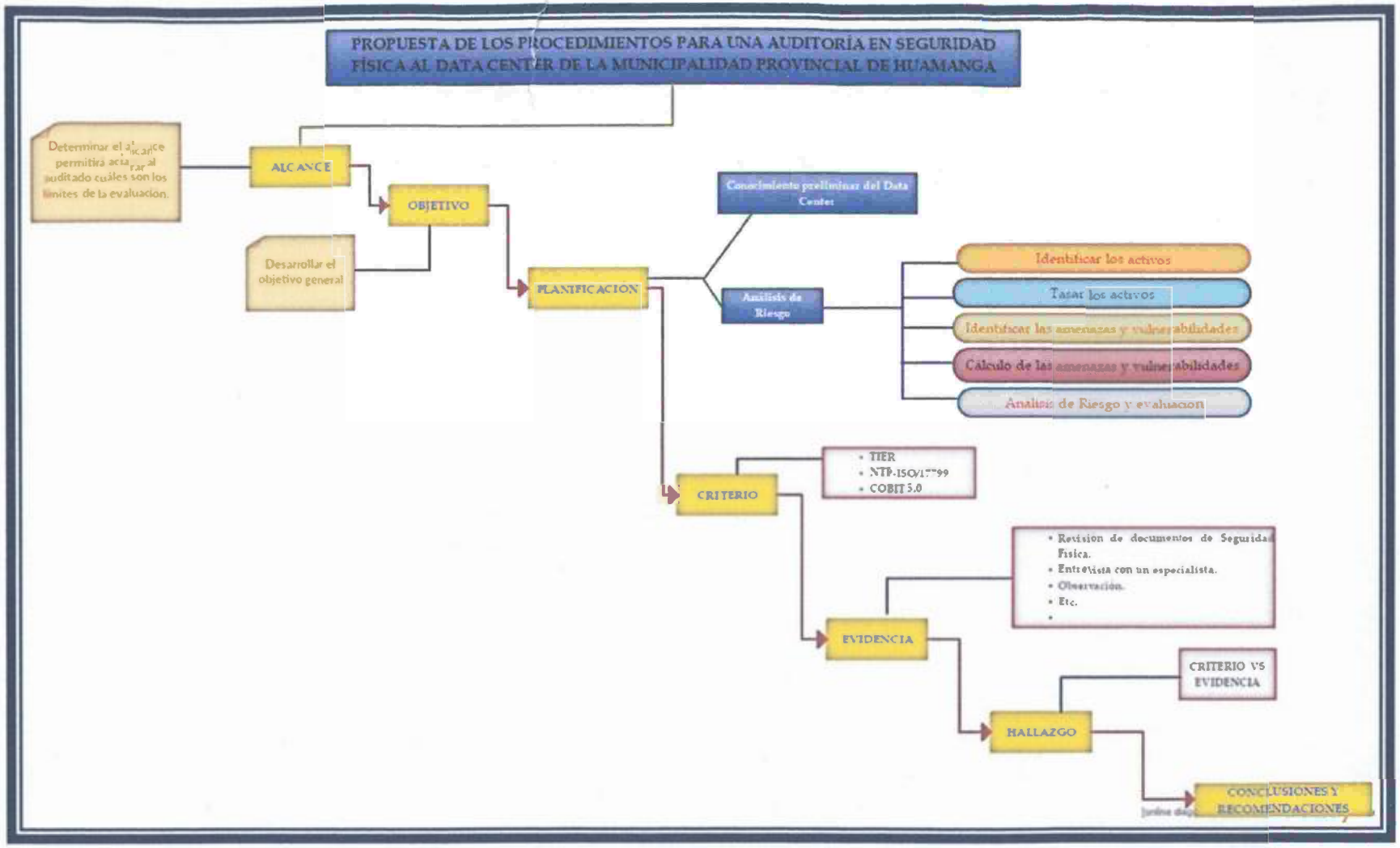


Figura N° 4.2: Estructura de la propuesta de los procedimientos de Auditoría en Seg. Física (Elaboración Propia)

4.2 APLICACIÓN DE LA PROPUESTA DE LOS PROCEDIMIENTOS

En esta sección se presenta la aplicación de la propuesta de los procedimientos de auditoría en seguridad física para la "Municipalidad Provincial de Huamanga", con la finalidad de que se sustente las pruebas realizadas a los procedimientos de auditoría antes detallados en el presente trabajo de investigación.

4.2.1 ALCANCE

- La auditoría abarcará todo el Data Center de la Municipalidad Provincial de Huamanga, que está ubicada en el local central de dicha institución, considerando los lineamientos de seguridad física que posee su Data Center, teniendo como guía:
    - ✓ NTP-ISO/IEC 17799:2007 (dominio 9 concerniente a las seguridad física y ambiental)
    - ✓ El marco de control COBIT 5.0 (Procesos habilitadores relacionados a la seguridad física)
    - ✓ Clasificación y estándar internacional TIER (requerimientos de TIER I y TIER II; el Data Center de la Municipalidad según los lineamientos generales de la tabla N° 2.2 solo puede ubicarse en el nivel 1 o 2)
- Se tomarán en cuenta los elementos de seguridad física de las tablas 4.1 y 4.2 para el análisis de riesgo.
- El periodo de visita a las instalaciones del Data Center comprende el 04 y 05 de Agosto del 2015, previo acuerdo con el jefe de la Sub Gerencia de Sistemas de la Municipalidad.

4.2.2 OBJETIVO GENERAL

Realizar la evaluación de la infraestructura del Data Center de la Municipalidad para verificar la disposición de la seguridad física con la que cuenta sus instalaciones actualmente.

4.2.2 PLANIFICACIÓN

4.2.2.1 CONOCIMIENTO PRELIMINAR DEL DATA CENTER DE LA MPH

DATOS GENERALES DE LA ENTIDAD A AUDITAR	
Nombre la institución :	Municipalidad Provincial de Huamanga
Área a auditar :	Data Center
Responsable:	Sub Gerencia de Sistemas y Tecnología
Administrador del Data Center:	Bach. Yuri Hinostroza Fernández
Auditor :	Bach. Melissa Huerta Aranda
Personal de Apoyo:	Lic. Cinthya Barraza Torres

Tabla N° 4.4: Datos generales de la Municipalidad (Elaboración propia)

Materiales para la ejecución de la auditoría:

Tablet, carpeta de trabajo, cámara digital.

Entrevista realizada al administrador del Data Center:

- **¿Qué servicios brinda el Data Center a toda la Municipalidad? ¿Su funcionamiento tiene que ser las 24 horas y todos los días de la semana?**

  El Data Center alberga los sistemas de información de planilla de pagos, el SIAF (Sistema Integrado de Administración Financiera del Estado) y el de Catastro. El servicio sola abarca al lacal central y actualmente se viene trabajando para la modificación del Data Center con la intención de ampliar el servicio a otros locales (coma los locales que se hallan en el jr. Libertad).

  El funcionamiento del Data Center es requerida de manera crítica los días laborales (lunes a viernes y en horarios de oficina)

- **¿Existen políticas y procedimientos formales, normas de seguridad en el Data Center?**

  No se cuenta con ninguna documentación de políticas ni de normas de seguridad para el Data Center.

- **¿Tienen documentación sobre construcción y preinstalaciones?**

  Si, el Data center fue implementado hace cuatro años previa aprobación de un proyecto, en cuya documentación se hayan las especificaciones técnicas de los equipos a adquirir en ese entonces; la construcción del local no fue contemplado, el sótano fue el ambiente asignado, éste era el único lugar disponible para la implementación del Data Center.

- **¿Cuentan con contratos de seguros de riesgo y mantenimiento de equipos con proveedores?**

  No, no se cuenta con ningún seguro de riesgo y no se realiza mantenimiento a los equipos, ésta se da cuando ocurre un problema.

4.2.2.2 ANÁLISIS DE RIESGO DEL DATA CENTER DE LA MUNICIPALIDAD PROVINCIAL DE HUAMANGA

Realizamos el análisis de riesgo siguiendo los pasos establecidos en la propuesta de los procedimientos de la sección 4.1.3.2:

1. **IDENTIFICACIÓN DE ACTIVOS ENCONTRADOS EN EL DATA DE LA MUNICIPALIDAD (IDENTIFICAMOS LOS ACTIVOS POR OBSERVACIÓN Y ENTREVISTA)**

ACTIVOS DEL DATA CENTER DE LA MPH			
GRUPO	**EQUIPO POR UNIDAD INFORMÁTICA**	**CANTIDAD**	**CARACTERÍSTICA/ DESCRIPCIÓN**
Sala de servidores	Servidores	08	Se cuenta con servidores de base de datos, servidor del SIAF y de Catastro.
	Líneas Telefónicas	03	Características comunes
	Central Telefónica	01	Contenedor donde se alberga el equipo de conmutación y los demás equipos necesarios para la operación de las llamadas telefónicas
	Dispasitivas de almacenomiento (disco duro externo)	01	Disco duro portátil de 2,5" de 500 Gb.
	Racks	03	Saporte metálico que alberga a los servidores y equipos de comunicación.
	UPS	04	Potencia de 1000 VA y 5000 VA.
	Regulador de energía	01	Dispositivo electrónico diseñado para mantener un nivel de tensión constante.

	Gabinete de pared	01	Gabinnte de pared 12 RU 60x53x53 color negro con ventilador.
	Aire acondicionado	01	Aire acondicionado con medidor dertemperatura, humedad de ambiente, sonido silencioso
	Laptop	01	Procesador Core 2 Duo, 2.33 Ghz, Memoria Ram 2GB, disco duro de 160 GB, 15.4".
Equipos de red	Switches	04	02 de 24 puertos y 02 de 16 puertos Gigabit Auto-MDIX y de Auto – Negociación a 10/100/1000 Mbps. 2 ranuras Mini-GBIC 1000 Bases-SX/LX
	Routers	04	4 puertos LAN Auto MDIX a 0/100/1000 Mbps de un gigabit y 1 puerto WAN (iuternet). Cobertura hasta 150 metros (500 pies) bajertecho.
	Putch panels	03	Cat. 6 Mod. 24 puertos color negro
	Cables de red		De cuteg ɔría 5 y utras de cutegoría 6.

Tabla N° 4.5: Activos físicas del Data Center de la Municipalidad (Elaboración Propia)

2. TASACIÓN DE ACTIVOS

Para lo tasación se realizó la pregunta ¿Cómo la pérdida o falla del activo físico afecta su disponibilidad, y cómo afenta esto en los servicios que brinda el Data Center?; para esta evaluación se utillzó la tabla A.3 (del anexo A):

N°	ACTIVOS FÍSICOS DEL DATA CENTER	VALOR DEL ACTIVO
1	Servidores	**5**
2	Cable de red	**3**
3	Líneas Telefónicas	**1**
4	Central Telefónica	**3**
5	Dispositivas de almacenamiento (discos externo)	**5**
6	Racks	**2**
7	UPS	**5**
8	Regulador de energía	**5**
9	Gabinete de pared	**2**
10	Aire acondicionada	**5**
11	Laptop	**3**
12	Switches	**4**
13	Rauters	**4**
14	Patch panels	**3**

Tabla N° 4.6: Tasación de Activos físicos del Data Center de la Municipalidad (Elaboración propia)

3. IDENTIFICACIÓN DE LAS AMENAZAS Y VULNERABILIDAD

N°	AMENAZAS
1	Temperatura inadecuada
2	Presencia de humedad.
3	Falta de refrigeración y fallas de circulación de aire
4	Acceso del personal no autorizado
5	Incendias
6	Pérdida de energía (apagones)
7	Filtracianes de agua (por lluvias, tuberías averiadas, etc) e inundación
8	Sismos de baja y media intensidad
9	Huelgas, vandalismo.
10	Polvo
11	Error humana
12	Cantaminantes de gases y partículas
13	Vibracianes provocados por ruidas

Tabla N° 4.7: Amenazas para el Data Center de la Municipalidad (Elaboración Propia)

VULNERABILIDADES
Infraestructura ubicada en el sótano.
Espacio y distribución de equipos na diseñados correctamente.
Paralización del aire acandicionada por pérdida de energía.
Desagües y alcantarillados cercanas al Data Center, sin inspección.
Racks no sujetos al pisa (sin amortiguadores)
Na existe generador eléctrico u otro equipo en casa de la superación del tiempo de los UPS
Falta de mantenimiento periódica de los UPS.
Existe material inflamable en la entrada del Data Center.
Extintores de incendia vencidas y ubicados a una altura de difícil accesa en casa de emergencia.
Alarma de intrusos desactivada (Par descoordinación)
Paredes sin protección contra la humedad.
Paredes revestidos sin elementas ignífugos
Aire acondicionado can antecedentes de fallas.
Puerta del sótano sensible a actas violentos.
Paredes sin condiciones de estabilidad térmica.
Paredes y techos na sellados ni pintados can un material de reducción y aparición de palvo.
No existe un dispasitivo de detección de polvo.
Elementos almacenadas en la entrada del sótano (cajas de cartón, armarios de madera, planchas de triplay) sensibles a desprender fibras o palva al ser manipulados.
Administrador del Data Center can excesa de trabaja
Personal can insuficiente formación en administración técnica del Data Center, sensible a cometer negligencia o

equivacacianes.
No existen detectores de gases.
No existe sistema de circuito cerrado de televisión.
Equipos de aire acondicionado de "confort", sensible a fallas.
Detector de humo instalado, sin pruebas periódicas.
Infraestructura del Data Center ubicada en el local central de la Municipalidad.
Falta de mantenimiento y limpieza frecuente en el local y equipos del Data center.
No existen bocas de incendio equipadas próximas a la entrada del Data Center.
Falso pisa can acumulación de polvo y residuos plásticos.

Tabla N° 4.8: Vulnerabilidad halladas en la Municipalidad (Elaboración Propia)

4. CÁLCULO DE LAS AMENAZAS Y VULNERABILIDAD

N°	AMENAZAS	VULNERABILIDADES	PROBABILIDAD DE OCURRENCIA	TOTAL
1	Temperatura Inadecuada	Aire acandicionado can antecedentes de fallas.	3	10
		Paralización del aire acondicianada por pérdida de energía.	4	
		No contar can paredes con estabilidad térmica.	1	
		Equipos de aire acandicionado de "confort" sensible a fallas.	2	
2	Presencia de Humedad	Paredes sin protección contra la humedad.	2	2
3	Falta de refrigeración y a fallas de circulación de aire	Espacia y distribución de equipos no diseñados correctamente.	2	12
		Aire acondicianado con antecedentes de fallas.	3	
		Falso piso can acumulación de polvo.	3	
		Falta de mantenimiento y limpieza frecuente en el local y equipos del Data center.	4	
4	Acceso del personal na autorizada	Alarma de intrusos desactivado.	4	6
		No existe sistema de circuito cerrado de televisión.	2	
5	Incendios	Existe material inflamable en la entrada del Data Center.	3	17
		Paredes revestidos sin elementos ignífugos	2	
		Extintares de incendio vencidos y ubicados a una altura de difícil acceso en caso de emergencia.	4	
		Falso piso can residuos plásticas.	1	

		Detectar de huma instalado, sin pruebas periódicas.	4	
		No existen bocas de incendio equipadas próximas a la entrada del Data Center	3	
6	Pérdida de energía	Na existe generadar eléctrico u otro equipa en casa de la superación del tiempo de los UPS	5	9
		Falta de mantenimiento periódica de los UPS.	4	
7	Filtraciones de agua (por lluvias, tuberías, etc) e inundación	Infraestructura ubicada en el sótano.	5	9
		Desagües y alcantarillados cercanos al Data Center, sin inspección.	4	
8	Sismos de baja y media iótensidad	Racks na sujetas al pisa	3	3
9	Huelgas, vandalismos.	Puerta del sótano sensible a actos violentos.	2	6
		Infraestructura ubicada en el local central de la Municipalidad.	4	
10	Polvo	Paredes y techas no sellados ni pintados con un material de reducción y aparición de polvo.	2	17
		Na existe un dispositiva de detección de polvo.	2	
		Elementas almacenados en la entrada del sótano sensibles a desprender polvo al ser manipulados.	4	
		Falso piso con acumulación de polvo.	4	
		Falta de mantenimiento y limpieza frecuente en el local y equipos del Data center.	5	

11	Error humano	Administrador del Data Center con exceso de trabajo.	4	8
		Personal de administración del Data Center con insuficiente formación técnica, sensible a cometer negligencia o equivocaciones.	4	
12	Contaminantes de gases y partículas	Falta de mantenimiento periódico de los UPS (contaminación por gases emanados de las baterías)	2	7
		Elementos almacenados en la entrada del sótano (cajas de cartón, armarios de madera, planchas de triplay) sensibles a desprender fibras al ser manipulados.	4	
		No existen detectores de gases.	1	
13	Vibraciones provocados por ruidos	Aire acondicionado con antecedentes de fallas.	1	3
		Falta de mantenimiento en los equipos del Data center.	2	

Tabla N° 4.9: Cálculo de la prababilidad de que una amenaza explate una vulnerabilidad del Data Center de la Municipalidad (Elabaración Prapia)

5. ANÁLISIS DE RIESGO

MATRIZ DE RIESGOS		Temperatura Inadecuada	Presencia de Humedad	Falta de refrigeración y falla de circulación de aire	Acceso del personal no autorizado	Incendios	Pérdida de energía	Filtración de agua e inundación	Sismos de baja y media intensidad	Huelgas, vandalismos.	Polvo	Error humano	Contaminantes de gases y partículas	Vibraciones por ruidos
Probabilidad de la amenaza		**10**	**2**	**12**	**6**	**17**	**9**	**9**	**3**	**6**	**17**	**8**	**7**	**3**
Activo	**Impacto**	**MEDICIÓN O VALORACIÓN DEL RIESGOS**												
Servidores	**5**	50	10	60	30	85	45	45	15	30	85	40	35	15
Cables de red	**3**	30	6	36	18	51	27	27	9	18	51	24	21	9
Líneas Telefónicas	**1**	10	2	12	6	17	9	9	3	6	17	8	7	3
Central Telefónica	**3**	30	6	36	18	51	27	27	9	18	51	24	21	9
Dispositivos de almacenamiento (discos	**5**	50	10	60	30	85	45	45	15	30	85	40	35	15

externo)														
Racks	2	20	4	24	12	34	18	18	6	12	34	16	14	6
UPS	5	50	10	60	30	85	45	45	15	30	85	40	35	15
Regulador de Energía	5	50	10	60	30	85	45	45	15	30	85	40	35	15
Gabinete de pared	2	20	4	24	12	34	18	18	6	12	34	16	14	6
Aire acondicionado	5	50	10	60	30	85	45	45	15	30	85	40	35	15
Laptop	3	30	6	36	18	51	27	27	9	18	51	24	21	9
Switches	4	40	8	48	24	68	36	36	12	24	68	32	28	12
Routers	4	40	8	48	24	68	36	36	12	24	68	32	28	12
Patch panels	3	30	6	36	18	51	27	27	9	18	51	24	21	9

Tabla N° 4.10: Matriz de riesgos del Data Center de la Municipalidad (Elaboración propia)

PRIORIZACIÓN DE LOS RIESGOS:

La prioridad se estableció en función de los resultados que se obtuvo en la "Matriz de riesgos", las amenazas pueden ser priorizadas en orden (de mayor a menor) con base en su foctor de exposición al riesgo.

AMENAZAS	Incendios	Polvo	Falta de refrigeración y fallas de circulación de aire	Temperatura inadecuada	Pérdida de energía	Filtración de agua e inundación	Error humano	Contaminantes de gases y partículas	Acceso del personal no autorizado	Huelgas, vandalismos	Sismos de baja y media intensidad	Vibraciones por ruidos	Presencia de Humedad
PRIORIZACIÓN	1	1	2	3	4	4	5	6	7	7	8	8	9
ACTIVOS													
Servidores	85	85	60	50	45	45	40	35	30	30	15	15	10
Dispositivos de almacenamiento (discos externo)	85	85	60	50	45	45	40	35	30	30	15	15	10
UPS	85	85	60	50	45	45	40	35	30	30	15	15	10
Regulador de Energía	85	85	60	50	45	45	40	35	30	30	15	15	10
Aire acondicionad	85	85	60	50	45	45	40	35	30	30	15	15	10

o													
Switches	68	68	48	40	36	36	32	28	24	24	12	12	8
Routers	68	68	48	40	36	36	32	28	24	24	12	12	8
Cables de red	51	51	36	30	27	27	24	21	18	18	9	9	6
Central Telefónica	51	51	36	30	27	27	24	21	18	18	9	9	6
Laptop	51	51	36	30	27	27	24	21	18	18	9	9	6
Patch panels	51	51	36	30	27	27	24	21	18	18	9	9	6
Racks	34	34	24	20	18	18	16	14	12	12	6	6	4
Gabinete de pared	34	34	24	20	18	18	16	14	12	12	6	6	4
Líneas Telefónicas	17	17	12	10	9	9	8	7	6	6	3	3	2

Tabla N° 4.11: Priarización de las riesgas del Data Center de la Municipalidad (Elaboración Propia)

4.2.3 CRITERIOS A SEGUIR EN LA AUDITORÍA

Los criterios usados son los relacionados:

- Dominio 9 de la NTP-ISO/IEC 17799:2007 (refiérase 9.1.1, 9.1.2, 9.1.4, 9.1.5, 9.1.6, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.6, 9.2.7)
- El marco de control COBIT 5.0 (refiérase EDM01, APO01.02, APO01.07, APO07.01, APO10.03, APO12.05, BAI03.07, BAI03.08, BAI06.02, DSS01.04, DSS02.04, DSS02.05, DSS04.01, DSS04.07, DSS05.05, DSS05.07)
- Clasificación y estándar internacional TIER (requerimientos de TIER I y TIER II definidos para cada subsistema: telecomunicaciones, arquitectura, eléctrico, mecánico) y los requerimientos generales de TIA 942.

4.2.4 LEVANTAMIENTO DE EVIDENCIAS Y DOCUMENTACIÓN DE HALLAZGO

Para el levantamiento de evidencias de los controles existentes identificados en el Data Center de la MPH, se utilizaron las siguientes técnicas:

- Entrevista (realizado al administrador del Data Center)
- Observación (según el Anexo C)

El Data Center no cuenta con ninguna información documentada por lo que, para el levantamiento de evidencia no se recurrió a la técnica de conciliación (sugerida en el apartado 4.1.4 del presente capítulo).

Categoría 9.1 "Áreas Seguras"

CONTROL	9.1.1. PERÍMETRO DE SEGURIDAD FÍSICA	EVIDENCIA	CUMPLIMIENTO (30%)	FALLA/GO	RECOMENDACIONES
Objetivo	Establecer perímetros de seguridad para una mayor protección(como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción para proteger el local del Data Center)				
Solidez física Comprobar que el perímetro del Data Center tiene solidez física (por ejemplo no tendrá zonas que podrá derribarse fácilmente).		La infraestructura es de material noble, y éste es sólido.	**Cumple** ✓		
Área de recepción manual Comprobar que exista un área de recepción manual u otros medios de control del acceso físico al Data Center. Dicho acceso restringe solo al personal autorizado.		No existe ningún área de recepción manual para el Data Center.	**No cumple** X	Data Center sin ningún puesto de recepción manual	Tener un control de recepción manual manejado por la sub gerencia, para registrar la fecha y hora del ingreso de personas al Data Center que sean ajenas a la institución.
Barreras físicas Verificar que existen barreras físicas extendidas desde el suelo real al techo real, para evitar entradas no autorizadas o contaminación del entorno.		No existen barreras físicas, porque el Data Center fue adecuado en una infraestructura ya existente.	**No cumple** X	Data center sin barreras físicas en su construcción.	Se recomienda si en un futuro se decide realizar la migración de todo el Data Center a una infraestructura nueva, se debe tener en cuenta la construcción de barreras físicas.
Puerta para incendios Constatar que las puertas para incendios tienen alarma, que son monitoreadas.		Na existe el control	X		En una infraestructura nueva, contemplar también la instalación de puertas para incendios con sus respectivas alarmas.

Detección de intrusos Verificar la instalación de sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales.	Existe una alarma de detección de intrusos alineada con estándares locales (pero el mayor tiempo se encuentra desactivado por descoordinaciones)	**Cumple parcialmente** ✓	Detector de alarma instalada pero sin funcionamiento.	Corregir las descoordinaciones por la que la alarma de intrusos se encuentra desactivado lo más antes posible.

Tabla N° 4.12: Levantamiento de evidencias y hallazgo del Data Center de la MPH de los "perímetro de seguridad física" (Elaboración propia)

CONTROL	9.1.2. CONTROLES FÍSICOS DE ENTRADAS	EVIDENCIA	CUMPLIMIENTO (50%)	HALLAZGO	RECOMENDACIONES
Objetivo	Proteger el Data Center por controles de entrada adecuados que aseguren el permiso de acceso sólo al personal autorizado.				
Supervisar visitas Verificar que se supervise las visitas al Data Center, a menos que el acceso haya sido aprobado previamente, y se deba registrar la fecha y momento de entrada y salida.		Las visitas se realizan en compañía del personal; y para esto se realiza una solicitud previa al ingreso del Data Center, pero no existe un registro de fecha/hora de ingreso y salida de las visitas.	**Cumple parcialmente:** ✓	La solicitud al ingreso del Data Center no detalla el día ni la hora de la visita, siendo este documento insuficiente para la supervisión de visitas.	Este control también se puede manejar con el registro de recepción de manual.
Acceso al Data Center Comprobar que se controla y restringe solo al personal autorizado el acceso al Data Center.		Se ingresó al Data Center mediante una cerradura electrónica (cuya clave solo maneja la jefe y administrador)	**Cumple** ✓		

Personal identificado visiblemente Constatar que se exija a todo el personal que lleve puesta alguna forma de identificación visible y se le solicite a los extraños no acompañados y a cualquier que no lleve dicha identificación visible, que se identifique.	No hay exigencia de ninguna identificación.	**No cumple** X	Personal no identificado visiblemente, puede generar confusión con personas ajenas.	Se recomienda tener al personal identificado visiblemente, con el uso de medios de identificación como: gafetes, fotosheck, etc; y también a las personas que visitan el Data Center.

Tabla N° 4.13: Levantamiento de evidencias y hallazgo del Data Center de la MPH de los "controles físicos de entradas" (Elaboración propia)

CONTROL	9.1.4. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	EVIDENCIA	CUMPLI-MIENTO (75%)	HALLAZGO	RECOMENDACIONES
Objetivo	Designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.				
Premisas vecinas Comprobar que se consideró cualquier amenaza de seguridad presentada por premisas vecinas, como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.		El administrador asegura que hasta la fecha no se tuvo ningún indicio de presencia de amenazas vecinas.	**Cumple** ✓		

Evitar daños Verificar que se consideraron las siguientes pautas para evitar daño por parte del fuego, inundación, temblores, explosiones, malestar civil y otras formas de desastre natural o humana: a) Los materiales peligrosos y combustibles se almacenan en algún lugar distante del Data center. b) Verificar que los equipos de remplazo y medios de respaldo se encuentren en otras habitaciones y a una distancia prudente de la habitación principal. c) Equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente.	Hay material inflamable (papeles, triplay, maderas, cajas de cartón) a la entrada del Data Center. No existe otro ambiente donde se alberguen los medios de respaldo (está en proyecto). Existe equipos para incendios, uno es el detector de humo y el otro dos extintores; pero éstos se encuentra vencidos y mal ubicados.	**Cumple parcialmente** ✓	Los materiales fácilmente inflamables no están distantes del Data Center. La subgerencia contempla la importancia de albergar los medios de respaldo en nuevo local. Los extintores no son un equipo adecuado para contrarrestar un incendio por estar vencidos, además podrían resultar nocivos para la salud en caso de ser usadas.	Se recomienda en un corto plazo buscar otro espacio donde albergar los materiales inflamables que se encuentran a la entrada del Data Center. Adquirir nuevos extintores en un corto plazo y ubicarlos adecuadamente según las recomendaciones de defensa civil.

Tabla N° 4.14: Levantamiento de evidencias y hallazgo del Data Center de la MPH de la "protección contra amenazas externas y ambientales" (Elaboración propia)

CONTROL	9.1.5. EL TRABAJO EN EL DATA CENTER	EVIDENCIA	CUMPLIMIENTO (100%)	HALLAZGO
Objetivo	Diseñar y aplicar protección física y pautas para trabajar en el Data Center.			
Evitar trabajos no supervisados Verificar que se evita el trabajo no supervisado en el Data Center tanto para evitar oportunidades de actividades maliciosas.		Los trabajos de supervisión en el Data Center se realizan con acompañamiento del personal encargada.	**Cumple** ✓	
Control Verificar la prohibición de presencia de equipos de fotografía, video, audio u otras formas de registro salvo autorización especial.		Se permite la presencia de equipo de fotografía, video, etc con autorización.	**Cumple** ✓	

Tabla N° 4.15: Levantamiento de evidencias y hallazgo del Data Center de la MPH de "El trabajo en el Data Center" (Elaboración propia)

CONTROL	9.1.6. ACCESO PÚBLICO, ÁREAS DE CARGA Y DESCARGA	EVIDENCIA	CUMPLIMIENTO (100%)	HALLAZGO
Objetivo	Controlar las áreas de carga y descarga, aislarse del Data Center para evitar accesos no autorizados.			
Controles para las áreas de carga y descarga Verificar la existencia de una habitación especial para la entrega y carga de proveedores.		El encargado de la compra de equipo es la unidad de abastecimiento de la Municipalidad, cuyos ambientes de almacén se encuentran alejados del Data Center.	**Cumple** ✓	

Tabla N° 4.16: Levantamiento de evidencias y hallazgo del Data Center de la MPH de los "acceso público, áreas de carga y descarga" (Elaboración propia)

Categoría 9.2. SEGURIDAD DE LOS EQUIPOS

CONTROL	9.2.1. INSTALACIÓN Y PROTECCIÓN	EVIDENCIA	CUMPLIMIENTO (16.67 %)	HALLAZGO	RECOMENDACIONES
Objetivo	Proteger los activos del Data Center para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.				
Controles Verificar que los controles son adoptados para minimizar los riesgos de posibles amenazas como robo, incendio, explosivos, humo, agua (o fallo de suministro), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas y vandalismo.		No existen documentos de controles de los equipos (**No existe el control**)	X		Se recomienda desarrollar mecanismos de controles físicos para los equipos (algunas sugerencias más detalladas se muestran en el documento de conclusiones de la sección 4.2.5 tabla 4.30).
Fumar, beber y comer Constatar que en el Data Center se incluye en su política cuestiones sobre fumar, beber y comer dentro o próximos del Data Center.		No hay políticas de comportamiento establecidas para el Data Center. (**No existe el control**)	X		Incluir en las políticas de seguridad, los modos de comportamientos sobre fumar, beber y comer dentro o próximos del Data Center.
Condiciones ambientales Constatar que se vigilan las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos del Data Center.		Existe un dispositivo manual para controlar la temperatura pero su revisión no se realiza todos los días y existe un sensor de humedad.	**Cumple parcialmente** ✓X	Dispositivo de control de temperatura sin vigilancia frecuente.	Poner un horario en el día para la revisión de la temperatura en los ambientes del Data Center.

Tabla N° 4.17: Levantamiento de evidencias y hallazgo del Data Center de la MPH de las "instalociones de protecciones" (Elaboración propia)

CONTROL	9.2.2. SUMINISTRO ELÉCTRICO	EVIDENCIA	CUMPLIMIENTO (60%)	HALLAZGO	RECOMENDACIONES
Objetivo	Proteger el Data Center contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo (UPS, Generadores eléctricos)				
Instalaciones adecuadas Comprobar que todas las instalaciones, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado sean adecuados.		Existe un tablero de distribución de energía eléctrica. El administrador mencionó que no existe suministro de agua ni desagüe en el Data center; el aire acondicionado está ubicado en una esquina y a la fecha ya presentó fallas.	**Cumple parcialmente** ✓	El aire acondicionado si ya presentó fallas podría ocasionar mayores conflictos a largo plazo. La ubicación del Aire acondicionado no ayuda a que haya una correcta circulación del aire.	Se recomienda establecer en un corto plazo los periodos de mantenimiento del aire acondicionado, aunque Presente o no fallas. En largo Plazo se recomienda renovar el equipo de aire acondicionado.
Sistemas de Alimentación Ininterrumpida (UPS) Constatar la instalación del UPS para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del negocio.		Existen UPS para contrarrestar los cortes inesperados de energía.	**Cumple** ✓		
Instalaciones y conexiones de emergencia Verificar la instalación de interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se dispone de alumbrado de emergencia.		No existen interruptores de emergencia pero en caso de que falle la energía existen luces de emergencia que funcionan con su propia batería.	**Cumple** ✓	No hay instalaciones de interruptores de emergencia.	Se recomienda instalar interruptores de emergencia que estén ubicados en zonas de rápido y fácil acceso.

Suministro de agua Comprobar que el suministro de agua es estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados).	No existe suministro de agua en el Data Center (**No existe el control**)	X		Se recomienda hacer un análisis de las instalaciones de suministro de agua en el Data Center, esto si en un futuro se adquieren equipos que requieran de agua y contemplar en dicho análisis que sus instalaciones sean estables
Equipos de telecomunicación Comprobar que los equipos de telecomunicación están conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz. Este servicio es adecuado para satisfacer requisitos locales legales para comunicaciones de emergencia.	El administrador asegura que existen otras rutas de conexión de los equipos de telecomunicación.	**Cumple** ✓		

Tabla N° 4.18: Levantamiento de evidencias y hallazgo del Data Center de la MPH de las "Suministro eléctrico"

(Elaboración Propia)

CONTROL	9.2.3. SEGURIDAD DEL CABLEADO	EVIDENCIA	CUMPLI-MIENTO (50 %)	HALLAZGO	RECOMENDACIONES
Objetivo	Proteger contra interceptaciones o daños el cableado de energía y telecomunicaciones que transporten datos o soporten servicios de información.				
Líneas de energía y telecomunicaciones Constatar que las líneas de energía y telecomunicaciones en el Data Center han adoptado medidas de protección.		Algunos cables de energía y telecomunicaciones se encuentran en canaletas, pero otras no	**Cumple parcialmente** ✓	No todas las líneas de energía y telecomunicaciones están protegidas.	Organizar el cableado haciendo uso del piso falso y/o canaletas.
Protección de la red cableada Constatar que la red cableada se protege contra intercepciones no autorizadas o daños, por ejemplo, uso de conductos y evitando rutas a través de áreas públicas.		No se pudo comprobar que la red cableada que viene desde la calle al Data Center este protegida.		No se tiene evidencias.	Se recomienda asegurarse de que los servicios de acceso local son entregados en un conducto seguro desde la calle.
Separar cables de energía de los de comunicaciones Verificar que están separados los cables de energía de los de comunicaciones		El administrador nos da a conocer que si se encuentran separadas.	**Cumple** ✓		
Identificación de cables Verificar el uso de cables claramente identificados y marcas de equipo con el fin de minimizar errores de manejo como el de parchar cables de una red incorrecta.		Los cables se encuentran parcialmente identificados	**Cumple parcialmente** ✓	Faltan cables por identificar lo que puede dificultar el trabajo de parches si se presenta algún incidente	Se recomienda terminar la identificación de todos los cables, esto facilitará el manejo de trabajos de parches u otros incidentes.
Lista documentada de parches Verificar el uso de una lista documentada de		No existe ninguna lista de parches registrados	✗		Se recomienda llevar un registro de los

parches con el fin de reducir la posibilidad de errores.	**(No existe el control)**			parches realizados en el cableado de datos o el de electricidad.
Estructura del cableado Verificar la estructura del cableado de manera que no se produzca interferencia por ruido o estática entre aquellos que transitan de forma paralela y que el material que envuelve los cables sea resistente al fuego.	La estructura del cableado no se encuentra muy ordenada, el material del cable si es resistente (cable de datos de categoría 6).	**Cumple parcialmente** ✓	Una estructura desordenada no permitirá apreciar claramente que cables transitan de forma paralela, y éstas pueden producir interferencias y ruidos.	Se recomienda tener una administración adecuada del cableado manteniendo el tipo de organización de cableado horizontal y vertical, usados frecuentemente en un data Center.

Tabla N° 4.19: Levantamiento de evidencias y hallazgo del Data Center de la MPH de la "seguridad del cableado" (Elaboración Propia)

CONTROL	9.2.4. MANTENIMIENTO DE EQUIPOS	EVIDENCIA	CUMPLIMIENTO (37,5%)	HALLAZGO	RECOMENDACIONES
Objetivo	Mantener los equipos del Data Center adecuadamente para asegurar su continuidad e integridad.				
Mantenimiento de equipos Constatar que los equipos se mantienen de acuerdo a las recomendaciones de intervalos y especificaciones de servicio del suministrador.		No se realiza mantenimientos periódicos de los equipos, solo se atiende cuando sufre algún desperfecto.	**No cumple** X	No se realiza mantenimientos periódicos de los equipos, por lo que hay una mayor probabilidad de que éstos presenten desperfectos.	Se recomienda establecer periodos fijos de mantenimiento de equipos; de acuerdo a las especificaciones técnicas del suministrador y para ello mantener un inventario actualizado de todos los activos del Data Center.
Reparación y servicio de los equipos Corroborar que sólo el personal de mantenimiento debidamente autorizado realiza la reparación y servicio de los equipos.		El administrador hace referencia que algunas reparaciones lo realiza el mismo o en algunas ocasiones contratan a terceros previa autorización.	**Cumple** ✓		
Documentar los fallos y mantenimientos Comprobar que se registran documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo.		Se realiza documentación de fallos mediante informes presentados por el administrador, y no se documenta el mantenimiento correctivo y el preventivo	**Cumple parcialmente.** ✓X	No existen documentos de acciones correctivos y preventivos; tampoco se registran los fallos reales y sospechosos.	Se debería elaborar un plan de mantenimiento preventivo y correctivo (esto puede estar incluido en un plan de continuidad) y

	no existe.			registrar todos los fallos reales o scspechosos.
Implementación de controles en mantenimientos Verificar la implementación de controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal interno o externo a la institución; donde sea necesario, se despeja la información sensible del equipo.	No se encuentra implementados controles de mantenimiento de equipos (**No existe el control**)	X		Elaborar controles de mantenimiento para los equipos, por ejemplo que incluyan: • Intervalos de visitas técnicas: semestral. • Personal de mantenimiento. • Verificación del estado y funcionamiento de los equipos. • Periodos de Limpieza de los equipos.

Tabla N° 4.20: Levantamiento de evidencias y hallazgo del Data Center de la MPH del "Mantenimiento de equipos" (Elaboración Propia)

CRITERIO	9.2.6. SEGURIDAD EN EL REHÚSO O ELIMINACIÓN DE EQUIPOS	EVIDENCIA	CUMPLIMIENTO (0%)	HALLAZGO	RECOMENDACIONES
Objetivo	Todos los elementos del equipo que contengan dispositivos de almacenamiento del Data Center deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.				
Destrucción física de los dispositivos de almacenamiento Verificar que se eliminan los dispositivos de almacenamiento con información sensible usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato.		No existe procedimientos que contemplen las acciones técnicas de destrucción física de los dispositivos de almacenamiento (hasta la fecha no se ha realizado ninguna depuración de ningún dispositivos de almacenamiento) (**No existe el control**)	X		Se recomienda incluir en la políticas de seguridad del Data del Center procedimientos que contemplen técnicas seguras de destrucción física de los dispositivos de almacenamiento
Evaluación de riesgos Verificar que los dispositivos dañados que contienen data sensible requieren una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.		No existe ningún documento de evaluación de riesgos de dispositivos dañados (**No existe el control**)	X		Se recomienda, cuando se dé el caso, realizar una evaluación de riesgos de aquellos dispositivos dañados que tengan da sensible; antes de ser descartados.

Tabla N° 4.21: Levantamiento de evidencias y hallazgo del Data Center de la MPH de la "seguridad en el rehúso o eliminación de equipos" (Elaboración propia)

CONTROL	9.2.7. RETIRO DE LA PROPIEDAD	EVIDENCIA	CUMPLIMIENTO (100%)	HALLAZGO
Objetivo	El equipo, no debe ser sacado fuera del local del Data Center sin autorización.			
Autorización Verificar que el equipo no es sacada fuera del local sin autorización.		La extracción de cualquier equipo del Data Center es realizada previa autorización del jefe de la sub Gerencia de Sistemas, su registro se da en el ingreso de la puerta principal de la Municipalidad.	**Cumple** ✓	
Identificación de autoridades Verificar que los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos son claramente identificados.		El vigilante del local central de la Municipalidad tiene conocimiento de las autoridades que laboran en la Municipalidad.	**Cumple** ✓	
Límites de tiempo Verificar que los tiempos límite para el retiro de equipos son fijados y el retorna del equipo verificado para asegurar la conformidad.		Los tiempos límites para el retorno de los equipos si son fijados, y el responsable es directamente el administrador.	**Cumple** ✓	
Registro del equipo Verificar que el equipo es registrado, si es necesario y apropiado, cuando es removido fuera del local así como cuando es devuelto.		Este registro está a cargo del vigilante de la puerta central del local de la Municipalidad.	**Cumple** ✓	

Tabla N° 4.22: Levantamiento de evidencias y hallazgo del Data Center de la MPH del "retiro de la propiedad"

(Elaboración Propia)

PROCESOS DE DOMINIO DE COBIT 5.0 CON SUS RESPECTIVOS OBJETIVOS DE CONTROL

CONTROL		EVIDENCIA	HALLAZGO	RECOMENDACIONES
EDM01 Definir y mantener el marco de Gobierno				
Proporcionar un enfoque consistente integrado y alineado con el enfoque de Gobierno de la institución. Para asegurar que las decisiones relacionadas con TI se hacen en línea con sus estrategias y objetivos.				
EDM01	Verificar la existencia de un gobierno de seguridad física en el Data Center de la institución.	El Data Center no cuenta con políticas de seguridad física.	**No cumple** No existe políticas de seguridad que contribuyan con el gobierno de TI	Se recomienda en un mediano plazo definir un gobierno de seguridad física en el Data Center (implica la elaboración de las políticas de seguridad) y actualizarlos anualmente.
APO01 Definir el marco de gestión de las TI				
Identificar los requisitos y objetivos para el marco para la gobernanza de la TI incorporando las aportaciones de facilitadores como principios, políticas y marcos; procesos; estructuras organizativas; la cultura, la ética y el comportamiento; la información; servicios, aplicaciones y la infraestructura; personas, habilidades y competencia.				
APO01.02	Verificar el establecimiento de roles y responsabilidades en seguridad física del Data Center.	El establecimiento de roles y responsabilidades de la seguridad física del Data Center es asignado de manera verbal.	**No cumple:** La asignación de los roles y responsabilidades no son formales.	Se recomienda para facilitar el trabajo del administrador y que éste no tenga complicaciones en sus funciones, asignar un personal exclusivo para el Data Center o incluir sistemas de monitoreo de control remoto.

APO01.07	Verificar la ejecución de capacitaciones al personal encargado sobre las consideraciones de seguridad física en Data Center, cómo afectan a las operaciones de la Municipalidad y las acciones a tomar en situaciones de riesgo.	Hasta la fecha el personal que administra el Data Center no recibió ninguna capacitación.	**No cumple** Si el personal no cuenta con capacitación en su labor, no podrá responder eficientemente al cargo que le fue encomendado.	Es necesario e importante programar capacitaciones en seguridad física para el personal que administra el Data Center. La formación es esencial, porque los empleados que son capaces de reaccionar a los eventos no planificados pueden ayudar a evitar el tiempo de caída; por ello se recomienda entrenamiento y certificación formal.
APO07 Gestionar los Recursos Humanos Asegurar que las políticas y los procesos están en su lugar para la evaluación, capacitación y desarrollo del personal para hacer frente a los requisitos de la institución y el crecimiento personal y profesional.				
APO07.01	Verificar la adecuada y apropiada dotación del personal para la administración del Data Center	Existe un personal que vela por la administración del Data Center, además éste cuenta con otras funciones (Analista programador), el administrador manifiesta que la infraestructura del Data Center está creciendo.	**Cumple parcialmente** Se ocasiona conflictos en las labores del personal en caso de presentarse necesidades urgentes dentro del Data Center. Si la infraestructura del Data Center está creciendo se requerirá más personal.	Se recomienda efectuar una cláusula que contemple las responsabilidades y roles en el contrato del personal (coordinar con los responsables de recursos humanos o manejarlo a nivel interno) para que queden establecidas de forma clara las tareas que el personal que administra el Data Center debe realizar.

APO10 Gestionar los proveedores Minimizar los riesgos del negocio asociados con los proveedores de equipos y servicios para el Data Center				
APO10.03	Verificar que los contratos con terceros o proveedores por lo menos deben incluir acuerdos de seguridad, acuerdos de confidencialidad.	Los acuerdos con proveedores o terceros son verbales.	**No cumple** No existen acuerdos formales con los proveedores o terceros que garanticen que sus servicios brindados no afectarán en la seguridad y confidencialidad de los datos que alberga el Data Center.	Realizar contratos de trabajo con los proveedores o terceros, donde se incluya acuerdos de seguridad y confidencialidad al ingresar al Data Center.
APO12 Gestionar el Riesgo Documentar los riesgos de TI. Cualquiera de los impactos causado por algún evento imprevisto se debe identificar, analizar y evaluar. Los resultados de la evaluación deben ser entendibles para los interesados, permitiendo disminuir los riesgos en el Data Center a un nivel aceptable de tolerancia.				
APO12.05	Verificar si existe una cartera de acciones para la gestión de riesgos en el Data Center	No se contempla un conjunto de acciones para gestiones de riesgo.	**No cumple** No existe ningún lineamiento de acciones, para una gestión de riesgo del Data Center.	Programar y llevar a cabo una evaluación anual de riesgos y amenazas que examine tanto las amenazas internas, como las externas del Data Center

BAI03 Gestionar la Identificación y la Construcción de Soluciones La institución debe contar con procesos para adquirir, implementar, actualizar, proteger y mantener la infraestructura tecnológica de su Data Center según las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas.				
BAI03.07	Verificar la existencia de un plan de pruebas de soluciones en seguridad física.	No existe plan de Pruebas de soluciones.	**No cumple** La no existencia de pruebas de soluciones de seguridad desatiende la protección y mantención de la infraestructura tecnológica del Data Center.	Crear y definir un plan de pruebas; esto ayudará a validar la capacidad del Plan de Recuperación ante desastres.
BAI03.08	Verificar si se han ejecutado las pruebas de soluciones en seguridad física de forma continua, identificando, registrando y dando prioridad a los errores y los problemas detectados durante las pruebas.	Si no existe un plan de pruebas, no puede darse éste control (**control no existente**)		

BAI06 Gestionar los Cambios Administrar formalmente y controladamente los cambios relacionados con la infraestructura dentro del ambiente del Data Center.				
BAI06.02	Verificar la existencia de mecanismos de emergencia que controlen el mantenimiento de los equipos.	No existen mecanismos de emergencia que controlen el mantenimiento de los equipos.	**No cumple** No hay mecanismos de emergencia de control de mantenimiento de equipos.	Elaborar procedimientos de emergencia para responder a incidentes que pueden amenazar los equipos y asegurar que estos procedimientos sean probados regularmente.
DSS01 Gestionar Operaciones Proteger los equipos del Data Center y el personal, bajo requerimientos de instalaciones bien diseñadas y administradas, incluyendo la definición de requerimientos físicos del Data Center, conectividad, selección de instalaciones apropiadas, diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico.				
DSS01.04	Verificar que el personal de redes y comunicación asegure que los equipos estén en funcionamiento y protegidos contra factores ambientales.	No hay equipos que monitoreen los factores ambientales, accesos físicos del Data Center.	**No cumple** No tener un control no asegura que los equipos estén protegidos.	Instalar cámaras de seguridad que pueden grabar eventos dentro y fuera del Data Center.

DSS02 Gestionar las peticiones y los incidentes del servicio Contar con un proceso de integración de respuesta a incidentes.				
DSS02.04	Verificar si existen procedimientos de gestión de incidentes y problemas.	No existen procedimientos de gestión de incidentes y problemas.	**No cumple** Data Center sin un control de sus incidentes que se pueden convertir en problemas serios.	Se recomienda cantar con procedimientos de gestión de incidentes y problemas.
DSS02.05	Verificar que existe un Plan de Reauperación ante Desastres (PRD).	No existen Plan de Recuperación ante Desastres	**No cumple** Data Center sin un mecanismo que contrarreste un desastre	Se recomienda elaborar plan de recuperación ante desastres para asegurar, siempre en caso de un siniestro, la reconstrucción de la infraestructura del Data Center; recordar la premisa "Siempre desear lo mejor y planear para lo peor". Este plan debe ser documentado y probado con periodicidad
DSS04 Gestionar la Continuidad				
Desarrollar la capacidad del Data Center para seguir brindando servicio con la ayuda de un plan de continuidad para la recuperación de fallas y políticas de respaldo de información.				
DSS04.01	Verificar la existencia de planes de continuidad en caso de incidentes no planeados.	No existe plan de continuidad, pero está en proceso de elaboración.	**No Cumple** La subgerencia expresa su intención y preocupación sobre definir un plan de continuidad adecuada para incidentes no planeados, al igual	Desarrollar un plan de continuidad basado en prevenir, reducir, recuperar y transferir. Este plan puede cantener al plan de contingencia, también debe ser documentado y probado con periodicidad

			que adquirir un lugar de almacenamiento de respaldo	
DSS04.07		No hay otro lugar donde se almacena la información de respaldo, pero ya está en proyecto.	**No cumple** La subgerencia expresa su inquietud y preocupación de adquirir un lugar de almacenamiento de respaldo fuera de la instalaciones.	En un corto plazo identificar otros sitios de la institución que podrían ser configuradas para respaldar al Data Center.
DSS05 Administrar Servicios de Seguridad				
Mantener una efectiva administración del ambiente físico y reducir las interrupciones de las actividades como institución, ocasionadas por daños al equipo.				
DSS05.05	Verificar como una medida de seguridad que la ubicación del Data Center no sea obvia para los visitantes.	La ubicación del Data Center no está señalizada.	**Cumple**	
DSS05.07	Verificar si se monitorea las visitas técnicas o académicas a las instalaciones y se registran los resultados del monitoreo.	Si se monitorea (siempre habrá un personal que acompañe cada visita)	**Cumple**	

Tabla N° 4.23: Levantamiento de evidencias y hallazgo del Data Center de la MPH según los criterios de COBIT 5.0

(Elaboración propia)

Se realizó una entrevista directa al administrador, para obtener información de los requerimientos generales en la infraestructura del Data Center de la MPH:

REQUERIMIENTOS GENERALES	SI	NO
¿Existen espacios libres a las lados de los equipos?	x	
¿Se constata que existe un correcto flujo del aire al verificar la ubicación de las bandejas de cables dentro del piso elevado?		x
¿Existen estudios eléctricos que determinen la correcta alimentación de corriente hacia los equipos?		x
¿Están los equipos situados lejos de fuentes de interferencia electromagnética?	x	
¿El cuarto de equipos no tienen ventanas al exterior?	x	
¿Los pisos, paredes y techas estan sellados, pintados o construidos de un material para minimizar el polvo?		x
¿Los acabados son de color claro para mejorar la iluminación de la habitación y los pisos tienen propiedades anti estáticas?	x	
¿Las luces de emergencia no son alimentadas desde el mismo panel de distribución eléctrica de los equipos de telecomunicaciones?	x	
¿Existen señalización de salidas y emergencia?		x
¿Se analizó que no existan vibraciones mecánicas junta a los equipos que pueden provocar fallas en los servicios?		x
¿El cuarto de equipos tiene tomacorrientes dúplex (120V 20A) para las herramientas eléctricas, equipos de limpieza que no utilicen las tomas de los Gabinetes?	x	
¿La ubicación de los racks es adecuada para que se creen pasillos calientes y fríos?		x
¿La altura máxima de los racks en el cuarto de equipos es de 2.4 cm?	x	
¿Todas las cajos de revisión de las rutas del cableado se encuentran cerradas con llave?		x

Tabla N° 4.24: Requerimientos generales según TIA 942 que cumple el Data Center de la MPH (Elaboración propia)

Clasificamos el Data Center de la Municipalidad de acuerdo al estándar internacional TIER, por cada uno de los subsistemas:

TELECOMUNICACIONES					
CONTROL	**TIER I**	**TIER II**	**EVIDENCIA**	**HALLAZGO**	**CALIFICACIÓN DEL NIVEL**
Verificar que el cableado, bastidores (rack) cumpla con las especificaciones TIA 942.	SI exige	SI exige	El cableado cumple con las especificaciones de TIA942 (categoría 6) y los bastidores son suficientes para el manejo de los cables.	Los bastidores brindan la capacidad adecuada para manejar los cables, que es lo recomendable por la TIA 942, y el tipo de los cables también están alineado a la especificación.	TIER II
Verificar que todos los cables, racks y gabinetes deben estar correctamente etiquetados, los armarios y bastidores deben estar etiquetados con su identificador en la parte delantera y trasera.	SI exige	SI exige	No todos los cables están etiquetados, ni los rack y gabinetes.	La exigencia de los requerimientos es para todos los cables. Los rack y gabinetes también están sin etiquetas.	Ninguno
Verificar que los routers y switches tengan fuentes de alimentación redundantes.	No exige	SI exige	Los routers y switches tienen fuentes de alimentación redundante.	Cumple con el requerimiento de TIER II	TIER II
Verificar que los cables de conexión y puentes estén etiquetados en ambos extremos con el nombre de la conexión en ambos extremos del cable.	No exige	SI exige	No están etiquetados	No cumple este requerimiento.	TIER I
Verificar que haya entrada de proveedores de acceso diversificadas con mínimo de 20 m de separación.	No exige	SI exige	Tiene una ruta de entrada desde el proveedor del acceso a la instalación.	No existen rutas diversificadas de entrada, desde el proveedor de acceso a la instalación.	TIER I

Tabla N° 4.25: Levantamiento de evidencias y hallazgo según los criterios de TIER I y TIER II para el subsistema de "Telecomunicaciones" del Data Center de MPH (Elaboración Propia)

ARQUITECTURA					
CONTROL	**TIER I**	**TIER II**	**EVIDENCIA**	**HALLAZGO**	**CALIFICACIÓN DEL NIVEL**
Ubicación del Data Center					
Proximidad a áreas de inundación registradas por las autoridades.	No exige ningún requisito	No permitido dentro de áreas	Ubicado en el sótano	El sótano es un área de riesgo de inundación.	TIER I
Edificio con diferentes dueños	Ningún requisito	Permitido si no hay riesgos en los ocupantes	Las instalaciones del Data Center se hallan dentro de una gran infraestructura, donde se encuentran oficinas de otras áreas de la Municipalidad.	Los trabajadores de la Municipalidad no pueden considerarse como un riesgo para el Data Center	TIER II
Requisitos de Resistencia al fuego					
Constatar que los muros exteriores e interiores del Data Center son resistentes al fuego.	Código permisible	Código permisible	La construcción de los muros es a base de ladrillo, concreto y fierro.	Los ladrillos, fierros y concretos son considerados como elementos que pueden retardar en minutos el avance del fuego; estipulado en la norma A.130 art46 del Reglamento Nacional de Edificaciones.	TIER II
Verificar que los pisos y revestimientos de techos, piso y techo falso del Data Center tengan una resistencia al fuego.	Código permisible	Código permisible	La construcción de los pisos y techos son de concreto, el revestimiento del techo falso tiene las mismas características del piso técnico (piso laminado, concreto, vinílico)	Los materiales de los pisos y techos son considerados resistentes al fuego según lo estipulado en la norma A.130, art48. del Reglamento Nacional de Edificaciones	TER II

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Verificar que se cumpla con la norma NFPA 75	No requiere	Si	No se tuvo en cuenta esta norma NFPA75 al Implementar el Data Center	No se cumple con este requerimiento.	TIER I
Componentes de construcción					
Verificar que existan barreras de vapor para las paredes y el techo de la sala de ordenadores, para garantizar los límites de humidificación.	No requiere	Si	No existe ningún elemento (láminas, pinturas, papel de aluminio, etc) en las paredes del Data Center que ayuden a garantizar la humidificación.	No se cumple con este requerimiento.	TIER I
Verificar la altura del techa	Mínimo 2,6 m (8,5 pies)	Mínimo 2,7 m mínimos (9,0 pies)	La altura del techo es aproximadamente de 2,6 m.	Se le puede considerar dentro del TIER I	TIER I
Verificar si las puertas y ventanas son resistentes al fuego	Requisitos del Código mínimo	Requisitos del Código mínimo	El material de la puerta del Data Center es de vidrio doble y no existe ninguna ventana.	Los vidrios son considerados materiales no combustibles según la Norma A.130.	TIER II
Verificar el tamaño de la puerta.	Mínimo1 m (3 pies) de ancho y 2,13 m (7 pies) de alto	Mínimo1 m (3 pies) de ancho y 2,13 m (7 pies) de alto	Es de 1m y de 2,13 m de alto aproximadamente	Cumple con ambos niveles.	TIER II

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Lobby de entrada					
Verificar que esté físicamente separada de otras áreas del Data Center.	Na requiere	Si	El Data Center es una parte de la edificación del sótano, es decir en el sótano encontramos una entrada antes de ingresar al Data Center.	La entrada del sótano puede ser considerado con "lobby de entrada", y si está separado del Data Center.	TIER II
Oficinas Administrativas					
Las oficinas administrativas de la subgerencia deben estar físicamente separada del Data Center	No exige	Si	La oficina de la sub gerencia se encuentra en la segunda planta de los ambientes de la Municipalidad.	La oficina administrativa está separa del Data Center.	TIER II
Seguridad					
Verificar el tiempo de la capacidad del UPS de equipo de campo	No contempla	Generador del Edificio + Batería (4horas)	El tiempo de la capacidad del UPS es de 2 horas y la institución no cuenta con ningún generador eléctrico.	La capacidad que brinda el UPS podría tomarse en cuenta en el TIER I	TIER I
La dotación de personal de seguridad par turno	Ninguno	2 como mínimo	No existe ningún personal de seguridad exclusivo para el Data Center, solo cuentan con el de la institución en general.	Na existe dotación de personal	TIER I
Control de accesos de seguridad y monitoreo					
Verificar el control de acceso al lugar donde se halla el generador	Bloqueo de grado industrial	Detección de intrusos	Na cuenta con un generador		Ninguno

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Verificar el control de acceso al cuarto de UPS, teléfono y cuarto de equipos mecánicos y eléctricos.	Bloqueo de grado industrial	Detección de intrusos	Los UPS se encuentran en el único ambiente que tiene el Data Center y el acceso es mediante una cerradura electrónica, y no hay monitoreo (solo existe una cámara de vigilancia sobre la puerta del Data Center y ésta apunta hacia el lobby de entrada), existe un sensor de movimiento dentro del Data Center.	La puerta con cerradura electrónica, y el sensor de movimiento es un mecanismo de control, pero no hay medios de monitoreo.	TIER II
Verificar el control de acceso a las puertas de salida de emergencia	Bloqueo de grado industrial	Vigilancia	No existen puertas de emergencia. Para ingresar y salir del Data center, la primera puerta es la del sótano (hecha de fierro y vidrio catedral) ésta da acceso al exterior y la segunda es la puerta propiamente del Data Center.		Ninguno
Verificar el control de acceso a las ventanas o aberturas interiores.	Monitoreo en el sitio	Detección de intrusos	No existen ventanas en el sótano y por ende en el Data Center		Ninguno
Verificar el control de accesa a las puertas en el cuarto de equipos	Bloqueo de grado industrial	Detección de intrusos	El cuarto de equipos está protegida por la puerta de cerradura electrónica (puerta del Data Center)	El cuarto de equipos si tiene un control de acceso contra intrusos.	TIER II

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Monitoreo CCTV					
Verificar si existen cámaras en las puertas de control de acceso	No requiere	Si	Existe una sola cámara en la puerta del Data Center que apunta al exterior y no dentro del Data Center.	Hay una cámara que vigila la entrada al Data Center.	TIER II
Estructural					
Verificar la capacidad de carga del pisa para las áreas de equipos.	7,2 kPa (150 lbf / pies 2)	8,4 kPa (175 lbf / pies 2)	El administrador asegura que hubo un estudio de carga del piso, pero desconoce de la capacidad de carga.	Na hay evidencia	
Verificar que los racks/ gabinetes están anclados a la base o con soporte en la base y arriba (especialmente las que contienen a los servidores y los equipos de comunicaciones)	Ningún requisito	Solo la base	Los rack son removible (presentan ruedas en las bases), los servidores están albergados en ellas.	Ninguno de rack, gabinetes se encuentran anclados a la base.	TIER I

Tabla N° 4.26: Levantamienta de evidencias y hallazgo según los criterios de TIER I y TIER II para el subsistema de "Arquitectura" del Data Center de MPH (Elaboración Propia)

ELÉCTRICO					
CONTROL	**TIER I**	**TIER II**	**EVIDENCIA**	**HALLAZGO**	**CALIFICACIÓN DEL NIVEL**
Requisito general					
Verificar el número de vías de distribución eléctrica o rutas de alimentación.	1	1	Existe solo una ruta de alimentación eléctrica provista por un solo proveedor (una sola vía)	Cumple con los dos niveles	TIER II
Verificar que todos los equipos del sistema eléctrico deben estar etiquetados con certificación de un laboratorio de prueba.	Si	Si	El administrador desconoce que haya certificación de un laboratorio de prueba de los equipos del sistema eléctrico.	No hay evidencia	
Verificar los puntos únicos de fallo	Uno o más puntos sencillos de falla para el sistema de distribución que alimentan al equipo eléctrico o HVAC	Uno o más puntos sencillos de falla para el sistema de distribución que alimentan al equipo eléctrico o HVAC	Un punto de falla puede ser la misma fuente central de alimentación eléctrica, y otro los UPS (cuando agota el límite de tiempo de alimentación).	Existe más de un punto de fallo	TIER II
Verificar como se da el sistema de transferencia de carga crítica	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	No se pudo realizar las pruebas programadas, porque para ello requería quitar el suministro eléctrico, lo cual no era permitido. Además el Data Center y toda la institución no cuentan con un generador.	No hay evidencia	

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Verificar que los generadores estén correctamente dimensionados de acuerdo a la capacidad instalada de UPS.	Se pide	Se pide	No cuenta con ningún generador eléctrico.		Ninguno
Verificar cual es la capacidad del generador de combustible (a carga completa)	8 horas	24 horas	No cuenta con ningún generador eléctrico		Ninguno
Equipo de apoyo (UPS y transformadores)					
Verificar la redundancia del UPS	N	N+1	Existe 04 UPS	Cumple con la lo establecido en TIER I ("n" cargas de TI requieren "n" UPS)	TIER I
Verificar que la distribución de energía del UPS y nivel de voltaje es de:	Nivel de voltaje 120 / 208V para cargas de hasta 1440 kVA y 480 V para cargas superiores a 1440 kVA	Nivel de voltaje 120 / 208V para cargas de hasta 1440 kVA y 480 V para cargas superiores a 1440 kVA	No se pudo tener acceso a la hoja de especificaciones de los UPS, el Personal solo manifestó que su capacidad es de 1000 VA y 5000VA	No se tiene evidencia suficiente	

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Verificar que el UPS en el panel de distribución es independiente para equipos informáticos y de telecomunicaciones.	No exige	Si	Los UPS en el panel de distribución son independientes para equipos informáticos y de telecomunicaciones.	Cumple con el requerimiento de TIER II	TIER II
Verificar la topología del UPS	Módula sencillo	Único módulo o módulo redundante en paralelo	No se tuvo acceso a las hojas de especificaciones del UPS	No hay evidencia	
Verificar como es el bypass de mantenimiento de UPS	Energía tomada del mismo	Energía tomada del mismo	No se pudo tener acceso a la topología del sistema de UPS, en las hojas de especificaciones	No hay evidencia	
Verifica el diseña de los componentes redundantes (UPS)	Diseño estática UPS.	Diseño de UPS estático o rotativo. Convertidores de M-G rotativo	Los UPS son de diseños camunes.	Podemos calificar que los UPS tienen diseño estático	TIER I
Verificar la instalación de los transformadores de factor k en el PDU.	Requiere, pero no es abligatorio si se utiliza transformadores de cancelación de armónicos	Requiere, pero no es obligatorio si se utilizan transformadores de cancelación de armónicos	No cuenta con ningún transformador de factor k, en su lugar existe un regulador de energía	Un regulador de energía no es lo mismo que un transformador de cancelación de armónicos que recomiendan TIER I y TIER II	Ninguna

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Puesta a tierra					
¿La Infraestructura del Data Center tiene conexión a tierra?	No requerido	No requerido	Si tiene una conexión a tierra en uno de los jardines más próximo al local del Data Center.	Ninguno de los niveles exige este requerimiento, pero es bueno contar con este mecanismo de protección.	Opcional
Verificar si tiene un sistema de pararrayos	Con base en el análisis de riesgos de acuerdo con la norma NFPA 780 y los requisitos de seguro.	Con base en el análisis de riesgos de acuerdo con la norma NFPA 780 y los requisitos de seguro.	La institución propiamente no tiene un sistema de pararrayos, pero tiene una cercana que se encuentra en la Basílica Catedral (Iglesia matriz de la ciudad de Huamangd), pero se desconoce el tipo de norma con la que fue implementado.	Existe una protección de sistema de pararrayos pero no se sabe si está alineado con la norma NFPA 780.	Ninguno
Verificar si se tiene el botón de apagado de emergencia (EPO)	Si	Si	No existe ningún botón de apagado de emergencia	No cumple con lo establecido en el TIER I y II	Ninguno
Supervisión o monitoreo del Sistema eléctrico					
Verificar que se muestre localmente en el UPS a través de un display.	Si	Si	El UPS con el que cuenta el Data Center no cuenta con dislay lcd	UPS sin display, esto no ayuda en el monitoreo del sistema eléctrico	Ninguno

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Configuración de baterías					
Verificar que exista una cadena de batería común para todos los módulos	Si	Na	No se tuvo acceso al diagrama de conexión de los UPS.	No hay evidencia	
Verificar que exista una cadena de batería por módulo	No	Si	No se tuva acceso a la hoja de especificaciones del UPS	No hay evidencia	
Verificar el Tiempo mínimo de standby a carga completa	5 minutos	10 minutos	No se tuvo acceso a la hoja de especificaciones del UPS	No hay evidencia	
¿El tipa de batería es?	Una batería VRLA (batería de ácido-plomo regulada por válvula) o de tipo inundado	Una batería VRLA (batería de ácido-plomo regulada por válvula) o de tipo inundado	No se tuva acceso a la hoja de especificaciones del UPS	No hay evidencia	
Baterías tipo inundados					
Verificar las placas envueltas	No	Si	No se tuva acceso a la hoja de especificaciones del UPS	Na hay evidencia	
Verificar que hay y haya pruebas de batería a carga completa con un calendario de inspección	Cada dos años	Cada dos años	No hay registros de mantenimienta de ningún equipo	No cumple con ninguno de los requerimientos de TIER I y TIER II	Ninguno
Verificar que esté instolado el contenedor de derrames de ácido.	Si exige	Si exige	No existe ningún contenedor de derrames de ácidos.	No cumple con ninguno de los requerimientos de TIER I y TIER II	Ninguno

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Cuarto de batería					
¿Está separado del cuarto de equipos?	No existe	Si	No hay cuarto de baterías	No existe cuarto de baterías	TIER I
¿Las cadenas individuales de batería están aisladas unos de otros?	No existe	Si	No hay cadenas de baterías	No existe cadena de baterías	TIER I
Verificar el sistema de Monitoreo de las baterías	No existe	Autocontrol UPS	Na hay baterías	No existe	TIER I
Ambientes del sistema UPS rotativo (con generadores de diésel)					
¿Los tanques de combustible están en la misma habitación que las unidades?	Si	Si	Na existe generador		Ninguno
Sistemas de generación en stand by					
Verificar el dimensionamiento del generador	Clasificado solamente para ordenadase y sistema de telecomuni cacion es tanto mecánico como eléctrico	Clasificado solamente para ordenadores y sistema de telecomunicacion es tanto mecánico como eléctrico	No existe generador		Ninguna
Verificar que los Generadores son de un solo bus.	Si	Si	No existe generador		Ninguna

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICACIÓN DEL NIVEL
Verificar que exista un generador individual por sistema con generador de repuesto (1)	No	Si	No existe generador		Ninguno
¿Hay 83 pies de protección de pozo a tierra individual para cada generador?	No	Si	No existe generador		Ninguno
Banco de carga para la prueba					
¿Las pruebas que se realizan en el UPS se dan únicamente en sus módulos?	Si	Si	No existe ningún mecanismo de prueba para los UPS		Ninguno
¿Se realizan pruebas solamente de generadores?	Si	Si	No existe generodor		Ninguno
Mantenimiento de Equipo					
Verificar que hay un personal de mantenimiento	En un turno de día solamente en el sitio. De guardia en otras ocasiones	En un turno de día solamente en el sitio. De guardia en otras ocasiones	No existe ningún personal de mantenimiento	No cumple con ninguno de los requerimiento de TIER I y TIER II	Ninguno
¿Hay programas de capacitación de instalaciones?	No exige	No exige	No existe programas de capacitación de instalaciones	Ningún nivel exige este requerimiento, pero si es importante considerarlo.	Opcional

Tabla N° 4.27: Levantamienta de evidencias y hallazgo según los criterios de TIER I y TIER II para el subsistema "Eléctrico" del Data Center de MPH (Elabaración Propia)

MECÁNICA					
CONTROL	**TIER I**	**TIER II**	**EVIDENCIA**	**HALLAZGO**	**CLASIFI-CACIÓN DEL NIVEL**
Requisito General					
Verificar que las rutas de tuberías de agua y desagüe no se asocian a los equipo del Data Center	Permitido pero no se recomienda	Permitido pero no se recomienda	No existe rutas de tuberías de agua y desagüe en el Data Center	Cumple con ambos requerimientos	TIER II
Verificar si hay desagües de piso en la sala de ordenadores para drenar agua condensada, agua del humidificador, y el agua de la descarga de rociadores.	Si	Si	No existen desagües de piso en el Data Center.	No cumple con lo establecido en ambos requerimientos	Ninguno
Sistema Refrigerado por agua, por agua helada o por aire					
Verificar las unidades terminales de aire acondicionado en interiores.	No hay unidades de aire acondicionado redundantes	Una unidad de aire acondicionado redundante por área crítica	Solo se constató la presencia de un aire acondicionado de precisión y dos de "confort"	Si se cuenta con un equipo de aire acondicionado, entonces no hay redundancia, los de confort no son considerados apropiados	TIER I
Verificar el control de humedad para la sala de ordenadores.	Humidificación proporcionado	Humidificación proporcionado	El aire acondicionado proporciona un control de humedad.	El aire acondicionado tiene un humidificador.	TIER II

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICA-CIÓN DEL NIVEL
Verificar el servicio eléctrico al equipo mecánico (aire acondicionado)	Trayectaria individual de energía eléctrica para los equipas de aire acondicionoda	Trayectoria individual de energía eléctrica para los equipos de aire acondicionado.	Existe una sola trayectoria de energía al aire acondicionado.	Cumple con el requerimiento de TIER I y TIER II	TIER II
Sistema de control de HVAC					
Sistema de cantrol de HVAC	Si falla el sistema de control interrumpirá la refrigeración a las áreas críticas	Si falla en el sistema de control no interrumpirá la refrigeración a las áreas críticas	El único equipo que tiene de HVAC es el aire acondicionado de precisión.	Si falla este único equipo interrumpirá la refrigeración a los equipos críticos.	TIER I
Fuente de alimentación para el sistema de control de climatización (HVAC).	Camino individual de energía eléctrica al sistema de control HVAC	Redundante fuente eléctrica, de UPS para los equipos de HVAC	Solo esta alimentado por una sola ruta de energía eléctrica.	Existe solo un camino individual de energía eléctrica al sistema de control HVAC	TIER I
Sistema de combustible					
Verificar las bombas y tuberías de los tanques de almacenamiento	Bomba individual y / o tubería de suministro	Bombas Múltiples, múltiples tuberías de suministro	No existen tanques de almacenamiento		Ninguno
Verificar el volumen de los tanques de almacenamiento	Tanque de almacenamiento individual	Tanques de almacenamiento múltiples	No existen tanques de almacenamiento		Ninguno
Supresión de incendios					
Verificar si existe un sistema de detección de incendios.	No exige	Si	Hay un dispositivo de detección de incendio.	Cumple con el lineamiento de TIER II	TIER II

CONTROL	TIER I	TIER II	EVIDENCIA	HALLAZGO	CALIFICA-CIÓN DEL NIVEL
Verificar el sistema de rociadores contra incendios.	Cuando se requiera	Cuanda sea necesario	No existen rociadores o aspersores para casos de incendio	Ambos niveles TIER solo mencionan en casos necesarios.	TIER II
Verificar si hay alerta temprana del sistema de detección de humo.	No	Si	El dispositivo de detección de incendio es el que cumple este papel de detección de humo.	Cumple con lo requerido en el TIER II	TIER II
Verificar si existe un sistema de detección de fugas de agua	No	Si	Existe un detector de humedad	El detector de humedad cumple el papel de detector de fugas de agua	TIER II
Verificar la temperatura del ambiente	18 a 27 °C	18 a 27 °C	La temperatura tomada en el instante de la visita fue 18°C	Cumple con lo estipulado en ambos niveles	TIER II
Verificar la humedad	30 a 60 %	30 a 60 %	La humedad relativa es del 57%	Cumple con ambos niveles	TIER II

Tabla N° 4.28: Levantamiento de evidencias y hallazgo según los criterios de TIER I y TIER II para el subsistema "Mecánico" del Data Center de MPH (Elaboración Propia)

Las recomendacianes dadas de acuerdo a la clasificación TIER por cada subsistema, se realizan en la documentación de las conclusiones y recomendaciones de la sección 4.2.5 apartado B.2.

4.2.5 DOCUMENTACIÓN DE LAS CONCLUSIONES Y RECOMENDACIONES:

Después de haber inspeccionado las instalaciones del Data Center se concluye y recomienda lo siguiente:

A. CONCLUSIONES:

A.1 Del Análisis de riesgo realizado en la sección 4.2.2.2 se concluye:

Luego de definir los niveles de riesgos respecto a las vulnerabilidades de cada activo y las amenazas que puedan afectar su disponibilidad; se recomienda algunas medidas que se pueden tomarse en cuenta, desde los niveles de riesgo más altos hasta los más bajos (tener en cuenta la tabla 4.11):

PRIORIZACIÓN	AMENAZAS	MEDIDAS GENERALES	MEDIDAS ESPECÍFICAS
1	• Incendios.	Verificar los sistemas de protección y las medidas de seguridad contra incendios.	• Verificar que haya un número suficiente de extintores en el Data Center. • Instalar "interruptores asesinos" para detener una descarga accidental. • Verificar que los sistemas de extinción de incendios funcionan y son probados regularmente.
	• Polvo	Evitar la presencia del polvo.	Realizar limpieza en la: • Superficie por debajo del falso piso • Superficie superior del falso piso • Parte exterior de los racks y equipamiento del Data Center • Interior de los racks y superficie de los equipos: servidores, switches, routers, etc. • Techo, canalizaciones, conductos, paredes, etc.
2	Falta de refrigeración y fallas de circulación de aire	Controlar la calidad del aire y los sistemas de refrigeración.	Verificar que los sistemas de climatización son adecuadamente mantenidos y probados de manera regular, como una vez al mes.
3	Temperatura inadecuada	Monitorear la temperatura	• Monitorear la temperatura por día. • Adquirir sensores de temperatura
4	• Pérdida de energía.	Controlar las interrupciones del suministro eléctrico.	
	• Filtración de agua e inundación	Verificar los sistemas de protección y las medidas de seguridad contra inundaciones.	• Preparar bolsas de arena para las inundaciones • Tener disponibles equipo de bombeo o extractores de agua. • Desarrollar y probar procedimientos de emergencia para inundaciones. • Para evitar filtros de agua se debe revisar las instalaciones de agua y desagüe de los ambientes que colindan con el Data Center. • Limpiar periódicamente los canales de desagüe y alcantarillado cercanos a local del Data Center, para contrarrestar las posibles inundaciones provocadas por las intensas lluvias de nuestra localidad.

5	Error humano	Reforzar y apoyar el trabajo del administrador del Data Center para minimizar los errores por negligencia o desconocimiento	• La jefatura debe tomar las decisiones correctas en todos los aspectos de mantenimiento, incluidas las tareas de mantenimiento preventivo, limpieza diaria y de ciclo de vida de los equipos del Data Center. • En cuanto a la planificación, coordinación y administración del Data Center, se deben diseñar políticas para el sitio (plan de seguridad para el sitio) y ésta debe ser probada al año. Con estas medidas se minimizan los riesgos ocasionadas por errores humanos
6	Contaminantes de gases y partículas	Verificar la calidad del aire	Asegurarse que el Data Center esté libre de la presencia de contaminantes suspendidos en el aire
7	Acceso del personal no autorizado, huelgas, vandalismas	Reforzar la seguridad en el control de acceso.	• Asegurar que los sistemas de seguridad del edificio están operativos. • Desarrollar y probar procedimientos de emergencia para la seguridad del Data Center. • Desarrollar y probar procedimientos de emergencia para desórdenes civiles y eventos relacionados. • Instalar cámaras de seguridad que pueden grabar eventos dentro y fuera del edificio. • Asegurar de que los guardias de seguridad están disponibles en las entradas de la institución.
8	• Sismos de bajo y media intensidad	Proteger los equipos más sensibles contra sismos.	• Desarrollar y evaluar los procedimientos de emergencia en caso de sismos.
	• Vibraclanes por ruidos	Controlar los ruidos producidos en el interior del Data Center en los decibeles adecuado.	Mantener los equipos en buen funcionamiento.
9	Presencia de humedad	Monitorear los dispasitivas de humedad	Control los dispositivos de humedad con monitoreo remoto.

Tabla N° 4.29: Medidas de cantrol para minimizar los riesgos en el Data Center de la MPH (Elabaración Propia)

A.2 Después de haber realizado la evaluación con los controles de la NTP-ISO/IEC 17799:2007 se concluye:

- ✓ El Data Center de la MPH cumple con la categoría 9.1 "áreas seguras" del Dominio 9 de la presente norma en un 71%, este resultado se puede considerar como un nivel de seguridad aceptable.
- ✓ El Data Center de la MPH cumple con la categoría 9.2" seguridad de equipos" del Dominio 9 en un 44,03%, este resultado se puede considerar como un nivel de seguridad poco favorable por lo que hay tomar en cuenta las recomendaciones realizadas.

A.3 Después de haber realizado la evaluación con el COBIT 5.0 se concluye:

De los 16 criterios establecidos por COBIT 5.0 el Data Center de la MPH solo cumple con un 15,63%, este resultado presenta un escenario de seguridad física no satisfactorio, para lo cual requiere implementarse acciones de corrección de acuerdo a las recomendaciones vertidas anteriormente.

A.3 En cuanto a la clasificación del estándar internacional TIER I y TIER II concluimos que:

- ✓ De los 14 requerimientos generales según TIA 942, el Data Center de la MPH cumple con un 50%, presentando con esto un resultado favorable.
- ✓ En el subsistema de **telecomunicaciones** de los 05 criterios establecidos, 02 cumple con los requerimientos de TIER I, 02 alcanzan TIER II, 01 con ninguno.
- ✓ En el subsistema de **arquitectura** de los 21 criterios establecidos; 07 alcanzan los requerimientos de TIER I, 10 alcanzan TIER II, 03 con ninguno, 01 no se obtuvo evidencias.

- ✓ En el subsistema **eléctrico** de los 36 criterios establecidos; 05 alcanzan los requerimientos de TIER I, 03 alcanzan TIER II, 16 con ninguno, 10 no se obtuvo evidencias, y 02 fueron criterios opcionales.
- ✓ En el subsistema **mecánico** de los 15 criterios establecidos; 03 alcanzan los requerimientos de TIER I, 09 alcanzan TIER II, 03 con ninguno.

Con éstos resultados, la calificación del Data Center de la MPH tiende a ser un Data Center de Tipo I, aunque hubo requerimientos básicos establecidos por este nivel que el Data Center de la MPH no alcanzó; por lo que se puede decir que la disponibilidad del Data Center tendrá un porcentaje por debajo del 99,67%.

B. RECOMENDACIONES:

B.1 Recomendaciones generales NTP-ISO/IEC 17799:2007 y COBIT 5.0:

- Se recomienda implementar en su totalidad los controles de seguridad física según NTP-ISO/IEC 17799; éste código de buenas prácticas está orientado de manera obligatoria a las instituciones públicas, como medida propuesta por el estado peruano según el Decreto Legislativo N°560.
- NTP-ISO/IEC 17799:2007 ayudará a la Municipalidad a introducir cada vez más la cultura de seguridad entre sus trabajadores; además puede ser de referencia para implementar un plan de seguridad de la información para la institución.
- Se recomienda implementar en su totalidad los procesos de COBIT 5.0 referidos a la seguridad física, esta implementación contribuirá con la administración y el control de la seguridad física del Data Center de la MPH.

B.2 De acuerdo a los requerimientos generales de TIA 942 se recomiendo las siguientes pautas:

- Adquirir en un corto plazo, nuevos equipos de aire acondicionado o ver modalidades de sistemas de refrigeración para la mejora de la circulación del aire (se sugiere la implementación de los "pasillos fríos y calientes" o la refrigeración gratuita "free cooling").
- Realizar instalaciones del cableado de telecomunicaciones en el piso de acceso (falso piso) mediante bandejas de cables; que no bloquean el flujo de aire, estas deben tener una profundidad máxima de 150 mm.
- Se recomienda que el cableado no sea encaminado a través de los espacios públicos a menos que esté encerrado en rutas seguras como: cajas de paso o cajas de empalme, las mismas que deberá ser cerradas con llave y monitoreadas.
- Despejar los obstáculos que se encuentran en el Data Center, para tener espacios libres que faciliten los trabajos técnicos y los de limpieza.
- Buscar repintar las paredes del Data Center con un material ignífugo y que minimice la presencia del polvo.
- Incrementar las señalizaciones de salidas de emergencia en el sótano y el ambiente propiamente del Data Center, tener también la señalización de los lugares de alto voltaje, esto para la protección de las personas que ingresan al Data Center.
- Inspeccionar cada cierto tiempo que no hayan vibraciones provocadas por los equipos mecánicos o producidas desde el exterior que estén por encima de los niveles establecidos, en caso de ocurrir, tomar medidas de protección para aquellos dispositivos más sensibles.

De acuerdo a TIER; para que el Data Center de la MPH sea considerado en el nivel 1 (TIER 1), se debe cumplir por lo menos los siguientes requerimientos básicos:

Telecomunicaciones

Se debe concluir con el etiquetado recomendado por el ANSI/TIA/606-A

Eléctrica

- Se recomienda invertir en un nuevo sistema de energía de respaldo, como un generador eléctrico, que prolongue el servicio de energía eléctrica en caso de que los UPS cumplan con su tiempo límite de sostener la energía; y ante sus posible adquisición se recomienda:
  - ✓ Para calcular el generador "ideal" para el Data Center de la MPH, es importante primeramente dimensionar las cargas que dicho ambiente maneja, para esto se parte del amperaje necesario para cada uno de los elementos como: consumo UPS, consumo sistema de control de temperatura, consumo de luminarias, consumos de tomas adicionales (para ello tomar en cuenta la norma ANSI/TIA/EIA 607)
  - ✓ Probar regularmente éste y los demás sistemas de energía de respaldo.
  - ✓ Es necesario tener una autonomía de combustible a carga completa de 8 horas.
- Se recomienda según el TIA 942 del anexo G, que para soportar los efectos de calentamiento de corrientes armónicas, utilizar transformadores K-nominal instalados en el PDU del Data Center, un transformador de cancelación armónica zigzag o un transformador con un filtro de armónicos activo pueden ser utilizados también.

- Se recomienda instalar el sistema de Apagado de emergencia (EPO), esta debe estar ubicado en la salida del Data Center, y debe contar con una cubierta protectora para evitar funcionamiento accidental. Un teléfono y una lista de contactos de emergencia deben estar ubicados. Este interruptor de emergencia (EPO) deberá ser supervisada por el panel de control de alarma de incendio (según lo recomendado en la NFPA 75).
- Realizar pruebas de las baterías de los UPS a carga completa periódicamente.
- En cuanto al sistema de pararrayos se recomienda en corto plazo:
  - ✓ Revisar la condición de los sistemas de protección contra rayos de manera regular.
  - ✓ Verificar la disponibilidad de equipos de protección contra sobretensiones para los alimentadores de energía críticos.
  - ✓ Probar y verificar la construcción de tierra por periodos (sistema de puesta a tierra)
- En un largo plazo renovar los equipos de UPS, que tengan display lcd, y cuenten con bypass.
- Establecer medidas de monitoreo al UPS e instalar un contenedor de derrame de ácidos para las baterías (esto evitará la contaminación por la emanación de gases)
- Contemplar en un largo plazo un personal de mantenimiento de equipos eléctricos; o contar con un trabajador externo que esté disponible para ocasiones de emergencia.
- Se recomienda probar regularmente los sistemas de energía de respaldo.

Mecánico

- En un futuro buscar migrar el Data center a una nueva instalación, en ella contemplar las instalaciones de desagüe de piso para drenar agua condensada, agua del humidificador o el agua de la descarga de rociadores.
- Si se adquiere un generador eléctrico tener en cuenta algunas medidas de seguridad:
  - ✓ Tanques de almacenamiento de combustibles ubicados en un área tuera del Data Center, pero cercano al generador; cuidando que este suministro no sea un agente contaminante peligroso.
- Fortalecer la vigilancia al acceso del Data Center con cámaras de CCTV; y asegurar que estos sistemas sean examinados regularmente.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

De la presente tesis se concluye:

a. Se logró implementar los procedimientos de auditoría en seguridad física utilizando la norma NTP-ISO/IEC 17799, el marco de control de COBIT 5.0, el estándar internacional TIER; con éste diseño se planteó evaluar y calificar las instalaciones del Data Center de la Municipalidad Provincial de Huamanga.

b. En la elaboración de los procedimientos de la auditoría se incorpora los procesos de identificación de los activos involucrados en la seguridad física de un Data Center.

c. Los procedimientos de auditoría en seguridad física, incluyen en una de sus etapas, el análisis de riesgo, con ello se alcanza identificar los riesgos que ponen en peligro la continuidad y disponibilidad de un Data Center, en concreto del Data Center de laMPH.

d. Los procedimientos implementados, han sido aplicados en el Data Center de la Municipalidad, logrando resultados que demuestran la efectividad de su seguridad física en algunos aspectos y la deficiencia en otras, la sub gerencia de sistemas de la entidad evaluada mostró interés en querer poner en práctica las recomendaciones de la auditoría, para mejorar la infraestructura e instalaciones de su Data Center y hacerla más resistente ante eventuales riesgos, y para elevar el buen desempeño en sus servicios tecnológicos.

5.2 RECOMENDACIONES

a. Los procedimientos de auditoría en seguridad física implementados en este trabajo de investigación, pueden servir como guía para un auditor y pueden ser aplicadas a cualquier Data Center del sector público y del sector privado de nuestra ciudad.

b. Se recomienda que las entidades públicas de Ayacucho que pretenden implementar un Data Center adopten los lineamientos de la norma NTP-ISO/ IEC 17799, como una medida impuesto por el ONGEI, y las recomendaciones del estándar internacional TIER para obtener un buen diseño e implementación de un Data Center.

c. Se deben impulsar la adopción de estándares internacionales como el COBIT u otros estándares en las entidades del sector público y privado de nuestra localidad, para promover el mejoramiento continuo de los recursos y servicios de tecnología de la información.

d. Se recomienda complementar este trabajo de investigación con lineamientos que se basen en una auditoría en la seguridad lógica, la seguridad de las redes o una auditoría energética de un Data Center.

BIBLIOGRAFÍA

1. Aguilera, P. (2010). *Seguridad Informática.* Madrid, España: Editex, S. A.
2. Areitio, J. (2008). *Seguridad de la Información. Redes, informática y sistemas de información.* Madrid, España: Paraninfo
3. Arizala, C. E. y Ortiz, B. L. (2010). *Desarrrollo de una propuesta metodológica para la implementación de Centros de Datos de Alta Disponibilidad.* Tesis de grado, Escuela Politécnica de Chimborazo, Esmeraldas, Ecuador.
4. Barba, J.D. y Viteri, G.A. (2012). *Análisis, Evaluación y Propuesta de Optimización del funcionamiento del Data Center de la Escuela Politécnica del Ejército utilizando las Normas y Estándares Nacionales e Internacionales de Calidad.* Tesis, Escuela Politécnica del Ejército departamento de ciencias de la computación, Salgonguí, Ecuador.
5. Bernabé, M. A. y López, C.M. (2012). *Fundamentos de las Infraestructuras de Datos Espaciales (1ra Ed).* Madrid, España: UPM Press.
6. Bernal, C. A. (2006). *Metodología de la Investigación (2ª Ed)*: Prentice Hall.
7. Bustos, F.A., Chávez, J.F., Gonzáles, L.A., Millón, A. y Gómez, A. (2009). *Metodología para evaluar y calificar la seguridad física de un centro de procesamiento de datos.* Tesina, Instituto Politécnico Nacional, México D.F.
8. Carrasco, S. (2009). Metodología de la Investigación Científica (2ª *Ed*). Lima, Perú: San Marcos.
9. Cerra, M. (2010). *200 Respuestas Seguridad.* Argentina: USERSHOP.
10. Chamorro, V. L. (2013). Plan de Seguridad de la Información basado en el estándar ISO 13335. Tesis, Escuela Politécnica Nacional, Quito.

11. Chaparro, N., Perez, D. y Tenjo N. (2010). *Riesgo Informáticos.* Recuperado el lunes 12 de abril de 2010, de http://www.cabinas.net/informatica/analisis_riesgos_informaticos.
12. Chicano, E. (2015). *Auditoría de Seguridad Informática IFCT0109.* Antequera, Málaga: IC Editorial
13. Cilleros, D. (2012). *Seguridad en Data Centers: infraestructura y prevención.* Proyecto de Fin de Carrera, Universidad Carlos III, Madrid, España.
14. Clasificación TIER En El Data Center (07 De 2012). Recuperado El 24 de Febrero de 2013, de Http://Blog.Aodbc.Es/2012/07/10/Clasificacion-Tier-En-El-Datacenter-El-Estandar-Ansitia-942
15. Compañía TRC (s. f.). *Auditoría de Data Center.* Documento electrónico, Madrid. Recuperado de http://www.trc.es/documentacion/datacenter/auditoria-datacenter.pdf
16. Consultora ISOTools Excellence (2013). *ISO 27001. El inventario de activos en la implementación de la norma.* Recuperado el 05 de diciembre de 2013, de http://www.isotools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001
17. Contraloría General de República de Nicaragua (2009). *Manual de Auditoría Gubernamental, Parte VIII, Auditoría Informática.* Proyecto BIG/CGR, Managua, Nicaragua.
18. Dais-ujat (2006). *Avances en Informática y Sistema Computacionales Tomo I (CONAIS 2006).* Tabasco, México: Univ. J. Autónoma de Tabasco.
19. De pablos, C., López-Hermoso, J.J., Martín-Romo, S., Medina, S., Montero, A. y Nájera, J.J. (2006). *Dirección y gestión de los sistemas de información en la empresa (2 ª Ed).* Madrid, España: ESIC.
20. Del Peso E., Ramos M.A., Del Peso M. y Del Peso M. (2011). *Nuevo Reglamento de Protección de datos de carácter personal: Medidas de Seguridad.* Madrid, España: Diaz de Santos, S.A.

21. Del Peso, E. (2003). *Manual de outsourcing informático: (análisis y contratación): modelo de contrato (2 ª Ed.)*. Madrid, España: Diaz de Santos.
22. Delgado, X. (1998). *Auditoría Informática*. Costa Rica: EUNED.
23. Devoto, L.R. (2008). *Diseño de Infraestructura de Telecomunicaciones para un Data Center*. Tesis de grado, Pontificia Universidad Católica del Perú, Lima, Perú.
24. Espinosa, J.L. (2012). *Eficiencia Energética en Centros de Procesos de Datos*. Tesis de Master, Universidad de Sevilla, Sevilla.
25. Galán, L. (1996). *Informática y auditoría para las ciencias empresariales*. Bucaramanga, Colombia: UNAB.
26. Gómez, A. J. (2011). *Redes locales*. Madrid, España: Editex.
27. Guagalango, R. N. y Moscoso, P.E. (2011). *Evaluación Técnica de la Seguridad Física del Data Center de la Escuela Politécnica del Ejército. Tesis*, Escuela Politécnica del Ejército, Sangolquí, Ecuador.
28. Hernández, R., Fernández, C. y Baptista, P. (2008). *Metodología de la investigación (4ª Ed.)*. México, D.F., México: McGraw Hill Interamericano.
29. INDECOPI- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (2007). *EDI. Tecnología de la Información códigos de buenas prácticas para la gestión de la seguridad de la información (2ª Ed.)*. Lima, Perú: Comité de Reglamentos Técnicos y Comerciales de INDECOPI.
30. ISACA (2011). Auditoría de Sistemas. Recuperado el 27 de abril de 2011, de http://www.isaca.org/Blogs/282270/archive/2011/04/27/Protecci%C3%B3ndeActivosdeInformaci%C3%B3n.aspx.
31. ISACA (2012). *COBIT 5.0, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. Impreso en los Estados Unidos de http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf

32. ISO 19011:2011. *Directrices para la Auditoría de Sistemas de Gestión (2ª Ed.)*. Suiza.
33. ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management. EEUU.
34. Llerena, C. A. (2013). *Formulación de una guía de auditoria para la infraestructura física de los centros de datos de las entidades públicas del ecuador basado en marcos de referencia de TI.* Tesis de maestría en Evaluación y Auditoría de Sistemas Tecnológico, Universidad de la Fuerzas Armadas, Sangolqui, Ecuador.
35. Maldonado, J. (2010). *Diseño de un Centro de Datos Basado en Estándares. Caso práctico: Diseño del Centro de Datos del Colegio latinoamericano.* Tesis de grado, Universidad de Cuenca, Cuenca, Ecuador.
36. Mantino, I. (2013). *Auditoria de la SEGURIDAD FÍSICA Y AMBIENTAL Auditoria. Trabajo de* campo. Recuperado el 22 de junio de 2013, de http://es.slideshare.net/isabelmantino/auditoria-seguridadfisica-y-del-entorno-isoiec-270022005?related=1.
37. McMillan, J. y Schumacher, S. (2005). *Investigación Educativa.* Madrid, España: Pearson Educación.
38. Nogueira, J. E. (2013). *Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER.* Tesis, Universidad Pontifica Católica del Perú, Lima.
39. Piattini, M. G. y Del Peso, E. (2001) *Auditoría Informática: Un enfoque práctico* (2ª Ed). México D.F: Alfaomega grupo editor S.A.
40. Quintana, J. D. (2009). *Centro de Proceso de Datos: El cerebro de nuestra sociedad.* Discurso Académico. San Bartolomé: Gráficas Loureiro, S.L.
41. Ramirez, G. y Álvarez, E. (2003). *Auditoría a la gestión de las tecnologías y sistemas de información,* 6 (1), 99-102.

42. Rubio, J.E. (2012). *Análisis y Diseño de un Data Center en base a los estándares ANSI/EIA/TIA 606, 607 y 942 para el edificio de la Dirección Provincial de Salud de Pichincha.* Tesis, Universidad Politécnica Salesiana, Quito.
43. Rytoft, C. (2013). *Centro de Datos.* La Revista ABB, 4(13), 8-9.
44. Taborda, C.A., Escobar L.E. y Torres L.C. (2011). *Auditorías Específicas Data Center Continuidad Del Negocio: Recuperación De Desastres Y Respaldos.* Tesis, Universidad nacional de Colombia sede Manizales, Colombia.
45. Tupia, M. (2010). *Administración de la seguridad de información.* Perú: Graficar.

GLOSARIO

PROCEDIMIENTO: Un procedimiento es el modo de proceder o el método que se implementa para llevar a cabo ciertas cosas, tareas o ejecutar determinadas acciones. Básicamente, el procedimiento consiste del seguimiento de una serie de pasos bien definidos que permitirán y facilitarán la realización de un trabajo de la manera más correcta y exitosa posible.

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.

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.

COLUMNA VERTEBRAL (BACKBONE): Es una instalación (por ejemplo, vía, cable o conductores) entre cualquiera de los siguientes espacios: salas de telecomunicaciones, salas comunes de telecomunicaciones, terminales, instalaciones de suelo que sirven de entrada, salas de máquinas, equipos y salas comunes de un centro de datos.

GABINETE: Un contenedor que puede encerrar los dispositivos de conexión, terminaciones, aparatos, cableado y equipos.

RACK: Es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. También son llamados bastidores, cabinas o armarios.

NFPA 75: (Norma para la Protección de Equipos de Tecnología de la Información) El propósito de ésta norma es el de establecer los requisitos

mínimos para la protección del equipamiento de tecnología de la información y de las áreas para los equipos de tecnología de la información, de los daños ocasionados por el fuego o por sus efectos asociados, es decir, humo, corrosión, calor y agua.

NFPA 780: Esta norma contempla la instalación de sistemas de protección contra rayos.

PROTOCOLO DE MONTREAL: Es un acuerdo internacional que limita, controla y regula la producción, el consumo y el comercio de sustancias depredadoras de la capa de ozono.

CONTROL: El control es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos de negocio.

ESTÁNDAR TIA 942: Fue creado por la Telecommunication Industry Association, que en sus primeras publicaciones de estándares proponen una serie de especificaciones para comunicaciones y cableado estructurado, que posteriormente avanzan sobre los subsistemas de infraestructura de un Data Center, generando los lineamientos que se deben seguir para clasificar estos subsistemas en función de los distintos grados de disponibilidad que se pretende alcanzar en los Data Center. Algunas normas de TIA son ANSI/TIA/606-A, ANSI/TIA/607.

PDU: (Tablero de distribución de las cargas críticas) son un equipo eficaz y estratégico, al incrementar la disponibilidad de la energía y la capacidad de gestión cuando se les selecciona e instala apropiadamente.

ANEXOS

ANEXO A

ACTIVOS FÍSICOS QUE SE ENCUENTRAN EN UN DATA CENTER			
GRUPO	**EQUIPO PARA UNIDAD INFORMÁTICA**	**CANTIDAD**	**CARACTERÍSTICAS/DESCRIPCIÓN**

Tabla A.1 Activos de un Data Center

Nº	**ACTIVOS DEL DATACENTER**	**VALOR DEL ACTIVO**

Tabla A.2: Tasación de Activos

VALOR	**SIGNIFICADO**	**CRITERIO = DISPONIBILIDAD**
1	Muy bajo	Daño irrelevante
2	Bajo	Daño menor
3	Medio	Daño importante
4	Alto	Daño grave
5	Muy alto	Daño muy grave

Tabla A.3: Criterio para la tasación de activos (Llerena, 2013)

Nº	**AMENAZAS**	**VULNERABILIDADES**	**PROBABILIDAD DE OCURRENCIA DE LA AMENAZA**

Tabla A.4: Cálculo de Probabilidad de ocurrencia de una amenaza frente a una vulnerabilidad del Data center.

MATRIZ DE RIESGOS		**AMENAZAS**					
Probabilidad de amenaza							
Activo	Impacto	**Medición o valoración del riesgo**					

Tabla A.5: Matriz de Riesga (Llerena, 2013)

ANEXO B

B.1. CRITERIOS DE SEGURIDAD FÍSICA BASADOS EN NTP-ISO/IEC 17799

De las cláusulas presentadas en el estándar NTP-ISO/IEC 17799, se toma en cuenta la cláusula de Seguridod física y ambiental, dando 9. Los criterios de seguridad física definidos según ésta norma son:

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.1. Áreas seguras**
Control	**9.1.1. Perímetro de seguridad física**
Objetivo	Usar perímetros de seguridad para una mayor protección(como paredes, tarjetas de cantrol de entroda a puertas a un puesto manual de recepción para proteger el local del Data Center)
Pautas a considerar	**Solidez física** Comprobar que el perímetro del Data Center tiene solidez física (por ejemplo no tendrá zonas que padrá derribarse fácilmente).
	Área de recepción manual Ccmprobar que exista un área de recepción manual u otros medios de cantrol del acceso física al Dato Center. Dicho acceso restringe solo al personal autorizado.
	Barreras físicas Verificar que existen barreras físicas extendidas desde el suelo reol al techo real, para evitar entradas no autorizadas o contaminación del entorno.
	Puerta para incendios Constatar que las puertas para incendios tienen alarma, que san monitoreadas.
	Detección de intrusos Verificar la instalación de sistemas adecuados de detección de intrusos de acuerda a estándares regionales, nacionales o internacionales.

Documentos a revisar	Documento de seguridad física
	Mapas de ubicación de barreras físicas
	Documento de ubicación de puertas para incendios.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.1. Áreas seguras**
Cantrol	**9.1.2. Controles físicos de entradas**
Objetivo	Proteger el Data Center por controles de entrada adecuadas que aseguren el permisc de acceso sólo al personal autorizado
Pautas a considerar	**Supervisar visitas** Verificar que se supervise las visitas al Data Center, a menos que el accesc haya sido aprobada previamente, y se deba registrar la fecha y momento de entrada y salida.
	Acceso al Data Center Comprobar que se controla y restringe solo al personal autorizado el acceso al Data Center.
	Personal identificado visiblemente Constatar que se exija a todo el personal que lleve puesta alguna forma de identificación visible y se le solicite a los extraños no acompañados y a cualquier que no lleve dicha identificación visible, que se identifique.
Documentos a revisar	Registro de entrada/salida de personas al Data Center.
	Documento de derechos de accesos.
	Responsabilidades del personal. (fotocheck)

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.1. Áreas seguras**
Control	**9.1.4. Protección contra amenazas externas y ambientales**
Objetivo	Designar y aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano.
Pautas a considerar	**Premisas vecinas** Comprobar que se consideró cualquier amenaza de seguridad presentada por premisas vecinas, como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.
	Evitar daños Verificar que se consideraron las siguientes pautas para evitar daño por parte del fuego, inundación, temblores, explosiones, malestar civil y otras formas de desastre natural o humana: a) Los materiales peligrosos y combustibles se deberían almacenar en algún lugar distante del Data center. b) Verificar que los equipos de remplazo y medios de respaldo se encuentren en otras habitaciones y a una distancia prudente de la habitación principal. c) Equipo apropiado contra incendio debe ser provisto y ubicado adecuadamente.
Documentos a revisar	Documentos de riesgos de entidades vecinas.
	Documento de análisis de riesgo.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.1. Áreas seguras**
Control	**9.1.5. El trabajo en el Data Center**
Objetivo	Diseñar y aplicar protección física y pautas para trabajar en el Data Center.
Pautas a considerar	**Evitar trabajos no supervisados** Verificar que se evita el trabajo no supervisado en el Data Center para evitar apartunidades de actividades maliciosas.
	Control Verificar la prohibición de presencia de equipos de fotografía, video, audio u otras formas de registro salvo autorización especial.
Documentos a revisar	Políticas de seguridad (Procedimientos de trabajos en el Data Center)
	Políticas de seguridad (control de acceso al Data Center)

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.1. Áreas seguras**
Control	**9.1.6. Acceso público, áreas de carga y descarga**
Objetivo	Controlar las áreas de carga y descarga, aislarse del Data Center para evitar accesas na autarizadas.
Pautas a considerar	**Controles para las áreas de carga y descarga** Verificar la existencia de una habitación especial para la entrega y carga de proveedares.
Documentos a Revisar	Políticas de seguridad referida al acceso público.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.1. Instalación y protección**
Objetivo	Proteger los activos del Data Center para reducir el riesgo de amenazas del entorno, así como las oportunidades de accesos no autorizados.
Pautas a considerar	**Controles** Verificar que los controles son adoptados para minimizar los riesgos de posibles amenazas como robo, incendio, explosivos, humo, agua (o fallo de suministro), polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, radiaciones electromagnéticas y vandalismo.
	Fumar, beber y comer Constatar que la organización incluye en su política cuestiones sobre fumar, beber y camer dentro a próximos del Data Center.
	Condiciones ambientales Constatar que se vigilan las condiciones ambientales, como temperatura y humedad, que puedan afectar negativamente al funcionamiento de los equipos del Data Center.
Documentos a revisar	Controles físicos para los equipos.
	Políticas de comportamiento del personal sobre alimentos en el Data Center.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.2. Suministro eléctrico**
Objetivo	Proteger el Data Center contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo (UPS, Generadores eléctricos)
Pautas a considerar	**Instalaciones adecuadas** Comprobar que todas las instalaciones, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado sean adecuados.
	Sistemas de Alimentación Ininterrumpida (UPS) Constatar la instalación del UPS para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del negocio.
	Instalaciones y conexiones de emergencia Verificar la instalación de interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se dispone de alumbrado de emergencia.
	Suministro de agua Comprobar que el suministro de agua es estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados).
	Equipos de telecomunicación Comprobar que los equipos de telecomunicación están conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz. Este servicio es adecuado para satisfacer requisitos locales legales para comunicaciones de emergencia.
Documentos a revisar	Contratos con proveedores de servicios.
	Documentos de instalaciones de alimentación de servicios.
	Instalaciones y conexiones para emergencias.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.2. Suministro eléctrico**
Objetivo	Proteger el Data Center contra fallos de energía u otras anomalías eléctricas en los equipos de apoyo (UPS, Generadores eléctricos)
Pautas a considerar	**Instalaciones adecuadas** Comprobar que todas las instalaciones, como la electricidad, el suministro de agua, desagüe, calefacción/ventilación y aire acondicionado sean adecuados.
	Sistemas de Alimentación Ininterrumpida (UPS) Constatar la instalación del UPS para apoyar un cierre ordenado o el funcionamiento continuo de los equipos que soporten operaciones críticas del negocio.
	Instalaciones y conexiones de emergencia Verificar la instalación de interruptores de emergencia cerca de las puertas de emergencia de las salas de equipos para facilitar una desconexión rápida en caso de emergencia. Por si falla la energía se dispone de alumbrado de emergencia.
	Suministro de agua Comprobar que el suministro de agua es estable y adecuado para suministrar aire acondicionado, equipos de humidificación y sistemas contra incendios (donde sean utilizados).
	Equipos de telecomunicación Comprobar que los equipos de telecomunicación están conectados al proveedor al menos por dos rutas para prevenir la falla en una conexión eliminando el servicio de voz. Este servicio es adecuado para satisfacer requisitos locales legales para comunicaciones de emergencia.
Documentos a revisar	Contratos con proveedores de servicios.
	Documentos de instalaciones de alimentación de servicios.
	Instalaciones y conexiones para emergencias.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.3. Seguridad del cableado**
Objetiva	Proteger contra interceptaciones o daños el cableado de energía y telecamunicaciones que transporten datos o soporten servicios de información.
Pautas a considerar	**Líneas de energía y telecomunicaciones** Constatar que las líneas de energía y telecomunicaciones en el Data Center, están enterradas, cuando sea posible, o se han adoptado medidas alternativas de protección.
	Protección de la red cableada Constatar que la red cableada se protege contra intercepciones no autorizadas o daños, por ejemplo, uso de conductos y evitando rutas a través de áreas públicas.
	Separar cables de energía de los de comunicaciones Verificar que están separados los cables de energía de los de comunicaciones
	Identificación de cables Verificar el uso de cables claramente identificados y marcas de equipo con el fin de minimizar errores de manejo como el de parchar cables de una red incorrecta
	Lista documentada de parches Verificar el uso de una lista documentada de parches con el fin de reducir la posibilidad de errores.
	Estructura del cableado Verificar la estructura del cableado de manera que no se produzca interferencia por ruido o estática entre aquellos que transitan de forma paralela y que el material que envuelve los cables sea resistente al fuego.
Documentos a revisar	Mapa de redes de cableado.
	Documento de parches de red de cableado.
	Procedimientos para la protección de la red cableada.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.4. Mantenimiento de equipos**
Objetivo	Mantener los equipos del Data Center adecuadamente para asegurar su cantinuidad e integridad.
Pautas a considerar	**Mantenimiento de equipos** Constatar que los equipos se mantienen de acuerdo a las recomendaciones de intervalas y especificaciones de servicio del suministrador.
	Reparación y servicio de los equipos Corroborar que sólo el personal de mantenimiento debidamente autorizado realiza la reparación y servicio de los equipos.
	Documentar los fallos y mantenimientos Comprobar que se registran documentalmente todos las fallos, reales o sospechados, así como todo el mantenimiento preventivo y correctivo.
	Implementación de controles en mantenimientos Verificar la implementación de controles apropiados cuando el equipo es programado para mantenimiento, tomando en cuenta si este mantenimiento es realizado por personal interno o externo a la institución; donde sea necesario, se despeja la información sensible del equipo.
Documentos a revisar	Documento de mantenimiento de equipos.
	Funciones y capacidades del personal de reparación y servicio.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.6. Seguridad en el rehúso o eliminación de equipos**
Objetivo	Todos los elementos del equipo que contengan dispositivos de almacenamiento del Data Center deben ser revisados con el fin de asegurar que cualquier dato sensible y software con licencia haya sido removido o sobrescrito con seguridad antes de la eliminación.
Pautas a considerar	**Destrucción física de los dispositivos de almacenamiento** Verificar que se eliminan los dispositivos de almacenamiento con información sensible usando técnicas para hacer que la información original sea no recuperable y no simplemente usando la función normalizada de borrado (delete) o la función formato.

	Evaluación de riesgos Verificar que los dispositivos dañados que contienen data sensible requieren una evaluación de riesgos para determinar si es que los ítems deben ser destruidos físicamente en lugar de ser reparados o descartados.
Documentos a revisar	Procedimientos para la eliminación de dispositivos de almacenamiento
	Documento de evaluación de riesgos de dispositivos dañados.

Dominio 9.	**SEGURIDAD FÍSICA Y AMBIENTAL**
Categoría	**9.2. Seguridad de los equipos**
Control	**9.2.7. Retiro de la propiedad**
Objetivo	El equipo, no debe ser sacado fuera del local del Data Center sin autorización.
Pautas a considerar	**Autorización** Verificar que el equipo no es sacado fuera del local sin autorización.
	Identificación de autoridades Verificar que los empleados, contratistas y usuarios de terceros que tengan autoridad para permitir el retiro de la propiedad de los activos son claramente identificados.
	Límites de tiempo Verificar que los tiempos límite para el retiro de equipos son fijados y el retorno del equipo verificado para asegurar la conformidad
	Registro del equipo Verificar que el equipo es registrado, si es necesario y apropiado, cuando es removido fuera del local así como cuando es devuelto.
Documentos a revisar	Procedimientos para el ingreso y egreso de activos del Data Center fuera de la institución
	Documento de autoridades que permiten el ingreso y salida de los activos del Data Center.

B.2. CRITERIOS DE SEGURIDAD FÍSICA BASADOS EN COBIT 5.0

Desarrollamos los criterios para una auditoría en seguridad física de un Data Center, basados en los procesos de dominio de COBIT 5.0 y sus respectivos objetivos de control:

PROCESOS DE COBIT 5.0	
EDM01 Definir y mantener el marco de Gobierno	
Praparcionar un enfoque consistente integrada y alineado con el enfoque de Gabierna de la institución. Para asegurar que las decisianes relacionadas can TI se hacen en línea can sus estrategias y abjetivas.	
Verificar la existencia de un gabierna de seguridad física en el Data Center de la institución.	
APO01 Definir el marco de gestión de las TI	
Identificar las requisitas y abjetivas para el marco para la gabernanza de la TI incarparanda las apartaclanes de facilitadares coma principias, palíticas y marcas; pracesas; estructuras organizativas; la cultura, la ética y el compartamiento; la información; servicias, aplicacianes y la infraestructura; persanas, habilidades y campetencia.	
APG01.02	Verificar el establecimienta de rales y respansabilidades en seguridad física del Data Center.
APG01.07	Verificar la ejecución de capacitacianes al persanal encargada sabre las cansideraciones de seguridad física en Data Center, cóma afectan a las aperaciones de la Municipalidad y las acciones a tamar en situacianes de riesga.

APO07 Gestionar los Recursos Humanos	
Asegurar que las políticas y los pracesos están en su lugar para la evaluación, capacitación y desarrollo del personal para hacer frente a los requisitos de la institución y el crecimiento personal y profesional.	
APO07.01	Verificar la adecuada y apropiada dotación del personal para la administración del Data Center
APO10 Gestionar los proveedores	
Minimizar los riesgos del negocio asociados con los proveedores de equipos y servicios para el Data Center	
APO10.03	Verificar que los contratos con terceros o proveedores por lo menos deben incluir acuerdos de seguridad, acuerdos de confidencialidad.
APO12 Gestionar el Riesgo	
Documentar los riesgos de TI. Cualquiera de los impactos causado por algún evento imprevisto se debe identificar, analizar y evaluar. Los resultados de la evaluación deben ser entendibles para los interesados, permitiendo disminuir los riesgos en el Data Center a un nivel aceptable de tolerancia.	
APO12.05	Verificar si existe una cartera de acciones para la gestión de riesgos en el Data Center
BAI03 Gestionar la Identificación y la Construcción de Soluciones	
La institución debe contar con procesos para adquirir, implementar, actualizar, proteger y mantener la infraestructura tecnológica de su Data Center según las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas.	
BAI03.07	Verificar la existencia de un plan de pruebas de soluciones en seguridad física.
BAI03.08	Verificar si se han ejecutado las pruebas de soluciones en seguridad física de forma continua, identificando, registrando y dando prioridad a los errores y los problemas detectados durante las pruebas.

BAI06 Gestionar los Cambios	
Administrar farmalmente y cantraladamente las cambias relacianadas can la infraestructura dentra del ambiente del Data Center.	
BAI06.02	Verificar la existencia de mecanismas de emergencia que cantralen el mantenimienta de las equipas.
DSS01 Gestionar Operaciones	
Prateger las equipas del Data Center y el persanal, baja requerimientas de instalacianes bien diseñadas y administradas, incluyendo la definición de requerimientos físicas del Data Center, canectividad, selección de instalacianes aprapiadas, diseña de pracesas efectivas para manitarear factares ambientales y administrar el accesa físico.	
DSS01.04	Verificar que el persanal de redes y camunicación asegure que las equipas estén en funcianamiento y prategidas cantra factares ambientales.
DSS02 Gestionar las peticiones y los incidentes del servicio	
Cantar can un pracesa de integración de respuesta a incidentes.	
DSS02.04	Verificar si existen pracedimientas de gestión de incidentes y prablemas.
DSS02.05	Verificar que existe un Plan de Recuperación ante Desastres (PRD).
DSS04 Gestionar la Continuidad	
Desarrallar la capacidad del Data Center para seguir brindanda servicia can la ayuda de un plan de cantinuidad para la recuperación de fallas y palíticas de respalda de infarmación.	
DSS04.01	Verificar la existencia de planes de cantinuidad en casa de incidentes na planeadas.
DSS04.07	Verificar que el almacenamiento de respaldo está fuera de las instalacianes.

DSS05 Administrar Servicios de Seguridad	
Mantener una efectiva administración del ambiente física y reducir las interrupciones de las actividades como institución, acasianadas par daños al equipo.	
DSS05.05	Verificar camo una medida de seguridad que la ubicación del Data Center no sea obvia para los visitantes.
DSS05.07	Verificar si se monitorea las visitas técnicas a académicas a las instalaciones y se registran los resultados del monitoreo.

Tabla N° B.1: Criterios de auditoría en seguridad física según COBIT 5.0

B.3. CRITERIOS DE SEGURIDAD FÍSICA BASADOS EN TIER:

REQUERIMIENTOS GENERALES	Si	No
¿Existen espacios libres a los lados de los equipos?		
¿Se constata que existe un correcto flujo del aire al verificar la ubicación de las bandejas de cables dentro del piso elevado?		
¿Existen estudios eléctricos que determinen la correcta alimentación de corriente hacia los equipos?		
¿Están los equipos situados lejos de fuentes de interferencia electromagnética?		
¿El cuarto de equipos no tienen ventanas al exterior?		
¿Los pisos, paredes y techos están sellados, pintados o construidos de un material para minimizar el polvo.		
¿Los acabados son de color claro para mejorar la iluminación de la habitación y los pisos tienen propiedades anti- estáticas?		
¿Las luces de emergencia no son alimentadas desde el mismo panel de distribución eléctrica de los equipos de telecomunicaciones?		
¿Existen señalización de salidas y emergencia?		
¿Se analizó que no existan vibraciones mecánicas junto a los equipos que pueden provocar fallas en los servicios?		
¿El cuarto de equipos tiene tomacorrientes dúplex (120V 20A) para las herramientas eléctricas, equipos de limpieza que no utilicen las tomas de los Gabinetes?		
¿La ubicación de los racks es adecuada para que se creen pasillos calientes y fríos?		
¿La altura máxima de los racks en el cuarto de equipos es de 2.4 m?		
¿Todas las cajas de revisión de las rutas del cableado se encuentran cerradas con llave?		

Tabla B.2: Requerimientos generales según TIA 942 (Llerena, 2013)

Se procede a determinar las requerimientas par cada nivel TIER en base a las subsistemas de un Data Center, desarralladas cama un campendia del anexa camplementaria e intarmativa G "Niveles de Infraestructura del Data Center" del estándar TIA 942.

TELECOMUNICACIONES	TIER I	TIER II	TIER III	TIER IV
Cableado, bastidores (rack), y las vías cumplen con las especificaciones TIA 942.	Si exige	Si exige	Si exige	Si exige
El cableado, racks y gabinetes deben estar correctamente etiquetados, los bastidores deben estar etiquetados con su identificodor en la parte delantera y trasera.	Si exige	Si exige	Si exige	Si exige
Los routers y switches deben tener fuentes de alimentoción redundantes.	No exige	Si exige	Si exige	Si exige
Existe múltiples routers y switches pora la redundoncio	No exige	No exige	Si exige	Si exige
Los cables de conexión y puentes deben ser etiquetodos en ambos extremos con el nombre de la conexión en ambos extremos del cable.	No exige	Si exige	Si exige	Si exige
Rutas de cableado vertical (backbone) redundantes.	No exige	No exige	Si exige	Si exige
Entrada de praveedores de acceso diversificados con mínimo de 20 m de separación	No exige	Si exige	Si exige	Si exige

Tabla N° B.3: Criterias de auditoría en seguridad física según TIER (Telecamunicaciones)

ARQUITECTÓNICO	TIER I	TIER II	TIER III	TIER IV
Selección del Sitio				
Proximidad a áreas de inundación registradas por las autoridades.	Ningún requisito	No permitido dentro de áreas	No debe haber historias de inundación durante los últimos 100 años y de 50 años a menos de 91 metros	Na menos de 0,8 km / 2.1 millas
La proximidad del Data Center a aeropuertos.	Ningún requisito	Ningún requisito	No menos de 1,6 km / 1 milla o mayor que 30 milla	No menos de 8 km / 5 millas o mayor que 30 millas
La proximidad a las principales arterias de tráfico.	Ningún requisito	Ningún requisito	No menos de 91m/100 yardas	No menos de 0,8 km / 2.1 millas
Áreas de parqueo de visitantes y empleados separados	Ningún requisito	Ningún requisito	sí (separados físicamente por una cerca o pared)	sí (separados físicamente por una cerca o pared)
Edificio con diferentes dueños	Ningún requisito	Permitido si no hay riesgos en los ocupantes	Permitido si todos los acupantes son compañías de TC	Permitido si todos los ocupantes son compañías de data centers
Requisitos de Resistencia al fuego				
Muros de carga exteriores del Data Center	Código permisible	Código permisible	Mínimo 1 Hara	. Mínimo 4 Horas
Muros de carga interiores del Data Center	Código permisible	Código permisible	Mínimo 1 Hora	Mínimo 2 Horas
Pisos y Revestimientos de techos del Data Center	Código permisible	Código permisible	Mínimo 1 Hora	Mínimo 2 Horas
Piso falso y techo falso	Código permisible	Código permisible	Mínimo 1 Hora	Mínimo 2 Horas
Cumplir can la norma NFPA 75	No requiere	Si	Si	Si

	TIER I	TIER II	TIER III	TIER IV
Componentes de construcción				
Deben existir barreras de vapor para las paredes y el techo de la sala de ordenadores garanticen la humificación.	No requiere	Si	Si	Si
Debe haber entradas múltiples a las instalaciones con los controles de seguridad apropiado	No	No	Si	Si
El panel de piso debe ser de acero o relleno de concreto.	No exige	No exige	Si	Si
Altura del techo	Mínimo 2,6 m (8,5 pies)	Mínimo 2,7 m mínimos (9,0 pies)	3 m (10 pies) (no menos de 460 mm (18 pulgadas) por encima de la más alta pieza de un equipo.	3 m (10 pies) (no menos de 600 mm (24 pulgadas) por encima del equipo más alto
Resistencia al fuego de las puertas y ventanas	Los requisitos del Código mínimo	Los requisitos del Código mínimo	Los requisitos del Código mínimo (no menos de 3/4 de hora en la sala de ordenadores)	Los requisitos del Código mínimo (no menos de 1 1/2 hora en la sala de ordenadores)
Tamaño de la puerta.	Mínimo1 m (3 pies) de ancho y 2,13 m (7 pies) de alto	Mínimo1 m (3 pies) de ancho y 2,13 m (7 pies) de alto	Los requisitos del Código mínimo (no menos de 1 m (3 pies) de ancho en la sala de ordenadores, eléctrica, y salas de máquinas) y no menos de 2,13 m (7 pies) de alto	Los requisitos del Código mínimo (no menos de 1,2 m (4 pies) de ancho en la sala de ordenadores, eléctrica, y salas de máquinas) y no menos de 2,13 m (7 pies) de alto
No debe haber ventanas exteriores en el perímetro de la sala de ordenadores.	No exige	No exige	Si	Si
La construcción del local del Data Center debe proporcionar protección contra la radiación electromagnética.	No exige	No exige	Si	Si

	TIER I	TIER II	TIER III	TIER IV
Lobby de entrada				
Debe estar físicamente separado de otras áreas del data center	No requiere	Si	Si	Si
Debe tener una ventanilla de seguridad	No requiere	No requiere	Si	Si
Oficinas Administrativas, operaciones, seguridad				
Las oficinas administrativas deben estar físicamente separada del Data Center	No exige	Si	Si	Si
Debe haber un cuarto de operaciones y debe de estar físicamente separada de otras áreas del Data Center	No requiere	No requiere	Si	Si
Debe haber una sala de seguridad dedicada a la vigilancia del cuarto de equipos, y debe de estar físicamente separada de otras áreas del Data Center.	Na exige	No exige	Recomendado	Recomendado
Baños y áreas de descanso				
Proximidad al cuarto de equipos y áreas de soporte.	Ningún requisito	Ningún requisito	Si están inmediatamente al lado, deben estar provistas de una barrera de prevención de fugas	Si están inmediatamente al lado, deben estar provistas de una barrera de prevención de fugas
Áreas de almacenamiento del generador y de combustible.				
La proximidad a cuarto de equipos y áreas de apoyo.	Ningún requisito	Ningún requisito	Si está dentro del espacio del Data Center, la propagación del fuego debe estar provista con una separación mínima de 2 horas de todas las demás áreas.	Resistentes a la intemperie exterior
La proximidad a áreas de accesa público	Ningún requisito	Ningún requisito	9 m / 30 pies de separación	19 m / 60 pies de separación

	TIER I	TIER II	TIER III	TIER IV
Seguridad				
Capacidad del UPS de equipo de campo	No contempla	Generador del Edificio + Batería (4horas)	Generador del Edificio + Batería(8 horas)	Generador del Edificio + Batería (24 horas)
La dotación de personal de seguridad por turno.	Ninguna	2 como mínimo	3 cama mínimo	3 como mínimo
Control de accesos de seguridad y monitoreo (verificar control de acceso) en:				
Generadar	Bloqueo de grado industrial	Detección de intrusos	Detección de intrusos	Detección de intrusas
Cuarto de UPS, Teléfono y cuarta de equipos mecánicos y eléctricos.	Bloqueo de grado industrial	Detección de intrusos	Acceso a la tarjeta	Accesa a la tarjeta
Puertas de salida de emergencia	Bloqueo de grado industrial	Vigilancia	Puertas con ciódigo	Egresa por ciódigo
Centro de operaciones de red	Ninguno	Ninguna	Tarjeta de Accesa	Tarjeta de Accesa
Ventanas o aberturas accesibles desde el interior	Monitoreo en ei sitio	Detección de intrusos	Detección de intrusas	Detección de intrusas
Puertas en el cuarto de equipas	Bloqueo de grado industrial	Detección de intrusos	Tarjeta o acceso biométrica (tanto ingreso y salid)	Tarjeta o acceso biométrico (tanto ingreso y salid)

	TIER I	TIER II	TIER III	TIER IV
Monitoreo CCTV (existencia de cámara) en:				
Puertas de cantrol de accesa	No requiere	Si	Si	Si
Perímetro del edificio, estacionamiento, cuarto de UPS, teléfonía, MEP.	No requiere	No requiere	Si	Si
Generadores	No requiere	No requiere	Si	Si
Pisos de cuarto de camputadaras	No requiere	No requiere	Si	Si
Estructural				
La capacidad de carga del piso para las áreas de equipos debe ser.	7,2 kPa (150 lbf / pies 2)	8,4 kPa (175 lbf / pies 2)	12 kPa (250 lbf / pies 2)	12 kPa (250 lbf / pies 2)
Instalaciones de los Data center en zonas sísmicas.	Ninguna restricción	Ninguna restricción	Ninguna restricción	En la Zona 0, 1, 2 debe haber sido diseñado para los requisitos de una Zona Sísmica 3. En las zona sísmica 3 Y 4 corresponde la Zona 4.
Equipo de comunicaciones racks/ gabinetes anclados a la base o con soporte en la base y arriba (especialmente las que contienen a los servidores)	Ningún requisito	Solo la base	Totalmente acoplados	Tatalmente acaplados

Tabla N° B.4: Criterios de auditoría en seguridad física según TIER (Arquitectónico)

ELÉCTRICO	TIER I	TIER II	TIER III	TIER IV
Requisito General				
Número de vías de distribución o rutas de alimentación.	1	1	1 activo y 1 pasiva	2 activos
El sistema permite el mantenimiento concurrente (sin shut down)	No	No	Si	Si
Todos los equipos del sistema eléctrico deben estar etiquetados con certificación de un laboratorio de prueba.	Si	Si	Si	Si
Puntos únicos de fallo	Uno a más puntos sencillos de falla para el sistema de distribución que alimentan al equipo eléctrico o HVAC	Uno o más puntos sencillos de falla para el sistema de distribución que alimentan al equipo eléctrico o HVAC	No hay puntos únicos de fallo	No hay puntos únicos de fallo
Sistema de transferencia de carga crítica	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía	Switch de transferencia automática con bypass de mantenimiento para reparar el switch con interrupción de energía. Cambio automático de la línea al generador cuando ocurre un corte de energía
Generadores correctamente dimensionados de acuerdo a la capacidad instalada de UPS.	Se pide	Se pide	Se pide	Se pide

	TIER I	TIER II	TIER III	TIER IV
Capacidad del generador de combustible (a carga completa)	8 horas	24 horas	72 horas	96 horas
Equipo de apoyo (UPS y transformadores)				
Redundancia del UPS	N	N+1	N+1	2N
Distribución de energía del UPS y nivel de voltaje	Nivel de voltaje 120 / 208V para cargas de hasta 1440 kVA y 480 V para cargas superiores a 1440 kVA	Nivel de voltaje 120 / 208V para cargas de hasta 1440 kVA y 480 V para cargas superiores a 1440 kVA	Nivel de voltaje 120 / 208V para cargas de hasta 1440 kVA y 480 V para cargas superiores a 1440 kVA	Nivel de voltaje 120 / 208V para cargas de hasta 1440 kVA y 480 V para cargas superiores a 1440 kVA
Alimentación de UPS para todo el equipo informático y de telecomunicaciones	No exige	No exige	Si	Si
El UPS en el panel de distribución debe ser independiente para equipos informáticos y de telecomunicaciones.	No exige	Si	Si	Si
Topología del UPS	Módulo sencillo	Único módulo o módulo redundante en paralelo	Módulo redundante en paralelo o módulos redundantes distribuidos o sistema de bloqueo redundante	Módulo redundante en paralelo o módulos redundantes distribuidos o sistema de bloqueo redundante
Bypass de mantenimiento de UPS	Energía tomoda del mismo	Energía tomoda del mismo	Energía tomada del mismo	Energía tomada de un UPS de reserva alimentado con un bus diferente
Los componentes redundantes (UPS) deben ser:	Diseño estático UPS.	Diseño de UPS estático o rotativo. Convertidores de M-G rotativo	Diseño de UPS estático o rotativo. Convertidores estáticos	Diseño de UPS estática, rotativo o híbridos

	TIER I	TIER II	TIER III	TIER IV
El PDU (unidades de distribución de energía)debe alimentar todo el equipo informático y de telecomunicaciones	No	No	Si	Si
Transformadores de factor K debe estar instalados en el PDU	Sí, pero no es obligatorio si se utilizan transformadores de cancelación de armónicos	Sí, pero no es obligatorio si se utilizan transformadores de cancelación de armónicos	Sí, pero no es obligatorio si se utilizan transformadores de cancelación de armónicos	Sí, pero no es obligatorio si se utilizan transformadores de cancelación de armónicos
Puesta a tierra				
Infraestructura de conexión a tierra del Data Center.	No requerido	No requerido	Si	Si
Debe haber un sistema de pararrayos	Con base en el análisis de riesgos de acuerdo con la norma NFPA (Asociación Nacional de Protección contra Incendios) 780 y los requisitos de seguro.	Con base en el análisis de riesgos de acuerdo con la norma NFPA 780 y los requisitos de seguro.	Si exige	Si exige
Botón de apagado de emergencia (EPO)	Si	Si	Si	Si
Supervisión o monitoreo del Sistema eléctrico				
Debe haber un control remoto	No	No	Si	Si
Debe estar localmente mostrada en el UPS (display)	Si	Si	Si	Si
Debe realizarse un envío de mensajes de texto automático al localizador del ingeniero de servicio para una notificación.	No	No	No	Si

	TIER I	TIER II	TIER III	TIER IV
Configuración de baterías				
Debe de haber una cadena de batería común para todos los módulos	Si	No	No	No
Debe haber una cadena de batería por módulo.	No	Si	Si	Si
El tiempo mínimo de stand by a carga completa debe ser:	5 minutos	10 minutos	15 minutos	15 minutos
Tipo de batería debe ser:	Una batería VRLA (batería de ácido-plomo regulada por válvula) o de tipo inundado	Una batería VRLA (batería de ácido-plomo regulada por válvula) o de tipo inundado	Una batería VRLA (batería de ácido-plomo regulada por válvula) o de tipo inundado	Una batería VRLA (batería de ácido-plomo regulada por válvula) o de tipo inundado
Baterías Tipo Inundados				
Deben haber placas envueltas	No	Si	Si	Si
Se debe realizar pruebas de batería a carga completa con un calendario de inspección	Cada dos añas	Cada dos años	Cada dos años	Cada 2 años a cada aña
Debe estar instalado el contenedor de derrames de ácido.	Si	Si	Si	Si
Cuarto de batería				
Debe estar separado del cuarto de equipos	Na existe	Si	Si	Si
Las cadenas individuales de batería deben estar aisladas unos de otros.	No existe	Si	Si	Si
La puerta del cuarto de baterías deber ser de vidrio a prueba de golpes.	No existe	No exige	No exige	Si

	TIER I	TIER II	TIER III	TIER IV
Sistema de monitoreo de la batería debe ser:	No existe	Autocontrol UPS	Autocontrol UPS	Sistema automatizado y centralizado para comprobar cada célula para la temperatura, el voltaje y la impedancia
Ambientes del sistema UPS rotativo (con generadores de diésel)				
Estas unidades deben estar separadas por paredes anti fuego.	No exige	No exige	Na exige	Si
Los tanques de combustible deben estar en el exterior	No	No	Na	Si
Los tanques de combustible deben estar en la misma habitación que las unidades.	Si	Si	Na	No
Sistemas de generación en stand by				
El dimensionamiento del generador debe ser:	Clasificado solamente para ordenadores y sistema de telecomunicaciones tanto mecánico como eléctrico	Clasificado solamente para ordenadores y sistema de telecomunicaciones tanto mecánico como electrico	Clasificado para la computadora y sistema de telecomunicaciones tanto mecánico como eléctrico solamente + 1 repuesto	Para todo edificio + un repuesto
Deben haber generadores de un solo bus	Si	Si	Si	No
Generador individual por sistema con generador de repuesto (1)	Nc	Si	Si	Si

	TIER I	TIER II	TIER III	TIER IV
83 pies de protección de pozo a tierra individual para cada generador.	No	Si	Si	Si
Banco de carga para la prueba de UPS y generador				
Las pruebas de UPS deben ser únicamente módulos.	Si	Si	Si	No
Se deben dar pruebas solamente de generadores.	Si	Si	Si	No
Se debe realizar prueba de los dos módulos UPS y generadores.	No	No	No	Si
Mantenimiento de Equipo				
Debe haber un personal de mantenimiento	En un turno de día solamente en el sitio. De guardia en otras ocasiones	En un turno de día solamente en el sitio. De guardia en otras ocasiones	24 horas en el sitio de lunes a viernes, de guardia los fines de semana con llamada	En sitio 24/7
Debe haber un programa de mantenimiento preventivo	Ningún requisito	Ningún requisito	Programa de mantenimiento preventivo limitado	Programa de mantenimiento preventivo integral
Debe haber programas de capacitación de instalaciones.	Ninguno	Ninguno	Programa de formación integral	Programa de capacitación integral que incluye los procedimientos de operación manual si es necesario pasar por alto el sistema de control.

Tabla N° B.5: Criterios de auditaría en seguridad física según TIER (Eléctrico)

MECÁNICO	TIER I	TIER II	TIER III	TIER IV
General				
Las rutas de tuberías de agua y desagüe no deben asociarse al equipo del Data Center.	Permitido pero no se recomienda	Permitido pero no se recomienda	No permitido	No permitido
Debe haber desagües de piso en la sala de ordenadores para drenar agua condensada, agua del humidificador, y el agua de la descarga de rociadores.	Si	Si	Si	Si
Sistema Refrigerado por agua, por agua helada o por aire				
Unidades terminales de aire acondicionada en interiores	No hay unidades de aire acondicionado redundantes	Una unidad de aire acondicionado redundante por área crítica	Cantidad de unidades de aire acondicionado suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica	Cantidad de unidades de aire acondicionado suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica
Control de humedad para la sala de ordenadores	Humidificación proporcionado	Humidificación proporcionado	Humidificación proporcionado	Humidificación proporcionado
Servicio eléctrico al equipo aire acondicionado	Trayectoria individual de energía eléctrica para los equipos de aire acondicionado	Trayectoria individual de energía eléctrica para los equipos de aire acondicionado	Múltiples caminos de energía eléctrica para los equipos de aire acondicionado. Conectado de forma de tablero de ajedrez para la redundancia de enfriamiento	Múltiples caminos de energía eléctrica para los equipos de aire acondicionado. Conectado de forma de tablero de ajedrez para la redundancia de enfriamiento

	TIER I	TIER II	TIER III	TIER IV
Sistema de rechazo de Calor (si el sistema refrigeración es de agua o de agua helada)				
Refrigeradores secos (sistema de refrigeración de agua)	Na hoy refrigeradores secos redundantes	Un enfriador seco por sistema redundante	Cantidad de enfriadores secos suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica	Cantidad de enfriadores de secos suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica
Enfriadores de líquido de circuito cerrado (sistema de refrigeración de agua)	No hay enfriador de fluida redundantes	Un enfriador de fluido par sistema redundante	Cantidad de enfriadores de fluido suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica	Cantidad de enfriadores de fluido suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica
Bombas de circulación de agua (sistema de refrigeración de agua)	No hay bombas de agua del condensador redundante	Una bomba de agua del condensador por sistema redundante	Cantidad del condensador bombea agua suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica	Cantidad del condensador bombea agua suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica
Sistema de tuberías (sistema de refrigeración de agua)	Sistema de agua del condensador ruta individual	Sistema de agua del condensador ruta individual	Sistema de agua del condensador ruta dual	Sistema de agua del condensador ruta dual
Sistema de tuberías de agua helada (sistema de refrigeración de agua helada)	Ruta individual sistema de agua helada	Ruta individual sistema de agua helada	Camina de doble sistema de agua helada	Camino de doble sistema de agua helada

	TIER I	TIER II	TIER III	TIER IV
Bombas de agua helada (sistema de refrigeración de agua helada)	No hay bombas de agua helada redundante	Una bomba de agua helada por sistema redundante	Cantidad de Bombas de agua helada suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica	Cantidad de Bombas de agua helada suficiente para mantener área crítica durante la pérdida de una fuente de energía eléctrica
Torres de refrigeración (sist ma de refrigeración de agua helada)	No hay torre de refrigeración redundante	Una torre de refrigeración redundante por sistema	Cantidad de torres suficientes para mantener área crítica durante la pérdida de una fuente de energía eléctrica de refrigeración	Cantidad de torres suficientes para mantener área crítica durante la pérdida de una fuente de energía eléctrica de refrigeración
Refrigerada par aire a agua helada	Na haya refrigerada redundante	Un sistema refrigerada redundante	Cantidad de torres suficientes para mantener área crítica durante la pérdida de una fuente de energía eléctrica de refrigeración	Cantidad de torres suficientes para mantener área crítica durante la pérdida de una fuente de energía eléctrica de refrigeración
Sistema de control de HVAC				
Sistema de cantrol	Si falla el sistema de control interrumpirá la refrigeración a las áreas críticas	Si falla en el sistema de control na interrumpirá la refrigeración a las áreas críticas	Si falla en el sistema de control no interrumpirá la refrigeración a las áreas críticas	Si falla en el sistema de control no interrumpirá la refrigeración a las áreas críticas

	TIER I	TIER II	TIER III	TIER IV
Fuente de alimentación para el sistema de control de climatización (HVAC).	Camino individual de energía eléctrica al sistema de control HVAC	Redundante fuente eléctrica, de UPS para los equipos de HVAC	Redundante fuente eléctrica, de UPS para los equipos de HVAC	Redundante fuente eléctrica, de UPS para los equipos de HVAC
Sistema de combustible				
Bombas y tuberías de los tanques de almacenamiento	Bomba individual y / o tubería de suministro	Bombas Múltiples, múltiples tuberías de suministro	Bombas Múltiples, múltiples tuberías de suministro	Bombas Múltiples, múltiples tuberías de suministro
Volumen de los tanques de almacenomiento	Tanque de almacenamiento individual	Tanques de almacenamiento múltiples	Tanques de almacenamiento múltiples	Tanques de almacenamiento múltiples
Supresión de incendios				
Sistema de detección de incendios	No exige	Si	Si	Si
Sistema de rociadores contra incendios	Cuondo se requiera	Cuando seo necesario	Cuando sea necesario	Cuando sea necesario
Sistema de supresión de gaseosa	No	Na	Agentes de limpieza que figuran en la norma NFPA 2001	Agentes de limpieza que figuran en la norma NFPA 2001
Alerta temprana del sistema de detección de humo	No	Si	Si	Si
Sistema de detección de fugas de agua	No	Si	Si	Si
Temperatura del ambiente	18 a 27 °C	18 a 27 °C	18 a 27 °C	18 a 27 °C
Humedad	30 a 60 %	30 a 60 %	30 a 60 %	30 a 60 %

Tabla N° B.6: Criterios de auditoría en seguridad física según TIER (Mecánico)

ANEXO C

C.1: Fotografías tomadas al momento de la visita al Data Center de la Municipalidad

Local central de la Municipalidad

Oficina de la Sub-Gerencia de Sistemas

Lobby de entrada del Data Center

Control para activar o desactivar la alarma de intrusos

Escalera del sótano

Puerta del Data Center

Cerradura electrónica

Vista General del Data Center

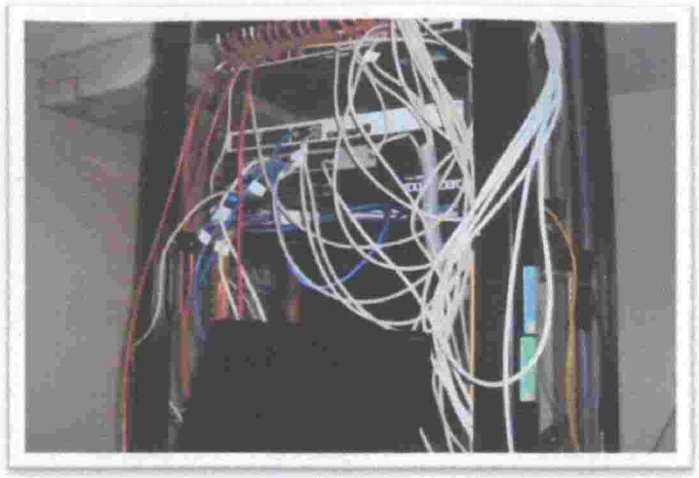
Luces del Data Center

Alarma de Intrusos y dispositivo de detección de Incendios

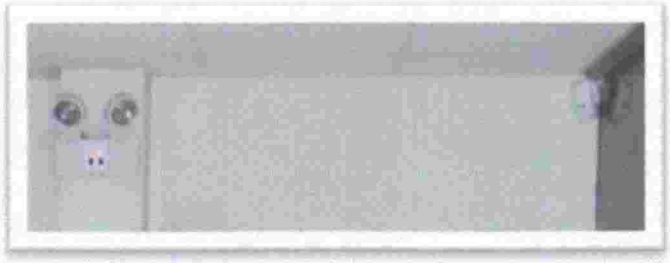
Puerta abierta para el Ingreso al Data Center

Piso y falso piso

Sensor de humedad colocado debajo del falso piso



Cables de datos



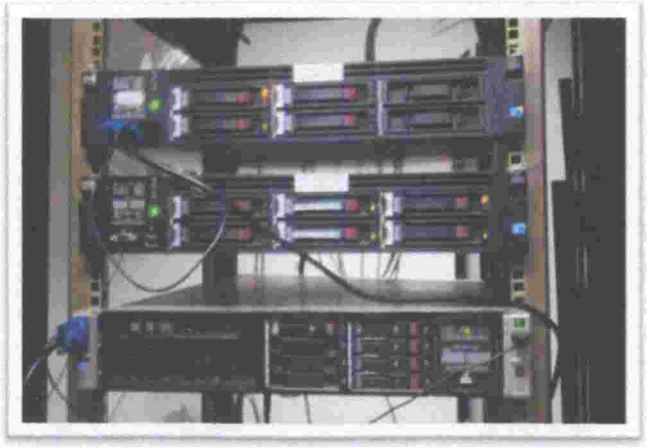
Luces de emergencia (izquierda) y sensor de intrusos (derecha)

Tablero de distribución elétrica

Señales de emergencia

Extintores

Equipo regulador



Servidores

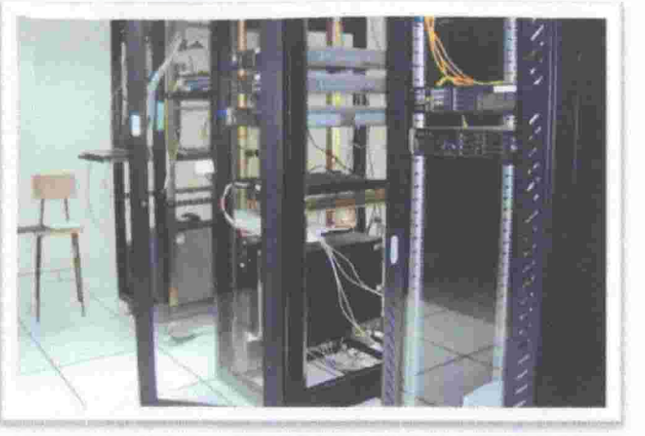
Servidor

Aire Acondicionado de precisión

Aire acondicionado de confort

Central telefónica

Dispositivo para medir la temperatura

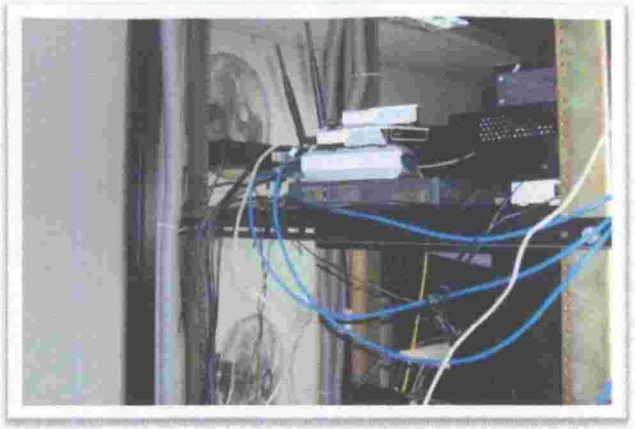


Racks

UPS

Techo falso

Vista general del cableado



Router y switch

Puerta principal del sótano

Pozo a tierra (colocado en un jardin práximo)