UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN - TACNA

Facultad de Ingeniería

Escuela Profesional de Ingeniería en Informática y Sistemas

EVALUACIÓN DE LA GESTIÓN DE RIESGOS PARA EL DATA CENTER DE LA MUNICIPALIDAD DISTRITAL DE ILABAYA BASADA EN LA ISO 31000, TACNA 2016

TESIS

Presentada por:

Bach. Mariella Olga Condori Joaquin

Para optar el Título Profesional de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

TACNA – PERÚ

2018

UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN, TACNA

FACULTAD DE INGENIERÍA

JURADO CALIFICADOR Y CALIFICACIÓN DE LA SUSTENTACIÓN DE TESIS

TESIS Nº _____

TITULO PROFESIONAL DE

Ingeniero en Informática y sistemas

La Secretaría Académica de la Facultad de Ingeniería, por resolución de Facultad Nº 04041-2017-FAIN/UNJBG, designó Jurado para la sustentación oral de la Tesis titulada: "Evaluación de la Gestión de Riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basada en la ISO 31000, Tacna 2016"

El mismo que está conformado por

Presidente: Mgr. Gianfranco Málaga Tejada
Secretario: MSc. Edgar Aurelio Taya Acosta
Vocal: Dr. Edwin Hinojosa Ramos
Para calificar la sustentación de la Tesis en acto público el día 20 de Enero del 2017.

Presentado por el Bachiller Mariella Olga Condori Joaquin, de la Escuela Académico Profesional de Ingeniería en Informática y Sistemas.

El Jurado Calificador en forma secreta e individual emitió su opinión sobre el tema de la tesis expuesta y procedió a obtener el promedio que arrojó el calificativo de aprobado con la nota de Doce (12).

Para ratificar lo detallado firman:

Mgr. Gianfranco Málaga Tejada
Presidente

MSc. Edgar Aurelio Taya Acosta
Secretario

Dr. Edwin Hinojosa Ramos
Vocal

UNIVERSIDAD NACIONAL JORGE BASADRE GROHMANN, TACNA

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

"EVALUACIÓN DE LA GESTIÓN DE RIESGOS PARA EL DATA CENTER DE LA MUNICIPALIDAD DISTRITAL DE ILABAYA BASADA EN LA ISO 31000, TACNA 2016"

TESIS SUSTENTADA Y APROBADA EL 20 DE ENERO DEL 2017 ESTANDO EL JURADO CALIFICADOR INTEGRADO POR:

Presidente:

Mgtr. Gianfranco Alexey Málaga Tejada
Presidente

Secretario:

MSc. Edgar Aurelio Taya Acosta
Secretario

Vocal:

Dr. Edwin Antonio Hinojosa Ramos
Vocal

Asesor:

Dr. Erbert Francisco Osco Mamani

Agradecimiento

Dedico este trabajo principalmente a Dios, por haberme acompañado y guiado a lo largo de mi carrera, por ser mi fortaleza en los momentos de debilidad y sobre todo porque está conmigo en cada paso que doy.

A mi familia, por darme todo su apoyo y quererme por sobre todas las cosas, por haberme inculcado valores; gracias a ellos tuve la oportunidad de tener una excelente educación en el transcurso de mi vida y sobre todo por ser un excelente ejemplo de vida a seguir.

A mi asesor, Dr. Erbert Osco, que siempre estuvo dispuesto a escucharme y a ofrecerme las claves que me han permitido afrontar las dificultades surgidas, y por haber compartido sus conocimientos.

A mis profesores de la Escuela Profesional de Ingeniería en Informática y Sistemas por brindarme sus conocimientos y guiarme a ser mejor persona no solo en lo profesional.

Dedicatoria

A mi amada madre Felicita, por ser el pilar más importante de mi vida; por demostrarme siempre su amor y apoyo incondicional, sin importar nuestras diferencias de opiniones.

A mi querido padre Florencio, quien con sus consejos ha sabido guiarme para culminar mi carrera profesional, gracias por demostrarme que no hay adversidad que exista cuando el motivo es la familia.

A mis hermanos, por ser el mejor regalo que Dios pudo enviar a mi vida, su existencia es mi motor y motivo por el cual debo esforzarme a ser una mejor persona.

A todos mis amigos, compañeros de trabajo y personas que fueron parte y apoyo en esta etapa de mi vida.

CONTENIDO

ANEXOS

ANEXO 01: Matriz de consistencia

ANEXO 02: Instrumento aplicado para la variable: gestión de riesgos

ANEXO 03: Base de datos del cuestionario

ANEXO 04: Confiabilidad del instrumento

ANEXO 05: Resultado de los indicadores

ANEXO 06: Fichas de validación del instrumento

ANEXO 07: Fotos

ANEXO 08: Plan Operativo Institucional de la MDI

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

En la presente tesis que lleva por título “Evaluación de la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basada en la Norma ISO 31000, Tacna 2016”, que tiene como objetivo evaluar la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya; la evaluación está basada en la Norma ISO 31000:2009 gestión del riesgo – principios y directrices.

El diseño de la investigación es de tipo descriptivo simple, este diseño busca y recoge información actual con respecto a una situación previamente determinada, es decir busca conseguir información para poder tomar una decisión. El instrumento que se utilizó para medir la única variable gestión de riesgos, fue un cuestionario validado por tres expertos, el cual fue aplicado al personal administrativo y técnico de la Sub Gerencia de Tecnologías de la Información y Comunicaciones (SGTIC) de la Municipalidad Distrital de Ilabaya (MDI).

Los resultados obtenidos del cuestionario aplicado muestran que existe un porcentaje del 47,5 % del grado de cumplimiento de la ISO 31000:2009 sobre el proceso gestión de riesgos, además se demuestra el cumplimiento de los requisitos por dimensiones: dimensión 1 (establecer contexto) con un 12,5 % del porcentaje total obtenido, dimensión 2

(identificar riesgos) con un 17,5 % del porcentaje total obtenido, dimensión 3 (analizar riesgos) con un 11,25 % del porcentaje total obtenido y dimensión 4 (evaluar riesgos) con un 6,25 % del porcentaje total obtenido, demostrando que este proceso está en un nivel medio de cumplimiento de la Norma ISO 31000 por parte de la institución.

Asimismo, en el trabajo de investigación se realiza un análisis que permitió mostrar el estado actual del Data Center de la Municipalidad Distrital de Ilabaya, de tal manera se pudo identificar de manera clara y clasificada los activos y amenazas existentes y poder llevar la evaluación de la gestión de riesgos de manera óptima para obtener mejores resultados y conclusiones.

INTRODUCCIÓN

La información de una organización es uno de los activos más importantes que posee, debido a que tiene un impacto directo en la toma de decisiones que se realizan a diario.

La situación de hoy en día ha demostrado que las empresas de cualquier rubro deben contar con una adecuada gestión de riesgos, la cual asegure la garantía de sus activos, procesos y demás, para que la organización pueda continuar sin problemas su trabajo diario y evitando una interrupción en la consecución de sus objetivos.

Es por ello que se considera la Norma ISO 31000:2009, la cual establece los principios y directrices para una realizar una gestión eficaz de los riesgos, además dicha norma proporciona las nociones básicas que se debe tener en cuenta en cualquier organización para la implementación de un sistema de gestión de riesgos.

El presente trabajo de investigación tiene como finalidad evaluar la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basada en la ISO 31000:2009 y se divide en los siguientes capítulos:

En el Capítulo I se describe los antecedentes del problema, se define el problema de la investigación, la formulación del problema, seguido de la justificación de la investigación, los alcances y limitaciones, se representa las variables del estudio, y el diseño de investigación.

En el Capítulo II se presenta el sustento del marco teórico de la investigación, en donde se realiza la recopilación de información bibliográfica relacionados al tema de la investigación, en la cual se detallan las bases teóricas que serán necesarias para el desarrollo del proyecto.

En el Capítulo III se hace referencia a las técnicas e instrumentos de recolección de datos para la variable en estudio, y la propuesta para el futuro tratamiento de los riesgos que resultaron priorizados en el Data Center de la Municipalidad Distrital de Ilabaya.

En el Capítulo IV se presenta los resultados obtenidos y discusiones de la investigación, en el cual se presenta los resultados alcanzados tras la aplicación del instrumento descrito.

Finalmente, se muestran las conclusiones, recomendaciones del trabajo de investigación y anexos del mismo.

CAPÍTULO I

PLANTEAMIENTO DEL ESTUDIO

1.1. Descripción del problema

1.1.1. Antecedentes del problema

Para apoyar la investigación se indagaron en distintos trabajos, publicaciones, revistas vinculadas a la gestión de riesgos y a la Norma ISO 31000:2009, siendo estos un gran aporte significativo. A continuación se presentan en síntesis una serie de investigaciones que se encuentran en el ámbito de la problemática de la presente investigación.

A nivel internacional se han encontrado diversos trabajos de investigación como la siguiente tesis que lleva por título “Elaboración de un modelo de gestión de riesgos de tecnologías de información para la Fiscalía General del Estado” de Chillogallo & Zambrano (2016), hace mención a la gestión de riesgos para la Fiscalía General del Estado de Ecuador y en particular para la Dirección de Tecnologías de la mencionada institución, proponiendo elaborar y validar un modelo de gestión de riesgos de tecnologías de la información con una propuesta metodológica basada en estándares internacionales como la NTE INEN-

ISO 31000 y NTE INEN-ISO/IEC 27005:2012 para el salvaguardo y cuidado de la información la institución accediendo gestionar los riesgos y continuar con la consecución de objetivos de la misma.

Se aplicó un cuestionario como instrumento en el trabajo de Chillogallo & Zambrano (2016), para tener una visión macro del nivel de cumplimiento del nivel de gestión de riesgos que tiene la institución; obteniendo los siguientes resultados, para la fase de establecimiento del contexto se obtuvo un 19,93 % que indica que la Dirección de Tecnologías al menos tiene una visión de los requisitos para identificar las características internas y externas de la institución pero aún no con total claridad, para la fase de identificación de riesgos se obtuvo un 25,38 % que indica que las reuniones de trabajo son apoyo fundamental para los administradores de tecnologías de la información para identificar de la mejor forma los riesgos institucionales de tal manera se propone establezcan mejor sus roles, para la fase de análisis de riesgos se obtuvo un 27,83 % que indica que deben mejorar la identificación de riesgos y asignación de recursos que deben ser claramente identificados, la fase de evaluación de riesgos obtuvo un 22,33 % que indica la debilidad en cuanto a realización de evaluaciones de riesgos de tecnologías de la información en la organización, donde no se muestra claramente las prioridades para la ejecución de actividades para la reducción de riesgos,

para la fase tratamiento de riesgos se obtuvo un 11 % que indica que no se evalúan propuestas de tolerancia de riesgos de manera adecuada, la fase de monitoreo y revisión obtuvo un 25,03 % que indica que no cuentan con políticas de riesgos ni planes de acción para la gestión de riesgos y para la fase de comunicación y consultas se obtuvo un 24,06 % que indica que no existe capacitación del personal de la institución en cuanto a identificación de riesgos. El resumen se ve en la Tabla 1.

Tabla 1
Nivel de cumplimiento general de gestión de riesgos de la dirección de TI

Fases	Distribución de las preguntas	Promedio de cumplimiento de las fases (%)
Establecimiento del contexto	Pregunta 7;19;20;23;24	19,93
Identificación de riesgos	Pregunta 8;16;17;18;21;25;30	25,38
Análisis de riesgos	Pregunta 9;10	27,83
Evaluación de riesgos	Pregunta 1;13;15	22,33
Tratamiento de riesgos	Pregunta 2;3;14	11
Monitoreo y revisión	Pregunta 4;11;22;26;27;28;31;32;33; 34;35;36	25,03
Comunicación y consultas	Pregunta 5;6;12;29;37;38	24,06
	Totales	22,22

Fuente: Chillogallo & Zambrano – Elaboración de un modelo de gestión de riesgos de tecnologías de información para la Fiscalía General del Estado

Entre sus conclusiones establece que los modelos de gestión de riesgos actuales cumplen apropiadamente con las etapas básicas de gestión, pero se debe en lo posible ajustar las características de estos modelos para que sean personalizados a la realidad institucional, así

mismo, menciona que se requiere de capacitación y comunicación de las políticas a los funcionarios que tienen actividades de coordinación, ya que si no se gestiona activamente la capacitación no se puede esperar que el equipo de apoyo reaccione adecuadamente a un eventual escenario de riesgo. (Chillogallo & Zambrano, 2016)

Así mismo, se encuentra la tesis titulada “Elaboración de una guía de gestión de riesgo basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia” de Arias, Dias, & Vargas (2014) se busca elaborar una guía de gestión de riesgos en el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia, donde sea posible establecer el riesgo presente en los subprocesos que ahí existan y poder realizar una gestión adecuada de este, para llegar a obtener un cumplimiento de los objetivos de manera eficaz y eficiente en las organizaciones. Señala también que la investigación beneficia a las empresas que están interesadas en conocer el funcionamiento de la gestión de los riesgos tecnológicos a los que están expuestos, ya que les brinda la oportunidad de tomar las medidas necesarias para minimizar las vulnerabilidades y amenazas que se puedan presentar, tomando como guía la norma NTC-ISO 31000 que

indica los requerimientos para realizar una buena gestión; esto siempre y cuando las mismas estén dispuestas a conocerlas y aplicarlas.

Por otro lado, Enriquez & Hidalgo (2015) en el artículo científico titulado “Metodología de valuación de riesgos como parte del Sistema de Gestión de Seguridad de la Información (SGSI) aplicado a un Data Center de Alta gama”, se presenta una metodología para gestionar el riesgo como una parte de un Sistema de Gestión de Seguridad de la Información basado en los lineamientos de la Norma ISO/IEC 27005:2008 tecnología de la información - técnicas de seguridad - gestión del riesgo de seguridad de la información. La metodología se enfoca en la valoración de activos, impactos y riesgos, como parte del análisis de riesgos; en la evaluación del riesgo y en la aplicación de controles sobre los activos de información de una Data Center de gama alta. Entre sus conclusiones afirma que la aplicación de ciertos controles puede eliminar o reducir de forma significativa los riesgos de seguridad además de hablar sobre la efectividad de los controles que varía dependiendo del tipo de activos a proteger, las dimensiones de seguridad consideradas y las amenazas que se pretende conjurar. Para medir la efectividad de los controles es necesario realizar una retroalimentación del análisis de riesgos utilizando la metodología propuesta.

Del mismo modo Arteaga, Villa, & Ladino (2014) en el artículo científico titulado “Definición de una metodología de gestión de riesgos para entidades del sector público bajo el estándar ISO 27001” se menciona que es necesario el uso de un modelo o metodología para la definición y análisis de riesgos asociados a los activos de información para la construcción del mapa de riesgos de dichos activos, que sirva como instrumento guía para emprender acciones tendientes a la reducción de la afectación a la integridad, confidencialidad y disponibilidad de la información, a partir del análisis comparativo y la evaluación de los diferentes modelos y metodologías disponibles en el medio para la evaluación de riesgos, se elaboró una metodología que cumpla con los requerimientos de la Norma ISO/IEC 27001:2005 tecnología de la información – técnicas de seguridad – sistemas de gestión de seguridad de la información – requerimientos, y se adapte a las características propias de las entidades públicas.

En el trabajo de investigación mencionado de Arteaga, Villa, & Ladino (2014) se aplica la metodología en un caso práctico de tal forma concluyó lo siguiente, la aplicación de la metodología de gestión de riesgos permite que los líderes de los procesos participen y proporcionen la información necesaria para darle el tratamiento adecuado a los activos de la información. El paso a paso de la metodología de la gestión de

riesgos permitió la aplicación de los instrumentos de una manera más sencilla para los involucrados en el proceso además que fue el insumo para definir la Política General de Seguridad de la Información y las asociadas a cada aspecto de la Norma ISO/IEC 27001:2005 tecnología de la información – técnicas de seguridad – sistemas de gestión de seguridad de la información – requerimientos, así como los lineamientos.

De tal manera, se tiene el siguiente trabajo de investigación de Quintero, Ascanio, & Cardenas (2015) que lleva por título “Guía de gestión de riesgos para el departamento de sistemas de la Empresa Apuestas Cúcuta 75” tiene como objetivo diseñar una guía para gestionar los riesgos de cualquier nivel o ámbito de aplicación (estratégico, tecnológico, operativo, financiero o de cumplimiento) del departamento de sistemas de la empresa Apuestas Cúcuta 75, pudiéndose aplicar también a un rango de actividades incluyendo estrategias, decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos. De tal forma, concluye que el desarrollo del proyecto permitió la identificación de estándares, normativas y técnicas especializadas para la valoración e implementación de acciones para dar tratamiento a los riesgos.

A nivel nacional se encontró el artículo científico de Sotelo, Torres, & Rivera (2012) titulado “Un proceso práctico de análisis de riesgos de

activos de información", se presenta un proceso de análisis de riesgos de activos de información, en el contexto de un sistema de gestión de seguridad de información alineado al estándar ISO/IEC 27001:2005 tecnología de la información - técnicas de seguridad - sistemas de gestión de seguridad de la información - requerimientos, este proceso sigue los lineamientos de los principales estándares y buenas prácticas en gestión de riesgos y seguridad de la información. Utiliza el marco referencial Magerit e incorpora el análisis del impacto de negocio, el cual tiene por objetivo evaluar el impacto sobre los procesos de negocio, debido a la no disponibilidad de los servicios de tecnologías de la información, lo que posteriormente se deriva del nivel de criticidad para cada activo de información, lo cual es indispensable para establecer el nivel de riesgo de los mismos.

1.1.2. Problemática de la investigación

A nivel mundial la incorporación de las nuevas tecnologías a la administración pública ya lleva realizándose desde hace muchos años, pero el reto está en aprovechar todas las ventajas que éstas pueden aportar y sobretodo en seguir el ritmo que demanda la sociedad. La administración tiene la obligación de adaptarse a una sociedad en constante movimiento, que incorpora la tecnología como un elemento más

de su realidad y ante la que tiene el desafío de responder en la misma medida. (Fundación Telefónica, 2016)

La realidad de la administración es muy compleja (…) En cualquier caso lo cierto es que las Tecnologías de la Información y Comunicaciones (TIC) apoyan mucho valor tanto a la relación con el ciudadano (la llamada e-Administración) como a la gestión interna. A medida que los modelos de incorporación de las TIC se vayan “abriendo” el impacto en la eficiencia en la Administración será mayor. Se trata de “liberar” recursos que podrán ser utilizados en otros servicios públicos que lo irán requiriendo. (Fundación Telefónica, 2016)

En la actualidad el uso masivo de las TIC en el funcionamiento diario de las organizaciones se ha generalizado. La capacidad de definición y gestión de una estrategia acorde con los objetivos y la estructura organizativa de una institución se ha transformado en una obligación inexcusable para su personal directivo siendo parte de la consecución de sus objetivos. (Macau, 2004)

Las tecnologías poco a poco se han convertido en un instrumento indispensable para las empresas ofreciendo una serie de ventajas, sin embargo, estas tecnologías no están libres de las amenazas latentes de diferentes factores en cualquier organización, no dejándolas libre de los

riesgos por las que puedan ser afectadas, generando así consecuencias que pueden significar pérdidas económicas, humanas entre otras si es que no se cuenta con una adecuada gestión de los riesgos más significativos, y demás que sean perjudiciales al marco de trabajo establecido en la institución.

En el país todas las instituciones públicas, municipalidades, consideran dentro de su estructura funcional el área de Tecnologías de la Información quienes son encargadas de velar por el soporte informático sea a nivel de hardware, software, asesoría informática y distintas funciones propias de la oficina; es por ello que gran parte de la información de las instituciones se encuentras almacenadas en fuentes de almacenamientos informáticos como servidores que están bajo resguardo de las oficinas de Tecnologías de la Información siendo el caso que en la mayoría de ellas no cuentan con una adecuada gestión los riesgos existentes que pueden causar daños perjudiciales, inclusive desestabilizando la consecución de los objetivos de la institución.

La Municipalidad Distrital de Ilabaya cuenta con la Sub Gerencia de Tecnologías de la Información y Comunicaciones en su estructura organizacional, y como parte de sus instalaciones su propio Centro de Datos, en el cual se puede evidenciar deficiencias en la gestión de riesgos

influyendo directamente sobre sus activos; generando así que no se permita identificar, analizar ni evaluar los riesgos, a pesar de los riesgos existentes pero no identificados e incidentes producidos recientemente por no contar con las medidas adecuadas.

En el Data Center de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la MDI se observaron los siguientes puntos, entre los cuales está el discontinuo mantenimiento de los equipos, además de contar con 4 años en uso continuo sin haber sido renovados a lo largo de su periodo de funcionamiento, también uno de los problemas más significativos y perjudiciales son los cortes de luz sin previo comunicado lo cual genera la interrupción de los servicios de los sistemas existentes en la institución, esto implica la pérdida de tiempo y descontento para los usuarios que manipulan los sistemas, entre estos el Sistema Integrado Municipal (SIMUN) el cual es muy utilizado por la Sub Gerencia de Abastecimiento y demás áreas usuarias en el módulo de logística para el procesamiento de cuadros de necesidades, solicitudes de cotización y ordenes de servicio y compras, que son tareas que realizan a diario, otro sistema de importancia es el Sistema de Administración Financiera (SIAF) y el servicio de mensajería instantáneo que lleva por nombre SPARK para la fluida comunicación entre las áreas usuarias.

El problema de los cortes genera retraso en las labores administrativas, debido a la dificultad que presenta al momento de recuperación ante los eventos no programados, ya que los equipos se ven vulnerables y sufren desperfectos al volver a su funcionamiento.

El registro irregular de incidentes ocurridos en el Data Center no permite que se lleve un control de los eventos pasados y tampoco de los eventos reincidentes, de tal forma tampoco permite tomar las medidas necesarias del caso.

Así mismo, se tiene el problema de desconocimiento de las causas de las interrupciones en los servicios de los sistemas municipales, se considera como interrupciones al corte de los servicios mencionados ya que el equipo informático que almacena la información sufre de constantes apagados fortuitos, debido a la inestabilidad del voltaje siendo el caso que aún se desconoce cuál es el motivo que lo provoca.

Entre los últimos sucesos en el Data Center, los que más consecuencias provocó fue el daño que sufrieron los conectores del servidor principal, cuya función era mantener el Servicio del Sistema Integrado Municipal (SIMUN), el cual alberga los archivos de código fuente, la base de datos y los archivos de los certificados digitales generados por los procesos que se realizaban a diario en el sistema por

parte de los usuarios de todas oficinas de la institución; siendo los más perjudicados el personal administrativo de la Sub Gerencia de Abastecimiento que utiliza el subsistema de logística y las áreas responsables de dichos documentos que son los certificados digitales en mención. Este incidente provocó la interrupción del servicio por un lapso de cuatro horas que significa media jornada laboral al día, se tuvo que restablecer el servicio de manera rápida y provisional ya que generaba malestar y demora a los usuarios finales, el incidente mencionado también provocó la pérdida de información importante, tal cual son los certificados digitales de los cuadros de necesidades, términos de referencias, cuadros comparativos, órdenes de compra y órdenes de servicio.

1.2. Formulación del problema

Problema general

¿Cómo es la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basada en la ISO 31000, Tacna 2016?

Problemas específicos

a) ¿Cómo es el contexto del Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?
b) ¿Cómo es la identificación de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?

c) ¿Cómo es el análisis de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?
d) ¿Cómo es la evaluación de los riesgos priorizados para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?

1.3. Justificación

Las tecnologías de la información tienen como fin facilitar los procesos de información y comunicación gracias a los grandes desarrollos tecnológicos que brindan en la actualidad y así poder satisfacer las necesidades de empresas, organizaciones y personas que requieran de estos medios.

Hoy en día se ha visto gran aceptación por las tecnologías de la información en los diversos rubros, tanto como agronomía, comercio, minería, educación, etc, pero no todas las organizaciones o personas dedicadas a estos rubros las utilizan adecuadamente o no las implementan, sea por falta de capacitación, orientación o desconocimiento sobre el adecuado uso de estas tecnologías de la información.

En estos últimos tiempos en los cuales la tecnología se ha convertido en un eje primordial para el manejo de las empresas también se debe tener en cuenta las amenazas que existen y si se produce un

efecto sobre los activos de dichas organizaciones pueden ser perjudiciales, provocando pérdidas económicas, humanas, entre otras; por tal motivo es importante conocer los riesgos existentes y priorizarlos para su debido tratamiento, con la finalidad de salvaguardar la información que es activo primordial de toda organización.

La Municipalidad Distrital de Ilabaya contempla dentro de su Plan Operativo Institucional (ver en Anexo 08) como objetivo estratégico Nº 03 el promover el aprovechamiento de las tecnologías de información de tal manera se realizan actividades para lograr el cumplimiento del objetivo, sea el caso de la Sub Gerencia de Tecnologías de la Información y Comunicaciones, para la cual se realizó un diagnóstico situacional en el cual muestra sus fortalezas, debilidades, oportunidades y amenazas.

En la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya se encuentran los activos importantes que permiten el almacenamiento de la información de la institución y así garantizar su seguridad, sin embargo, no se cuenta con las medidas necesarias para tratar con los posibles riesgos.

1.4. Alcances y limitaciones

- Alcances

El alcance de la presente investigación se ciñe en evaluar la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya, basándose en el ciclo de proceso de la gestión de riesgos de la Norma ISO 31000:2009, dicha evaluación permitió conocer el nivel de cumplimiento de la Norma ISO 31000:2009 que tiene sobre la gestión de riesgos con respecto a la fase de establecimiento del contexto, identificación de riesgos, análisis de riesgo y evaluación de los riesgos. Conociendo los valores resultantes para cada fase se realiza una propuesta la cual describe la situación actual del Data Center de la institución en cuanto a los riesgos, amenazas y vulnerabilidades existentes, así mismo poder valorar dichos riesgos y priorizarlos.

- **Limitaciones**

Para la selección de la población se consideró sólo el personal de la Sub Gerencia de Tecnologías de la Información y Comunicaciones conformado por ingenieros y técnicos con conocimiento sobre las tecnologías de la información y el funcionamiento del Data Center.

Para la investigación no se consideran las fases de tratamiento de

riesgos, monitoreo y revisión de riesgos ni comunicación y consultas, de la misma manera en la propuesta planteada debido a que involucraría tiempo, costo, personal involucrado y aprobación de alta dirección.

1.5. Objetivos

1.5.1. Objetivo general

Evaluar la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000, Tacna 2016.

1.5.2. Objetivos específicos

a) Evaluar el contexto del Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000
b) Evaluar la identificación de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000
c) Evaluar el análisis de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000
d) Evaluar los riesgos priorizados para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000

1.6. Hipótesis

1.6.1. Hipótesis global

La hipótesis se utiliza a veces en estudios descriptivos, para pretender predecir un dato o valor en una o más variables que se van a medir u observarse. Cabe mencionar que no en todas las investigaciones descriptivas se formulan hipótesis de esa clase o que sean afirmaciones más generales. (Hernandez, Fernández, & Baptista, 2010)

La investigación descriptiva se refiere a la etapa iniciadora del trabajo científico, que permite ordenar el resultado de las observaciones de las conductas, las características, los factores, los procedimientos y otras variables de fenómenos y hechos. Ese tipo de investigación no tiene hipótesis explícitas. (Pineda, De Canales, & Alvarado, 1994)

La investigación descriptiva se basa en la información conseguida, a ordenar los rasgos, atributos o características de la realidad observada con respecto al problema indagado, la descripción permite reunir los resultados de la observación en una exposición relacionada de los rasgos del fenómeno que se estudia de acuerdo con criterios que le den coherencia y orden a la exposición de los datos. En el nivel descriptivo de la investigación no se plantean claramente la hipótesis; por consiguiente

no es una condición necesaria para la investigación cualitativa la formulación de hipótesis. (Monje, 2011)

Considerando las anteriores citas, en la presente investigación no se formuló hipótesis ya que por medio de los datos estudiados se consiguió llegar a los objetivos definidos, asimismo, se realizó una propuesta de mejora para la gestión de riesgos para el Data Center de la MDI como aporte del trabajo de investigación, que se encuentra en el Capítulo de desarrollo.

1.7. Variables

1.7.1. Identificación de variables

La variable para el estudio de la investigación es única:

Variable: gestión de riesgos

1.7.2. Definición de variables

Gestión de riesgo

La definición de la variable única que se tiene para la realización de la presente tesis cuenta con cuatro dimensiones, de acuerdo a los límites considerados para el presente proyecto, para la gestión de riesgos según la ISO 31000, los cuales son:

- Establecer el contexto del Data Center de la Municipalidad Distrital de Ilabaya
- Identificar riesgos del Data Center de la Municipalidad Distrital de Ilabaya
- Analizar riesgos del Data Center de la Municipalidad Distrital de Ilabaya
- Evaluar riesgos del Data Center de la Municipalidad Distrital de Ilabaya

1.7.3. Operacionalización de variables

Tabla 2
Operacionalización de variables

Var.	Definición conceptual	Dimensión	Indicadores	Sub indicadores	Escala medición	
GESTIÓN DE RIESGOS	Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo. (ISO73, 2009)	D1: Establecer contexto	I1: Objetivos definidos		P1	Ordinal
			I2: Estrategias definidas		P2	
			I3: Responsables asignados		P3	
			I4: Procesos identificados		P3	
			I5: Recursos identificados		P5	
		D2: Identificar riesgos	I6: Riesgos internos	I6.1: Nivel de control de riesgos internos	P6	
				I6.2: Causas de los riesgos internos	P7	
				I6.3: Consecuencias de los riesgos internos	P8	
			I7: Riesgos externos	I7.1: Nivel de control de riesgos externos	P9	
				I7.2: Causas de los riesgos externos	P10	
				I7.3: Consecuencias de los riesgos externos	P11	
			I8: Fuentes de riesgo		P12	
			I9: Zonas de impacto		P13	
			I10: Controles de gestión de riesgo		P14	
		D3: Analizar riesgos	I11: Probabilidad de ocurrencia		P15	
			I12: Causas		P16	
			I13: Consecuencias		P17	
		D4: Evaluar riesgos	I14: Nivel de riesgo		P18	
			I15: Riesgos priorizados		P19	
			I16: Toma de decisiones		P20	

Fuente: Elaboración propia

1.7.4. Clasificación de variables

Se detalla la clasificación de las variables conforme a su naturaleza y su escala de medición.

- ✓ Variable: gestión de riesgos.
- ✓ Por su naturaleza: cualitativo.
- ✓ Por su escala: ordinal.

1.8. Diseño de la investigación

1.8.1. Diseño experimental o no experimental

La investigación que se realiza sin manipularse intencionadamente las variables, se trata de estudios donde no hace variar en forma intencional las variables independientes para ver su consecuencia sobre las otras variables. Es decir, se observa fenómenos tal como se dan en su contexto natural, para posteriormente analizarlos. (Hernandez et al., 2010)

Diseño descriptivo simple: El diseño de investigador busca y recoge información actual con respecto a una situación previamente determinada, no presentándose la administración o control de un tratamiento, es decir que se busca conseguir información para poder tomar una decisión. (Olano M., 2010)

Para el presente trabajo de investigación se consideró el diseño de la investigación descriptiva simple, el cual se esquematiza de la siguiente forma:

Figura 1. Investigación no experimental descriptiva simple
Fuente: Diseño de Investigación Educacional - Atilio G. Olano Martínez, 2010

M: Representa la muestra del personal de la Sub Gerencia de Tecnologías de la Información y Comunicaciones.

O: Representa la información recogida de la muestra.

Debido a esos fundamentos expuestos se debe tener en cuenta en la investigación, que solo se basó en la recolección de información actual con respecto a una situación objeto de estudio.

1.8.2. Población y muestra

Población

La población es el conjunto de personas, objetos o medidas que poseen algunas características comunes observables en un lugar y en un instante determinado, es decir, serán las personas que intervienen en la investigación a efectuar. (Supo, 2015)

La población son todos los administrativos de la oficina de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya, que son un total de 10 personas.

Tabla 3
Población de la SGTIC de la MDI

Descripción	Cantidad	Porcentaje (%)
Sub Gerente de TIC	1	10
Encargado de Sistemas	1	10
Encargado de Soporte Técnico	1	10
Soporte Técnico - Palacio	3	30
Soporte Técnico - GIDUR	3	30
Personal Administrativo	1	10
Total	10	100

Fuente: Secretaría de la SGTIC de la MDI

Muestra

La muestra se define como un conjunto de objetos y sujetos procedentes de una población, es decir que el conjunto de elementos seleccionado cumplen con determinadas especificaciones. (Monje, 2011)

Según Sampieri, la muestra es un subconjunto de elemento que pertenece a ese conjunto definido en sus características al que llamamos población. (Hernandez et al., 2010)

La muestra censal es aquella donde todas las unidades de investigación son consideradas como muestra.

La muestra fue censal pues se seleccionó el 100 % de la población, para el presente proyecto de investigación va a ser igual a la población (n=N) igual a los 10 empleados que pertenecen a la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya.

1.8.3. Técnicas e instrumento para recolección de datos

Técnica

Los autores (Pineda, De Canales, & Alvarado, 1994) indican que "La técnica se entiende como el conjunto de reglas y procedimientos que le permiten al investigador estableces la relación con el objeto o sujeto de la investigación."

Se aplicó la técnica de la encuesta para la variable (gestión de riesgos), en la cual obtuvo recopilaciones de datos, que ayudo a conocer la Situación actual de la gestión de riesgos en el Data Center con respecto a la Norma ISO 31000:2009.

- Encuesta

Es una averiguación o indagación, acopio de datos obtenidos mediante consulta o preguntas, referentes a estados de opinión, nivel económico o cualquier otro aspecto de la actividad humana, esta se

puede clasificar en abiertas, cerrada y de elección múltiple. (Pestana & Stracuzzi, 2012)

Instrumento

Los autores Pineda, De Canales, & Alvarado (1994) indican que “El instrumento es el mecanismo que utiliza el investigador para recolectar y registrar la información: Entre estos se encuentran los formularios, las pruebas psicológicas, las escalas de opinión y de actitud, las listas y hojas de control, entre otros.”

El instrumento de medición para la técnica seleccionada en la presente investigación fue el siguiente:

- El instrumento de medición que se utilizó para la variable gestión de riesgos fue un cuestionario, el cual se aplicó al personal administrativo de la Sub Gerencia de Tecnologías de la Información y Comunicaciones, el cual se encuentra en el Anexo 02.

1.8.4. Validación y confiabilidad de instrumento

Validación

La validez de un instrumento radica en que mida lo que tiene que medir (autenticidad), al evaluar la validez es necesario saber a ciencia

cierta qué rasgos o características se desean estudiar, a esta característica se le denomina variable criterio. (Corral, 2009)

La validación del instrumento se realizó con el juicio de tres expertos, las fichas de validación de juicios de expertos se encuentran en el anexo 06.

Confiabilidad

De acuerdo con Hernandez et al. (2010) “La confiabilidad de un instrumento de medición se refiere al grado en que su aplicación repetida al mismo individuo u objeto produce resultados iguales.”

Se utilizó el cuestionario referenciado en el Anexo 02 para la variable gestión de riesgos y medir sus indicadores de acuerdo a las preguntas formuladas para cada uno de ellos respectivamente, como se muestra en la Tabla , dicho cuestionario esta validado por tres expertos y se realizó el cálculo del coeficiente del Alfa de Cronbach resultando con un 0,889 aceptando su confiabilidad (Anexo 04)

Tabla 4
Relación de los indicadores con sus respectivas preguntas

Variable	Dimensión	Indicadores	Sub Indicadores	P
GESTIÓN DE RIESGOS	D1: Establecer contexto	I1: Objetivos definidos		P1
		I2: Estrategias definidas		P2
		I3: Responsables asignados		P3
		I4: Procesos identificados		P3
		I5: Recursos identificados		P5
	D2: Identificar riesgos	I6: Riesgos internos	I6.1: Nivel de control de riesgos internos	P6
			I6.2: Causas de los riesgos internos	P7
			I6.3: Consecuencias de los riesgos internos	P8
		I7: Riesgos externos	I7.1: Nivel de control de riesgos externos	P9
			I7.2: Causas de los riesgos externos	P10
			I7.3: Consecuencias de los riesgos externos	P11
		I8: Fuentes de riesgo		P12
		I9: Zonas de impacto		P13
	D3: Analizar riesgos	I10: Controles de gestión de riesgo		P14
		I11: Probabilidad de ocurrencia		P15
		I12: Causas		P16
		I13: Consecuencias		P17
	D4: Evaluar riesgos	I14: Nivel de riesgo		P18
		I15: Riesgos priorizados		P19
		I16: Toma de decisiones		P20

Fuente: Elaboración propia

1.8.5. Análisis de datos

Para el análisis de datos se utilizó el software de cálculos de datos MS Excel 2013 el cual hizo fácil la compresión del estudio de las variables, se calculó del porcentaje total del cumplimiento de la Norma ISO 31000:2009 para la gestión de riesgos en el Data Center explicándolo mediante tablas, gráficos de barra.

CAPÍTULO II

MARCO TEÓRICO

2.1. Bases teóricas

2.1.1. Riesgo

“Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de los esperado positivo y/o negativo.” (ISO73, 2009)

“Se define como la combinación de la probabilidad de un suceso y sus consecuencias pero también se puede definir como la incertidumbre sobre la ocurrencia y la magnitud de un suceso con efectos negativos. Posibilidad de que un peligro se materialice sobre un sujeto causando un daño.” (José-Marti, 2013)

2.1.2. Gestión de riesgo

“Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.” (ISO73, 2009)

“Todas las actividades de una organización implican riesgos. Las organizaciones gestionan el riesgo identificándolo, analizándolo y luego evaluando si el riesgo debe ser modificado por el tratamiento del riesgo

para satisfacer sus criterios de riesgo." (International Organization for Standardization, 2009)

"Una gestión de riesgos eficaz se centra en la identificación y el tratamiento de los riesgos y su objetivo es añadir el máximo valor sostenible a todas las actividades de la empresa, introduciendo una visión común del lado positivo y del lado negativo de aquellos factores potenciales que pueden afectar a la empresa. Aumenta la probabilidad de éxito y reduce tanto la probabilidad de fallo como la incertidumbre acerca de la consecución de los objetivos generales de la empresa." (José-Marti, 2013)

2.1.3. Vulnerabilidad

"Propiedades intrínsecas de algo que se resulta en la susceptibilidad a una fuente de riesgo que puede conducir a un evento con una consecuencia." (ISO73, 2009)

2.1.4. Consecuencia

"Resultado de un evento que afectan a los objetivos." (ISO73, 2009)

"Hecho o acontecimiento que se sigue o resulta de otro." (Real Academia Española, 2016)

2.1.5. Evento

"Ocurrencia o el cambio de un conjunto particular de circunstancias." (ISO73, 2009)

2.1.6. Posibilidad

"… se utiliza para referirse a la oportunidad de que algo definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y se describe el uso de términos generales o matemáticamente tal como una probabilidad o una frecuencia durante un periodo de tiempo determinado." (ISO73, 2009)

2.1.7. Peligro

"Fuente de daño potencial." (ISO73, 2009)

"Riesgo o contingencia inminente de que suceda algún mal." (Real Academia Española, 2016)

2.1.8. Probabilidad

"Medida de la oportunidad de ocurrencia que expresa como un numero entre 0 y 1, donde 0 es imposible y 1 es una certeza absoluta." (ISO73, 2009)

2.1.9. ISO 31000:2009 gestión de riesgos - principios y directrices

“Ofrece principios, un marco y un proceso de gestión del riesgo. Puede ser utilizado por cualquier organización independientemente de su tamaño, actividad o sector. El uso de la norma ISO 31000 puede ayudar a las organizaciones a aumentar la probabilidad de que el logro de objetivos, mejorar la identificación de oportunidades y amenazas y eficaz asignar y utilizar los recursos para el tratamiento del riesgo.” (International Organization for Standardization, 2016)

Esta norma internacional proporciona los principios y las directrices genéricas sobre la gestión del riesgo. Puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, no es específica de una industria o sector concreto. (Serra, 2016)

Principios y directrices: Contiene 11 principios expuestos:

- ✓ La gestión crea valor a la organización.
- ✓ Debe estar integrada a los procesos.
- ✓ Forma parte de la toma de decisiones en la empresa.
- ✓ Trata de forma explícita la incertidumbre.
- ✓ Debe ser sistemática, estructurada y adecuada.
- ✓ Es necesario que esté basada en la mejor información disponible.
- ✓ Debe adaptarse a la medida de cada caso.
- ✓ Implica la inclusión de factores humanos y culturales.

- ✓ Debe ser transparente, eficaz e inclusiva.
- ✓ Es necesario que sea iterativa y sensible al cambio.
- ✓ Tiene que ir orientada a la mejora continua de la organización.

Proceso de gestión de riesgos: para la gestión de riesgos se debe seguir una serie de pasos para que sea eficaz y cumpla con los objetivos trazados al inicio.

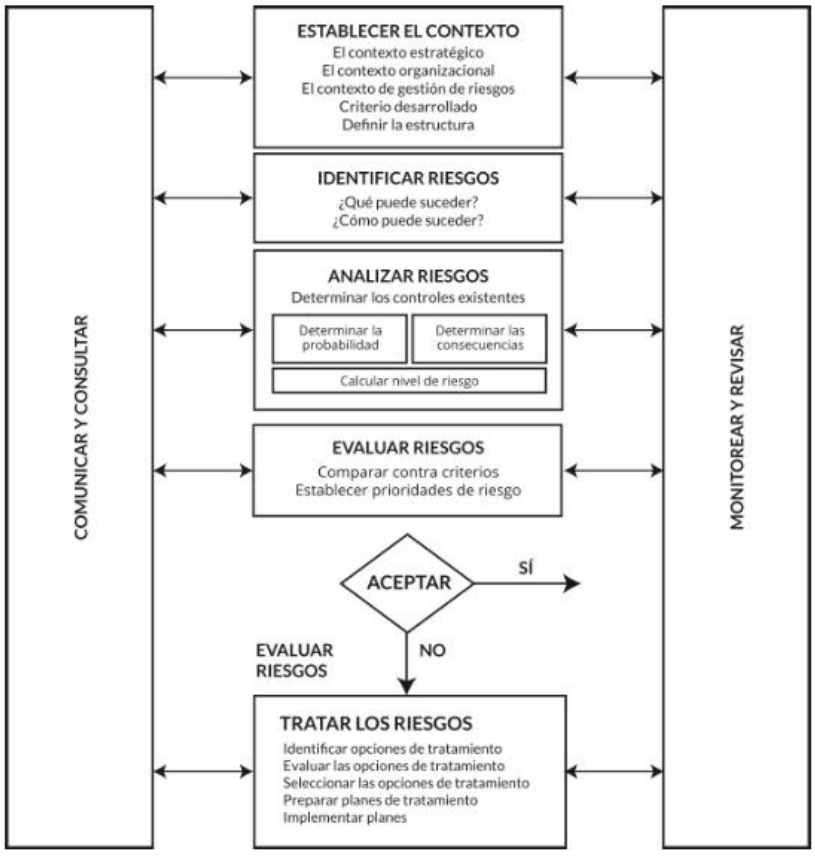


Figura 2: Proceso de gestión de riesgos.
Fuente: Norma ISO 31000:2009 – gestión de riesgos: principios y directrices

2.1.10. ISO Guide 73:2009 gestión de riesgos – vocabulario

Proporciona las definiciones de los términos genéricos relacionados con la gestión de riesgos. Su objetivo es fomentar una comprensión mutua y constante de un enfoque coherente, la descripción de las actividades relacionadas con la gestión del riesgo, y el uso de una terminología uniforme de gestión de riesgos en los procesos y marcos que se ocupan de la gestión de riesgos. (International Organization for Standardization, 2016)

2.1.11. ISO 27005:2011 técnicas de seguridad – gestión de riesgo de seguridad de la información

Proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro), que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización. (International Organization for Standardization, 2016)

2.2. Definición conceptual de términos

- **Objetivos**

Los objetivos pueden tener diferentes aspectos y pueden aplicarse a distintos niveles (como estratégica, en toda la organización, proyecto, producto y proceso). (ISO73, 2009)

- **Responsables**

Persona u organización que puede afectar, ser afectado por, o que crean que están afectadas por una decisión o actividad. (International Organization for Standardization, 2016)

- **Procesos identificados**

En toda Unidad o Servicio se realizan multitud de actividades y tareas diferentes. Todas ellas forman parte de procesos, pero a menudo, éstos no se conocen, por lo que se carece de un conocimiento real de la situación de cada tarea dentro del proceso y, por tanto, de las consiguientes posibilidades de mejora. (Gil Ojeda & Vallejo García, 2008)

- **Amenazas**

Es un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales. La

amenaza se determina en función de la intensidad y la frecuencia. (CIIFEN, 2016)

- **Riesgos históricos**

Riesgos registrados como antecedentes en una organización.

- **Riesgos existentes**

Riesgos latentes en la organización.

- **Controles existentes**

Medir ese riesgo es la modificación. Los controles incluyen cualquier proceso, la política, el dispositivo, la práctica, u otras acciones que modifican el riesgo. (ISO73, 2009)

- **Probabilidad de riesgo**

Medida de la probabilidad de ocurrencia expresa como un número entre 0 y 1, donde 0 es imposibilidad y 1 es una certeza absoluta. (ISO73, 2009)

- **Consecuencias del riesgo**

Resultado de un evento que afecta a los objetivos. (ISO73, 2009)

- **Nivel de riesgo**

Magnitud de un riesgo o una combinación de los riesgos, expresada en términos de la combinación de consecuencias y su probabilidad. (ISO73, 2009)

- **Riesgos priorizados**

  Riesgos destacados de acuerdo a su nivel de riesgo.

CAPÍTULO III

METODOLOGÍA

3.1. Planificación del diagnóstico de la variable: gestión de riesgos

3.1.1. Objetivos del diagnóstico

Son objetivos del presente diagnóstico:

- Conocer el contexto actual del Data Center de la Municipalidad Distrital de Ilabaya con el fin comprender en materia de la gestión de riesgos, con respecto a los requisitos establecidos por la Norma ISO 31000:2009.
- Identificar las actividades críticas existentes en el Data Center de la Municipalidad Distrital de Ilabaya y a su vez cuál es la priorización de ser tratadas con respecto a la Norma ISO 31000:2009.
- Elaborar una propuesta de mejora para la gestión de riesgos del Data Center, y asimismo orientarlo específicamente a las necesidades de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya.

Metodología

Se aplicó un cuestionario basado en la Escala de Likert aplicado a 10 personas que son el personal administrativo y técnico de la Sub Gerencia de Tecnologías de la Información y Comunicaciones, quienes conocen el proceso diario y continuo brindando la información necesaria, para así obtener los resultados esperados:

Para el cuestionario se considera la siguiente escala de evaluación:

Tabla 5
Criterio de evaluación para la variable: gestión de riesgos

CRITERIO DE EVALUACIÓN	ESCALA
(N) Nunca (MM) Muy malo (MB) Muy bajo	1
(CN) Casi nunca (B) Bajo	2
(AV) A veces (R) Regular	3
(CS) Casi siempre (A) Alto (F) Frecuente	4
(S) Siempre (MF) Muy frecuente (MA) Muy alto	5

Fuente: Elaboración propia.

De esta manera se logró evaluar la gestión de riesgos con respecto a su nivel de cumplimiento con respecto a los requisitos de la ISO 31000:2009.

Para el análisis de los datos del cuestionario se utilizó una metodología de valoración basada en otros trabajos de investigación para un mejor análisis de datos, tales como se utilizó en la tesis de (Medina Bocanegra, 2013) y (Pérez & Cristian Arias, 2011) dicha metodología sirve como apoyo y consiste en agregar un valor a cada uno de los criterios de evaluación en relación a la escala asignada, todo ello con fines prácticos para la evaluación de los resultados.

Tabla 6
Criterio de valoración para la variable: gestión de riesgos

Criterio de evaluación	Escala	Valoración (%)
(N) Nunca (MM) Muy malo (MB) Muy bajo	1	0
(CN) Casi nunca (B) Bajo	2	25
(AV) A veces (R) Regular	3	50
(CS) Casi siempre (A) Alto (F) Frecuente	4	75
(S) Siempre (MF) Muy frecuente (MA) Muy alto	5	100

Fuente: Elaboración propia.

Además se construyó la siguiente escala, ver **¡Error! No se ncuentra el origen de la referencia.**, para el presente trabajo de investigación con el fin de poder ubicar el nivel de porcentaje de cumplimiento de la norma en los resultados obtenidos.

Tabla 7
Valoración de resultados para la variable: gestión de riesgos

Escala de Valoración	Valor (%)	Descripción
B: Bajo	0-30	La gestión de riesgos tiene un nivel bajo de cumplimiento
M: Medio	30-60	La gestión de riesgos tiene un nivel medio de cumplimiento
A: Alto	60-100	La gestión de riesgos tiene un nivel alto de cumplimiento

Fuente: Elaboración propia

Se obtuvo un diagnóstico el cual demostró que el cumplimiento de la ISO 31000:2009 se encuentra a un dicho nivel de porcentaje, todo ello se cumple de manera indirecta por parte del personal administrativo de la Sub Gerencia de Tecnologías de la Información y Comunicaciones.

Se evaluó las cuatro dimensiones tales cuales son, la dimensión 1 (establecer contexto), dimensión 2 (identificar riesgos), dimensión 3 (analizar riesgos) y la dimensión 4 (evaluar riesgos) de la variable gestión de riesgos respecto a la ISO 31000:2009, de acuerdo a la valoración correspondiente de la Tabla las cuales fueron evaluadas al criterio de los encuestados (personal administrativo de la Sub Gerencia de Tecnologías de la Información y Comunicaciones), entendiendo que el puntaje máximo era de 100 % y el puntaje mínimo del 0 %.

3.1.2. Recolección de información

Los cuestionarios fueron llenados por 10 personas, que son el personal administrativo y técnico de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya, los cuales fueron encuestados en las instalaciones de su centro de trabajo. Las preguntas que se realizaron en el cuestionario se encuentran en el Anexo 02.

Asimismo, se consideró importante conocer las instalaciones del Data Center que se ubica dentro de la Sub Gerencia de Tecnologías de la Información y Comunicaciones para ampliar el conocimiento del mismo, en el Anexo 07 se pueden apreciar algunas fotografías de las zonas más críticas.

3.2. Desarrollo del diagnóstico de la variable : gestión de riesgos

3.2.1. Identificación del contexto del Data Center de la Municipalidad Distrital de Ilabaya con respecto a la Norma ISO 31000:2009

- Objetivos

- Determinar la capacidad de reacción del personal de la SGTIC ante posibles eventos.

- Establecimiento de responsables y responsabilidades

Tabla 8
Responsables y responsabilidades

Área	Responsable	Responsabilidades
Sub Gerencia	Ing. Luis Ángel Calderón Barja	- Preparación de un plan de respuesta a incidentes - Descripción de requerimientos de TI para los productos o servicios
Desarrollo de sistemas	Bach. Mariella Olga Condori Joaquin	- Informes de administración de las bases de datos de la institución - Plan de mantenimiento de software - Informes de control de los niveles de acceso a la información de los sistemas informáticos - Reportes de cumplimiento de normas existentes a nivel informático en la institución
Infraestructura tecnológica	Ing. Julio Cesar Corasi Flores	- Informes de la administración de la infraestructura tecnológica de la institución - Reportes de administración y mantenimiento de las centrales telefónicas - Informes de evaluación de propuestas recibidas por la empresas proveedoras para la adquisición de hardware - Reportes de la administración de los sistema de cableado estructurado
Mantenimiento y registro	Ing. Carlos Flores Miranda	- Propuestas para la actualización del software y llevar registro del licenciamiento - Informes de la aplicación de normas para el uso adecuado del equipo informático
Seguridades informáticas	Ing. Luis Ángel Calderón Barja	- Plan relacionado con la seguridad informática - Informes de evaluación de los planes de recuperación de desastres por ataques externos - Reportes de monitoreo de la red para prevenir posibles ataques externos

Fuente: Elaboración propia

- Alcance del estudio

El presente estudio se enfoca sobre el servicio tecnológico, específicamente en equipos y sistemas que se encuentren el Data Center.

Tabla 9
Resumen de la fase: establecer contexto

Establecimiento del contexto para el Data Center	
Definición:	
Gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya.	
Objetivos:	
Determinar la capacidad de reacción del personal de la SGTIC ante un eventual fallo	
Responsables	Responsabilidades
Ing. Luis Ángel Calderón Barja	- Preparación de un plan de respuesta a incidentes. - Descripción de requerimientos de TI para los productos o servicios.
Bach. Mariella Olga Condori Joaquin	- Informes de administración de las bases de datos de la institución - Plan de mantenimiento de software. - Informes de control de los niveles de acceso a la información de los sistemas informáticos. - Reportes de cumplimiento de normas existentes a nivel informático en la institución.
Ing. Julio Cesar Corasi Flores	- Informes de la administración de la infraestructura tecnológica de la institución. - Reportes de administración y mantenimiento de las centrales telefónicas. - Informes de evaluación de propuestas recibidas por las empresas proveedoras para la adquisición de hardware. - Reportes de la administración de los sistema de cableado estructurado.
Ing. Carlos Flores Miranda	- Propuestas para la actualización del software y llevar registro del licenciamiento. - Informes de la aplicación de normas para el uso adecuado del equipo informático.
Ing. Luis Ángel Calderón Barja	- Plan relacionado con la seguridad informática. - Informes de evaluación de los planes de recuperación de desastres por ataques externos. - Reportes de monitoreo de la red para prevenir posibles ataque externos.
ALCANCE	
El presente estudio se enfoca sobre el servicio tecnológico, específicamente en equipos y sistemas que se encuentren el Data Center.	

Fuente: Elaboración propia

3.2.2. Identificación de las actividades críticas en el Data Center de la Municipalidad Distrital de Ilabaya con respecto a la Norma ISO 31000:2009

Para ellos se procedió a la identificación de activos en el Data Center ya que es muy importante saber con qué recursos se cuenta para

poder así tener una noción más amplia de las causas y consecuencias que afectan directamente a estos activos.

Para la identificación de los activos se utilizó la siguiente clasificación de acuerdo a su naturaleza como el hardware, software, redes y la estructura de la Institución.

La Tabla 10 muestra la clasificación de los activos según los grupos mencionados en el párrafo anterior, debido a su manera ordenada y clara para el listado y presentación de los activos, sus respectivas amenazas y vulnerabilidades identificadas.

El criterio para la identificación de activos más importantes, amenazas y vulnerabilidades fue por parte del grupo encargado de la gestión de los riesgos, conformado por el personal de la Sub Gerencia de Tecnologías de la Información y Comunicaciones, el cual fue formado en el transcurso de la presente investigación.

- Identificar activos

La identificación de activos como se indica en el alcance, son los que se encuentran en el Data Center de la Municipalidad Distrital de Ilabaya y los que dan soporte a los servicios de nivel informático a las distintas áreas de la Institución. El listado de activos se muestra en la

Tabla clasificados según el tipo de activo y la cantidad existente de los mismos en el Data Center de la Municipalidad Distrital de Ilabaya.

Tabla 10
Clasificación de activos

Activo	Descripción	TIPO DE ACTIVO				
		HARDWAREE	SOFTWARE	REDES	ESTRUCTURA DE LA ORGANIZACION	CANTIDAD
001	Servidores Dell PowerEdge R220	x				3
002	Switch Core	x				1
003	Sistema operativo de servidores(Windows server 2012, Windows server 2008)		x			3
004	Gestores de Base de Datos(SQL server 2008 R2, PostgreSQL, FoxPro)		x			3
005	Aplicaciones(Sistema Municipal Integrado (SIMUN))		x			1
006	Aplicaciones(Sistema de Administración Financiera (SIAF))		x			1
007	Aplicaciones(Sistema de Gestión Administrativa (SIGA))		x			1
008	Aplicaciones (Servicio de mensajería interno SPARK)		x			1
009	Aire acondicionado	x				1
010	Cableado estructurado			x		1
011	Cámaras	x				2
012	Sistema eléctrico			x		1
013	Grupo electrógeno	x				1
014	Sistemas de Alimentación ininterrumpida (UPS)	x				1
015	Responsable de administración de sistemas				x	1
016	Responsable de infraestructura tecnológica y redes				x	2
017	Servidores para host de virtualización Blade IBM	x				1
018	Solución de almacenamiento 4 discos SAS 147GB	x				1

Fuente: Elaboración Propia

- Identificar amenazas

Para la identificación de las amenazas y su clasificación se tomará el siguiente criterio señalado en la Tabla 2 de tal manera se podrá

clasificar la amenaza de acuerdo a su origen sea natural, deliberada o accidental.

Tabla 2
Listado de amenazas

Cód.		Amenaza
AM1		Fuego
	Descripción	Incendios: posibilidad de que el fuego acabe con recursos tecnológicos
	Origen	Deliberadas, accidental
AM2		Desastre Natural
	Descripción	Otros incidentes que se producen sin intervención humana, por ejemplo fenómeno sísmico
	Origen	Natural
AM3		Contaminación
	Descripción	Vibraciones, polvo, suciedad, etc.
	Origen	Deliberadas, accidental
AM4		Averías
	Descripción	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen u otros durante el funcionamiento del sistema.
	Origen	Deliberadas, accidental
AM5		Corte de Suministro Eléctrico
	Descripción	Cese de la alimentación de potencia eléctrica
	Origen	Accidental
AM6		Condiciones inadecuadas de temperatura o humedad
	Descripción	Deficiencias en la aclimatación de las instalaciones, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.
	Origen	Deliberadas, Accidental
AM7		Errores del administrador
	Descripción	Equivocaciones de personas con responsabilidades de instalación y operación
	Origen	Accidental
AM8		Abuso de privilegios de acceso
	Descripción	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
	Origen	Deliberadas
AM9		Acceso no autorizado

	Descripción	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.
	Origen	Deliberadas
AM10		Manipulación de los equipos
	Descripción	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
	Origen	Deliberadas
AM11		Pérdida de equipos
	Descripción	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
	Origen	Accidental, deliberadas
AM12		Denegación de servicio
	Descripción	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
	Origen	Deliberadas
AM13		Eliminación de información
	Descripción	Eliminación de información con el fin de obtener beneficio o causar prejuicio
	Origen	Deliberada
AM14		Alteración de información
	Descripción	Alteración intencionada de la información , con el fin de obtener un beneficio o causar perjuicio
	Origen	Deliberada
AM15		Manipulación del sistema
	Descripción	Alteración intencionada del funcionamiento del software buscando un beneficio
	Origen	Deliberada
AM16		Envío de información malintencionada
	Descripción	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros
	Origen	Accidental, Deliberado
AM17		Fugas de información
	Descripción	Revelación por indiscreción
	Origen	Accidental
AM18		Vulnerabilidades de los programas
	Descripción	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.

	Origen	Accidental
AM19		Indisponibilidad del personal
	Descripción	Ausencia accidental del puesto de trabajo: enfermedad, motivos personales
	Origen	Accidental, deliberado
AM20		Extorsión
	Descripción	Reacción que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.
	Origen	Deliberadas

Fuente: Elaboración propia

Se muestra a continuación la Tabla que relaciona el activo con sus posibles amenazas clasificadas según su origen.

Tabla 12
Relación entre activo y amenaza

Cód. activo	**Cód. amenaza**	**Descripción de la amenaza**	Naturaleza			Activo		
			NATURAL	DELIBERADA	ACCIDENTAL	HARDWARE	SOFTWARE	REDES	ESTRUCTURA
001	AM1	Fuego		x	x	x			
001	AM2	Desastre natural	x			x			
001	AM3	Contaminación			x	x			
001	AM4	Averías		x	x	x			
001	AM5	Corte de suministro eléctrico			x	x			
001	AM6	Condiciones inadecuadas de temperatura o humedad			x	x			
001	AM7	Errores del administrador			x	x			
001	AM8	Abuso de privilegios de accesos			x	x			
001	AM9	Acceso no autorizado a los recursos del sistema			x	x			
001	AM10	Manipulación de los equipos			x	x			
001	AM12	Caída del sistema por motivos varios			x	x			
002	AM1	Fuego		x	x	x			
002	AM2	Desastre natural	x			x			
002	AM3	Contaminación			x	x			
002	AM4	Averías			x	x			
002	AM5	Corte de suministro eléctrico			x	x			
002	AM10	Manipulación de los equipos				x			

002	AM11	Pérdida de equipos			x		
003	AM12	Caída del sistema por motivos varios	x			x	
003	AM9	Acceso no autorizado a los recursos del sistema				x	
004	AM4	Averías		x		x	
004	AM7	Errores del administrador		x		x	
004	AM14	Eliminación de información	x	x		x	
004	AM15	Alteración de información	x			x	
004	AM16	Manipulación del sistema	x			x	
005	AM4	Averías		x		x	
005	AM7	Errores del administrador		x		x	
005	AM17	Envío de información malintencionada		x		x	
005	AM14	Eliminación de información		x		x	
005	AM18	Fugas de información		x		x	
005	AM19	Vulnerabilidades de los programas		x		x	
005	AM15	Alteración de información		x		x	
005	AM14	Eliminación de información	x	x		x	
006	AM4	Averías		x		x	
006	AM7	Errores del administrador		x		x	
006	AM17	Envío de información malintencionada		x		x	
006	AM14	Eliminación de información	x	x		x	
006	AM18	Fugas de información		x		x	
006	AM19	Vulnerabilidades de los programas		x		x	
006	AM15	Alteración de información		x		x	
007	AM4	Averías		x		x	
007	AM7	Errores del administrador		x		x	
007	AM17	Envío de información malintencionada		x		x	
007	AM14	Eliminación de información	x	x		x	
007	AM18	Fugas de información		x		x	
007	AM19	Vulnerabilidades de los programas		x		x	
007	AM15	Alteración de información		x		x	
008	AM4	Averías		x		x	
008	AM7	Errores del administrador		x		x	
008	AM17	Envío de información malintencionada		x		x	
008	AM14	Eliminación de información	x	x		x	
008	AM18	Fugas de información		x		x	
008	AM19	Vulnerabilidades de los programas		x		x	
008	AM15	Alteración de información		x		x	
009	AM4	Averías		x	x		
009	AM6	Condiciones inadecuadas de temperatura o humedad		x	x		
010	AM1	Fuego	x	x			x
010	AM5	Corte suministro eléctrico		x			x
011	AM6	Condiciones inadecuadas de temperatura o humedad		x	x		
012	AM5	Corte suministro eléctrico		x			x
012	AM6	Condiciones inadecuadas de temperatura o humedad		x			x
012	AM7	Errores del administrador		x			x

013	AM6	Condiciones inadecuadas de temperatura o humedad			x	x		
013	AM7	Errores del administrador			x	x		
013	AM1	Fuego		x	x	x		
013	AM2	Desastre natural	x			x		
013	AM3	Contaminación			x	x		
013	AM4	Averías			x	x		
014	AM6	Condiciones inadecuadas de temperatura o humedad			x	x		
014	AM7	Errores del administrador			x	x		
014	AM1	Fuego		x	x	x		
014	AM2	Desastre natural	x			x		
014	AM3	Contaminación			x	x		
014	AM4	Averías			x	x		
015	AM19	Indisponibilidad del personal			x			x
015	AM20	Extorsión		x				x
016	AM19	Indisponibilidad del personal			x			x
016	AM20	Extorsión		x				x
017	AM1	Fuego		x	x	x		
017	AM2	Desastre natural	x			x		
017	AM3	Contaminación			x	x		
017	AM4	Averías			x	x		
017	AM5	Corte suministro eléctrico			x	x		
017	AM6	Condiciones inadecuadas de temperatura o humedad				x		
017	AM7	Errores del administrador			x	X		
017	AM8	Abuso de privilegios de accesos			x	X		
017	AM9	Acceso no autorizado a los recursos del sistema			x	X		
017	AM10	Manipulación de los equipos			x	X		
017	AM12	Caída del sistema por motivos varios			x	x		
018	AM1	Fuego		x	x	x		
018	AM2	Desastre natural	x			x		
018	AM3	Contaminación			x	x		
018	AM4	Averías			x	x		
018	AM5	Corte de suministro eléctrico			x	x		
018	AM6	Condiciones inadecuadas de temperatura o humedad				x		
018	AM7	Errores del administrador			x	x		
018	AM8	Abuso de privilegios de accesos			x	x		
018	AM9	Acceso no autorizado a los recursos del sistema			x	x		
018	AM10	Manipulación de los equipos			x	x		
018	AM12	Caída del sistema por motivos varios			x	x		

Fuente: Elaboración Propia

- Identificar vulnerabilidades

Las vulnerabilidades a tomar en cuenta se establecen de acuerdo el tipo de activo, tal como se muestra en la Tabla 313.

Tabla 33
Listado de vulnerabilidades

Tipos de activos	Código	Vulnerabilidad	Resultado de la vulnerabilidad
Hardware	VH01	Mantenimiento insuficiente	Pérdida
	VH02	Susceptibilidad a la humedad, el polvo y la suciedad	Pérdida
	VH03	Susceptibilidad a las variaciones de voltaje	Interrupción
	VH04	Susceptibilidad a las variaciones de temperatura	Interrupción
	VH05	Almacenamiento sin protección	Pérdida
	VH6	Ausencia de un eficiente control de cambios en la configuración	Modificación
	VH7	Ausencia de esquemas de reemplazo	Pérdida
Software	VS01	Ausencia o insuficiencia de pruebas de software	Interrupción
	VS02	Software nuevo o inmaduro	Interrupción
	VS03	Configuración incorrecta de parámetros	Modificación
	VS04	Tablas de contraseñas sin protección	Revelación
	VS05	Gestión deficiente de las contraseñas	Revelación
	VS06	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Modificación
	VS07	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Revelación
	VS08	Interfaz de usuario compleja	Modificación
	VS09	Ausencia de documentación	Modificación
	VS10	Fechas incorrectas	Modificación
	VS11	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	Revelación
	VS12	Ausencia de copias de respaldo	Pérdida
	VS13	Ausencia de protección física de la edificación, puertas y ventanas	Pérdida
	VS14	Falla en la producción de informes de gestión	Interrupción
	VS15	Asignación errada de los derechos de acceso	Revelación
	VR01	Ausencia de pruebas de envío o recepción de mensajes	Pérdida
	VR02	Conexión deficiente de los cables.	Interrupción
	VR03	Susceptibilidad a las variaciones de voltaje	Interrupción

Redes	VR04	Gestión inadecuada de la red	Interrupción
	VR05	Conexiones de red pública sin protección	Revelación
	VR06	Susceptibilidad a las variaciones de temperatura	Interrupción
	VE01	Ausencia del personal	Interrupción
Estructura de la organización	VE02	Ausencia de procedimiento formal para la autorización de la información disponible al público	Revelación

Fuente: Elaboración propia

En relación a las amenazas encontradas se listan las vulnerabilidades en la Tabla 4 que muestra la relación de activo, amenaza y vulnerabilidad según el criterio por parte de los encargados de infraestructura tecnológica quienes apoyaron en todo momento a su clasificación y valoración.

Tabla 14
Relación de activo, amenaza y vulnerabilidad

Cód. activo	Cód. amenaza	Cód. vulnerabilidad	Resultado de la vulnerabilidad
001	AM1	VH03	Interrupción
001	AM2	VH02	Pérdida
001	AM3	VH02	Pérdida
001	AM4	VH06	Modificación
001	AM5	VH03	Interrupción
001	AM6	VH04	Interrupción
001	AM7	VH06	Modificación
001	AM8	VH06	Modificación
001	AM9	VH06	Modificación
001	AM10	VH06	Modificación
001	AM12	VH07	Pérdida
002	AM1	VH03	Interrupción
002	AM2	VH02	Pérdida
002	AM3	VH02	Pérdida
002	AM4	VH06	Modificación
002	AM5	VH03	Interrupción
002	AM10	VH06	Modificación
002	AM11	VH05	Pérdida
003	AM12	VH07	Pérdida
003	AM9	VH06	Modificación

004	AM4	VS02	Interrupción
004	AM7	VS03	Modificación
004	AM14	VS12	Pérdida
004	AM15	VS11	Revelación
004	AM16	VS11	Revelación
005	AM4	VS02	Interrupción
005	AM7	VS03	Modificación
005	AM17	VS11	Revelación
005	AM14	VS12	Pérdida
005	AM18	VS15	Revelación
005	AM19	VS01	Interrupción
005	AM15	VS11	Revelación
005	AM14	VS12	Pérdida
006	AM4	VS02	Interrupción
006	AM7	VS03	Modificación
006	AM17	VS11	Modificación
006	AM14	VS12	Pérdida
006	AM18	VS15	Revelación
006	AM19	VS01	Interrupción
006	AM15	VS11	Modificación
007	AM4	VS02	Interrupción
007	AM7	VS03	Modificación
007	AM17	VS11	Modificación
007	AM14	VS12	Pérdida
007	AM18	VS15	Revelación
007	AM19	VS01	Interrupción
007	AM15	VS11	Modificación
008	AM4	VS02	Interrupción
008	AM7	VS03	Modificación
008	AM17	VS11	Modificación
008	AM14	VS12	Pérdida
008	AM18	VS15	Revelación
008	AM19	VS01	Interrupción
008	AM15	VS11	Modificación
009	AM4	VH03	Interrupción
009	AM6	VH03	Interrupción
010	AM1	VR06	Interrupción
010	AM5	VR03	Revelación
011	AM6	VH03	Interrupción
012	AM5	VR03	Interrupción
012	AM6	VR06	Interrupción
012	AM7	VR04	Interrupción
013	AM6	VH04	Interrupción
013	AM7	VH06	Interrupción
013	AM1	VH03	Interrupción
013	AM2	VH02	Pérdida
013	AM3	VH02	Pérdida
013	AM4	VH06	Modificación

014	AM6	VH04	Interrupción
014	AM7	VH06	Modificación
014	AM1	VH03	Interrupción
014	AM2	VH02	Pérdida
014	AM3	VH02	Pérdida
014	AM4	VH06	Modificación
015	AM20	VE01	Interrupción
015	AM21	VE02	Revelación
016	AM20	VE01	Interrupción
016	AM21	VE02	Revelación
017	AM1	VH03	Interrupción
017	AM2	VH02	Pérdida
017	AM3	VH02	Pérdida
017	AM4	VH06	Modificación
017	AM5	VH06	Modificación
017	AM6	VH04	Interrupción
017	AM7	VH06	Modificación
017	AM8	VH06	Modificación
017	AM9	VH06	Modificación
017	AM10	VH06	Modificación
017	AM12	VH07	Pérdida
018	AM1	VH03	Interrupción
018	AM2	VH02	Pérdida
018	AM3	VH02	Pérdida
018	AM4	VH06	Modificación
018	AM5	VH03	Interrupción
018	AM6	VH04	Interrupción
018	AM7	VH06	Modificación
018	AM8	VH06	Modificación
018	AM9	VH06	Modificación
018	AM10	VH06	Modificación
018	AM12	VH07	Pérdida

Fuente: Elaboración propia

3.2.3. Propuesta para la mejora de la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya

El objetivo de la propuesta es lograr que la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya pueda identificar y tomar conciencia de sus activos más importantes, además de determinar las amenazas a los cuales se ven expuestos, las causas que puedan ocasionar el impacto y las consecuencias que puedan generarse si no se conoce la realidad actual por la cual atraviesa dicha oficina, como se muestra en la Tabla , basándose en los requisitos de la Norma 31000:2009, que involucran la preservación de la consecución de los objetivos de la institución.

Los resultados del cuestionario son de vital importancia ya que muestran la situación actual de la gestión de riesgos basándose en los requerimientos de la Norma ISO 31000:2009 mostrando el nivel de cumplimiento de manera indirecta con el estándar en mención.

Las actividades que se recomiendan identificar, analizar y evaluar periódicamente están basadas en la Norma ISO 31000:2009, dicha norma garantizará un desempeño óptimo de la gestión de riesgos dentro del

Data Center de la Institución en mención. Asimismo, complementará algunas actividades que se encuentran deficientes.

Las fases involucradas en la presente investigación están en concordancia de las dimensiones definidas para la variable de estudio del presente proyecto como lo son, establecer el contexto, identificar los riesgos, analizar riesgos y evaluar el riesgo.

La Figura 3 muestra las fases de la gestión de riesgos que sirvieron como base para poder conocer la situación actual del Data Center de la Municipalidad de Ilabaya.

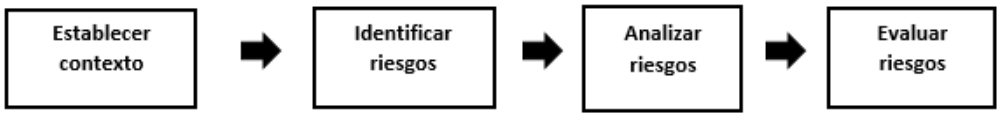


Figura 3: Fases para elaboración de propuesta
Fuente: Elaboración propia

Es parte de la propuesta para la SGTIC adoptar el siguiente modelo propuesto para realizar el análisis evaluación de sus riesgos basándose en la Norma ISO 31000:2009.

- ANALIZAR RIESGOS

Obtenida la información de activos, amenazas y vulnerabilidades es necesario analizar los datos, para ello es preciso valorar el nivel de importancia de los mismos.

- Valoración de activos

Se muestra la Tabla que contiene la escala de valoración de los activos:

Tabla 15
Valoración de activos

Escala de valoración	Valor	Descripción
MB: Muy bajo	0	Activo que no influye para el funcionamiento del Data Center
B: Bajo	1	Activo de menor importante para el funcionamiento del Data Center
M: Medio	2	Activo importante para el funcionamiento del Data Center
A: Alto	3	Activo altamente importante para el funcionamiento del Data Center
MA: Muy alto	4	Activo de vital importancia para el correcto funcionamiento del Data Center

Fuente: Elaboración propia

Es necesario valorar el nivel de importancia de los activos de acuerdo a la Tabla :

Tabla 16
Relación de activos con respectiva valoración

ACTIVO	DESCRIPCIÓN	Valoración
001	Servidores Dell PowerEdge R220	Muy alto
002	Switch Core	Muy alto
003	Sistema operativo de servidores(Windows server 2012, Windows server 2008)	Muy alto
004	Gestores de Base de Datos(SQL server 2008 R2, PostgreSQL, FoxPro)	Muy alto
005	Aplicaciones(Sistema Municipal Integrado (SIMUN))	Muy alto
006	Aplicaciones(Sistema de Administración Financiera (SIAF))	Muy alto
007	Aplicaciones(Sistema de Gestión Administrativa (SIGA))	Alto
008	Aplicaciones (Servicio de chat interno SPARK)	Muy alto
009	Aire acondicionado	Alto
010	Cableado estructurado	Muy alto
011	Cámaras	Bajo
012	Sistema eléctrico	Muy alto
013	Grupo electrógeno	Alto
014	Sistemas de alimentación ininterrumpida (UPS)	Alto
015	Responsable de administración de sistemas	Muy alto
016	Responsable de infraestructura tecnológica y redes	Muy alto
017	Servidores para host de virtualización Blade IBM	Muy alto
018	Solución de almacenamiento 4 discos SAS 147GB	Alto

Fuente: Elaboración propia

- Valoración de amenazas

Es necesario valorar el nivel de importancia de los activos de acuerdo a la Tabla 4 que muestra la escala de valoración de amenazas:

Tabla 4
Valoración de amenazas

Escala de valoración	Valor	Descripción
B: Bajo	0	La amenaza se presenta raras veces
M: Medio	1	La amenaza se presenta regularmente
A: Alto	2	La amenaza se presenta muy frecuentemente

Fuente: Elaboración propia

Así mismo, se le asigna un criterio de valoración a las amenazas identificadas como se puede ver en la Tabla :

Tabla 18
Relación de amenazas y su respectiva valoración

Cód.	Amenaza	Valoración
AM1	Fuego	0
AM2	Desastre natural	0
AM3	Contaminación	1
AM4	Averías	1
AM5	Corte de suministro eléctrico	2
AM6	Condiciones inadecuadas de temperatura o humedad	1
AM7	Errores del administrador	0
AM8	Abuso de privilegios de acceso	0
AM9	Acceso no autorizado	0
AM10	Manipulación de los equipos	0
AM11	Pérdida de equipos	0
AM12	Denegación de servicio	0
AM13	Eliminación de información	0
AM14	Alteración de información	0
AM15	Manipulación del sistema	0
AM16	Envío de información malintencionada	0
AM17	Fugas de información	1
AM18	Vulnerabilidades de los programas	1
AM19	Indisponibilidad del personal	0
AM20	Extorsión	0

Fuente: Elaboración propia

- Valoración de vulnerabilidades

Es necesario valorar el nivel de importancia de las vulnerabilidades de acuerdo a la Tabla que muestra la escala de valoración de vulnerabilidades:

Tabla 19
Valoración de vulnerabilidades

Escala de Valoración	Valor	Descripción
B: Bajo	0	Puede tratarse más adelante
M: Medio	1	Debe tratarse a la brevedad en un plazo determinado en el transcurso del mes
A: Alto	2	Debe tratarse inmediatamente en el transcurso de la semana

Fuente: Elaboración propia

Así mismo, se le asigna un criterio de valoración a las vulnerabilidades identificadas como se puede ver en la Tabla :

Tabla 20
Relación de vulnerabilidades con su respectiva valoración

Tipos de activos	Cód.	Descripción	Vulnerabilidad
HARDWARE	VH01	Mantenimiento insuficiente	1
	VH02	Susceptibilidad a la humedad, el polvo y la suciedad	1
	VH03	Susceptibilidad a las variaciones de voltaje	2
	VH04	Susceptibilidad a las variaciones de temperatura	1
	VH05	Almacenamiento sin protección	1
	VH6	Ausencia de un eficiente control de cambios en la configuración	2
	VH7	Ausencia de esquemas de reemplazo	2
SOFTWARE	VS01	Ausencia o insuficiencia de pruebas de software	0
	VS02	Software nuevo o inmaduro	0
	VS03	Configuración incorrecta de parámetros	2
	VS04	Tablas de contraseñas sin protección	1
	VS05	Gestión deficiente de las contraseñas	0
	VS06	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	0
	VS07	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2
	VS08	Interfaz de usuario compleja	0
	VS09	Ausencia de documentación	0
	VS10	Fechas incorrectas	2
	VS11	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario	2
	VS12	Ausencia de copias de respaldo	2

	VS13	Ausencia de protección física de la edificación, puertas y ventanas	0
	VS14	Falla en la producción de informes de gestión	0
	VS15	Asignación errada de los derechos de acceso	2
REDES	VR01	Ausencia de pruebas de envío o recepción de mensajes	1
	VR02	Conexión deficiente de los cables.	1
	VR03	Susceptibilidad a las variaciones de voltaje	2
	VR04	Gestión inadecuada de la red	0
	VR05	Conexiones de red pública sin protección	2
	VR06	Susceptibilidad a las variaciones de temperatura	1
ESTRUCTURA DE LA ORGANIZACIÓN	VE01	Ausencia del personal	1
	VE02	Ausencia de procedimiento formal para la autorización de la información disponible al público	1

Fuente: Elaboración propia

- Nivel de estimación del riesgo

Es necesario valorar el nivel de importancia de los riesgos de acuerdo a la Tabla para identificarlos de manera clara tal como se muestra a continuación la escala de valoración de riesgos:

Tabla 21
Valoración de riesgos

Escala de Valoración	Valor	Descripción
B: Bajo	0-2	Puede ser tratado más adelante
M: Medio	3-5	Deben tratarse lo más pronto posible
A: Alto	6-8	Deben tratarse inmediatamente

Fuente: Elaboración propia

Al haber consolidado la información como los activos, amenazas y vulnerabilidades con sus respectivas valoraciones permitió hallar el total

sumando dichos valores asignados, lo cual muestra el riesgo según los resultados calculados, todo ello se puede apreciar en la Tabla .

Tabla 22
Nivel de estimación de riesgos

COD. ACTIVO	VA	COD. AMENAZA	VM	COD. VULNERABILIDAD	VV	Valor total
001	4	AM1	0	VH03	2	6
001	4	AM2	0	VH02	1	5
001	4	AM3	1	VH02	1	6
001	4	AM4	1	VH06	2	7
001	4	AM5	2	VH03	2	8
001	4	AM6	1	VH04	1	6
001	4	AM7	0	VH06	2	6
001	4	AM8	0	VH06	2	6
001	4	AM9	0	VH06	2	6
001	4	AM10	0	VH06	2	6
001	4	AM12	0	VH07	2	6
002	4	AM1	0	VH03	2	6
002	4	AM2	0	VH02	1	5
002	4	AM3	1	VH02	1	6
002	4	AM4	1	VH06	2	7
002	4	AM5	2	VH03	2	8
002	4	AM10	0	VH06	2	6
002	4	AM11	0	VH05	1	5
003	4	AM12	0	VH07	2	6
003	4	AM9	0	VH06	2	6
004	4	AM4	1	VS02	0	5
004	4	AM7	0	VS03	2	6
004	4	AM14	0	VS12	2	6
004	4	AM15	0	VS11	2	6
004	4	AM16	0	VS11	2	6
005	4	AM4	1	VS02	0	5
005	4	AM7	0	VS03	2	6
005	4	AM17	1	VS11	2	7
005	4	AM14	0	VS12	2	6
005	4	AM18	1	VS15	2	7
005	4	AM19	0	VS01	0	4
005	4	AM15	0	VS11	2	6
005	4	AM14	0	VS12	2	6
006	4	AM4	0	VS02	0	4

006	4	AM7	0	VS03	2	6
006	4	AM17	1	VS11	2	7
006	4	AM14	0	VS12	2	6
006	4	AM18	1	VS15	2	7
006	4	AM19	0	VS01	0	4
006	4	AM15	0	VS11	2	6
007	3	AM4	1	VS02	0	4
007	3	AM7	0	VS03	2	5
007	3	AM17	1	VS11	2	6
007	3	AM14	0	VS12	2	5
007	3	AM18	1	VS15	2	6
007	3	AM19	0	VS01	0	3
007	3	AM15	0	VS11	2	5
008	4	AM4	1	VS02	0	5
008	4	AM7	0	VS03	2	6
008	4	AM17	1	VS11	2	7
008	4	AM14	0	VS12	2	6
008	4	AM18	1	VS15	2	7
008	4	AM19	0	VS01	0	4
008	4	AM15	0	VS11	2	6
009	3	AM4	0	VH03	2	5
009	3	AM6	1	VH03	2	6
010	4	AM1	0	VR06	1	5
010	4	AM5	2	VR03	2	8
011	1	AM6	1	VH03	2	4
012	4	AM5	2	VR03	2	8
012	4	AM6	1	VR06	1	6
012	4	AM7	0	VR04	0	4
013	3	AM6	1	VH04	1	5
013	3	AM7	0	VH06	2	5
013	3	AM1	0	VH03	2	5
013	3	AM2	0	VH02	1	4
013	3	AM3	1	VH02	1	5
013	3	AM4	1	VH06	2	6
014	3	AM6	1	VH04	1	5
014	3	AM7	0	VH06	2	5
014	3	AM1	0	VH03	2	5
014	3	AM2	0	VH02	1	4
014	3	AM3	1	VH02	1	5
014	3	AM4	1	VH06	2	6
015	4	AM19	0	VE01	1	5
015	4	AM20	0	VE02	1	5
016	4	AM19	0	VE01	1	5

016	4	AM20	0	VE02	1	5
017	4	AM1	0	VH03	2	6
017	4	AM2	0	VH02	1	5
017	4	AM3	1	VH02	1	6
017	4	AM4	1	VH06	2	7
017	4	AM5	2	VH03	2	8
017	4	AM6	1	VH04	1	6
017	4	AM7	0	VH06	2	6
017	4	AM8	0	VH06	2	6
017	4	AM9	0	VH06	2	6
017	4	AM10	0	VH06	2	6
017	4	AM12	0	VH07	2	6
018	3	AM1	0	VH03	2	5
018	3	AM2	0	VH02	1	4
018	3	AM3	1	VH02	1	5
018	3	AM4	1	VH06	2	6
018	3	AM5	2	VH03	2	7
018	3	AM6	1	VH04	1	5
018	3	AM7	0	VH06	2	5
018	3	AM8	0	VH06	2	5
018	3	AM9	0	VH06	2	5
018	3	AM10	0	VH06	2	5
018	3	AM12	0	VH07	2	5

Fuente: Elaboración propia

➢ EVALUAR RIESGOS

- Evaluación del riesgo

Con el análisis realizado sobre los activos y sus respectivas amenazas y vulnerabilidades y según la Tabla que muestra la valoración de los riesgos, se pudo identificar los activos que presentan como riesgo “alto” con respecto la escala establecida en la Tabla , además en la Tabla se muestra los activos con riesgo “alto” y los destacados con el mayor

puntaje obtenido según su valoración permitiendo así conocer la situación actual en la cual se encuentran los activos del Data Center de la Municipalidad Distrital de Ilabaya; por lo cual se le pide tratar estos riesgos a la brevedad o se tomen las medidas necesarias por parte de alta dirección.

Tabla 23
Relación de activos y su nivel de riesgo

Nº	CÓD	DESCRIPCIÓN	NIVEL DE RIESGO
1	001	Servidores Dell PowerEdge R220	Alto
	AM5	Corte de suministro eléctrico	
	VH03	Susceptibilidad a las variaciones de voltaje	
2	002	Switch Core	Alto
	AM5	Corte de suministro eléctrico	
	VH03	Susceptibilidad a las variaciones de voltaje	
3	010	Cableado estructurado	Alto
	AM5	Corte de suministro eléctrico	
	VR03	Susceptibilidad a las variaciones de voltaje	
4	017	Servidores para host de virtualización Blade IBM	Alto
	AM5	Corte de suministro eléctrico	
	VH03	Susceptibilidad a las variaciones de voltaje	

Fuente: Elaboración propia

Los principales riesgos identificados se muestran en la Tabla ahora se sugiere que la Sub Gerencia de Tecnologías de la Información y Comunicaciones tome las medidas del caso para el tratamiento de los riesgos identificados, según la Norma ISO 31000:2009 propone las siguientes opciones en la Tabla :

Tabla 24
Opciones de tratamiento de riesgo

Opción	Descripción
1	Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo
2	Tomar o aumentar el riesgo para poder aprovechar una oportunidad
3	Eliminar la fuente de riesgo
4	Cambiar la probabilidad
5	Cambiar las consecuencias
6	Compartir el riesgo con otra parte o partes (incluyendo contratos y financiamiento de riesgo)
7	Retener el riesgo mediante una decisión informada

Fuente: Norma ISO 31000:2009 – gestión de riesgos - principios y directrices

La selección de la opción de tratamiento de riesgos más adecuada consiste en equilibrar los costos y los esfuerzos de implementación con los beneficios derivados de los requisitos legales, reglamentarios y otros, según indica la Norma ISO 31000:2009.

CAPÍTULO IV

RESULTADOS Y ANÁLISIS

4.1. Resultados descriptivos para la variable: gestión de riesgos

Se representan a continuación los resultados de la evaluación por dimensiones: dimensión 1 (establecer contexto), dimensión 2 (identificar riesgos), dimensión 3 (analizar riesgos) y dimensión 4 (evaluar riesgos) de la variable gestión de riesgos, teniendo en cuenta lo siguiente:

- Se muestran aquellos aspectos que están parcialmente o ausentes completamente.
- Se presenta el grado de cumplimiento actual encontrado en la gestión de riesgos del Data Center de la Municipalidad Distrital de Ilabaya respecto a la Norma ISO 31000:2009.
- Se realiza la valorización del cumplimiento utilizando la escala de Likert según la metodología establecida.

4.1.1 Resultados de la variable por indicadores

Tabla 25
Grado de cumplimiento de la variable: gestión de riesgos (por indicadores)

Dimensión	Indicador	Descripción	Sub indicadores	Puntaje total esperado	Puntaje total obtenido	**(%)**
	I1	Objetivos definidos		100	50	2,5
	I2	Estrategias definidas		100	25	1,25
D1	I3	Responsables asignados		100	50	2,5
	I4	Procesos identificados		100	50	2,5
	I5	Recursos identificados		100	75	3,75
	I6	Riesgos internos	Nivel de control de riesgos internos	100	50	2,5
			Causas de los riesgos internos	100	25	1,25
D2			Consecuencias de los riesgos internos	100	25	1,25
	I7	Riesgos externos	Nivel de control de riesgos externos	100	50	2,5
			Causas de los riesgos externos	100	25	1,25
			Consecuencias de los riesgos externos	100	75	3,75
	I8	Fuentes de riesgo		100	75	3,75
	I9	Zonas de impacto		100	25	1,25
	I10	Controles de gestión de riesgo		100	50	2,5
D3	I11	Probabilidad de ocurrencia		100	50	2.5
	I12	Causas		100	50	2,5
	I13	Consecuencias		100	75	3,75
	I14	Nivel de riesgo		100	50	2,5
D4	I15	Riesgos priorizados		100	25	1,25
	I16	Toma de decisiones		100	50	2,5
		Porcentaje total		100 %		47,5

Fuente: Elaboración propia

Interpretación:

En la Tabla se muestra el resumen del diagnóstico del grado de cumplimiento de la ISO 31000:2009 (por indicadores) sobre la gestión de riesgos en el Data Center perteneciente a la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya, donde se muestra que existe un 47,5 % del cumplimiento total de la Norma ISO 31000:2009 sobre la gestión de riesgos del Data Center, lo cual significa que existe aspectos deficientes que se deben mejorar y otros requisitos que deben ser implementados, según la norma, para que la gestión de riesgos en el Data Center se encuentre totalmente alineada en dichos niveles de la Norma ISO 31000:2009.

Demostrando en la Figura 10 el gráfico de barras por indicador de la variable gestión de riesgos, exponiendo los porcentajes sobre el cumplimiento de cada uno de ellos, se muestran cuatro indicadores con mayor cumplimiento de la Norma ISO 31000:2009 los cuales son: indicador 5 (recursos identificados) con un porcentaje de cumplimiento del 3,75 %, el sub indicador 3 del indicador 7 (consecuencias de los riesgos externos) con un porcentaje de cumplimiento del 3,75 %, el indicador 8 (fuentes de riesgo) con un porcentaje de cumplimiento del 3,75 % y el

indicador 13 (consecuencias) con un porcentaje de cumplimiento del 3,75 %.

Los indicadores que fueron calificados con mayor porcentaje son los que tienen mayor cumplimiento para el proceso de gestión de riesgos.

Por otro lado, los indicadores con menor cumplimiento de la Norma ISO 31000:2009 son el indicador 2 (estrategias definidas), sub indicadores 2 (causas de los riesgos internos) y 3 (consecuencias de los riesgos internos) del indicador 6 (riesgos internos), el sub indicador 2 (causas de los riesgos externos) del indicador 7 (riesgos externos), el indicador 9 (zonas de impacto) y el indicador 15 (riesgos priorizados) con un porcentaje de cumplimiento del 1,25 %.

Los indicadores que fueron calificados con menor porcentaje son los que tienen menor cumplimiento para la gestión de riesgos.

4.1.2 Resultados de la variable por dimensiones

Tabla 26
Grado de cumplimiento de la variable gestión de riesgos (por dimensiones)

RESULTADO DEL DIAGNÓSTICO POR DIMENSIONES DE LA VARIABLE: GESTIÓN DE RIESGOS		
Dimensión	**Descripción**	**Porcentaje del cumplimiento (%)**
Dimensión 1	Establecer contexto	12,5
Dimensión 2	Identificar riesgos	17,5
Dimensión 3	Analizar riesgos	11,25
Dimensión 4	Evaluar riesgos	6,25
	Porcentaje total	47,5

Fuente: Elaboración propia

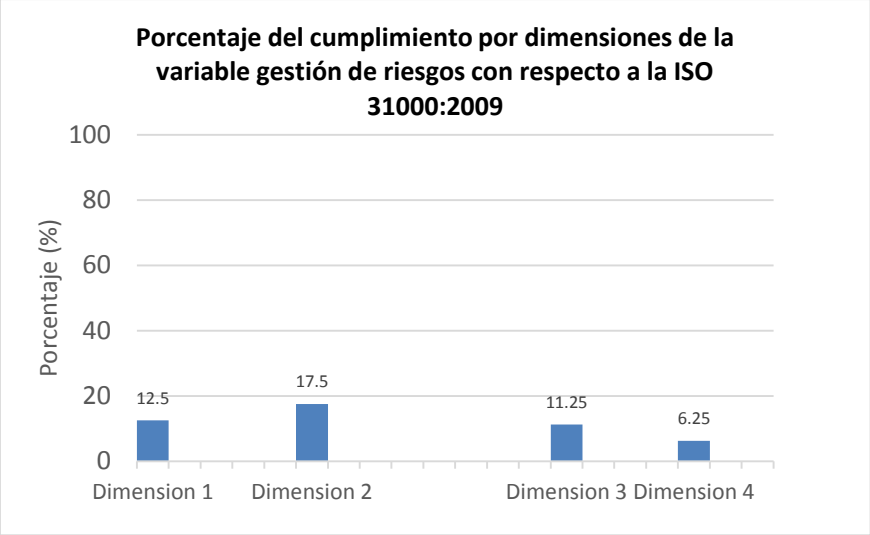


Figura 4. Cuadro de porcentaje del cumplimiento por dimensiones de la Norma ISO 31000:2009 sobre la gestión de riesgos
Fuente: Elaboración propia

Interpretación

En la Tabla se muestra el resumen del diagnóstico del grado de cumplimiento de la ISO 31000:2009 (por dimensiones), en la gestión de riesgos del Data Center de la Municipalidad Distrital de Ilabaya, con un porcentaje total obtenido del 47,5 % del cumplimiento de la Norma ISO 31000:2009 en dicha variable.

Demostrando en la Figura 5 el cuadro de barras por dimensiones de la variable gestión de riesgos, resultando de la siguiente manera: cumplimiento de la dimensión 1 (establecer contexto) con un 12,5 % del porcentaje total obtenido, dimensión 2 (identificar riesgos) con un 17,5 % del porcentaje total obtenido, dimensión 3 (analizar riesgos) con un 11,25 % del porcentaje total obtenido y dimensión 4 (evaluar riesgos) con un 6,25 % del porcentaje total obtenido.

Tabla 27
Grado de cumplimiento de la dimensión 1 de la variable gestión de riesgos

RESULTADO DEL DIAGNÓSTICO DE LA DIMENSIÓN 1 DE LA VARIABLE GESTIÓN DE RIESGOS			
Dimensión	**Indicador**	**Descripción**	**Porcentaje obtenido (%)**
D1 : ESTABLECER CONTEXTO	I1	Objetivos definidos	2,5
	I2	Estrategias definidas	1,25
	I3	Responsables asignados	2,5
	I4	Procesos identificados	2,5
	I5	Recursos identificados	3,75
Total de la dimensión 1			12,5

Fuente: Elaboración propia

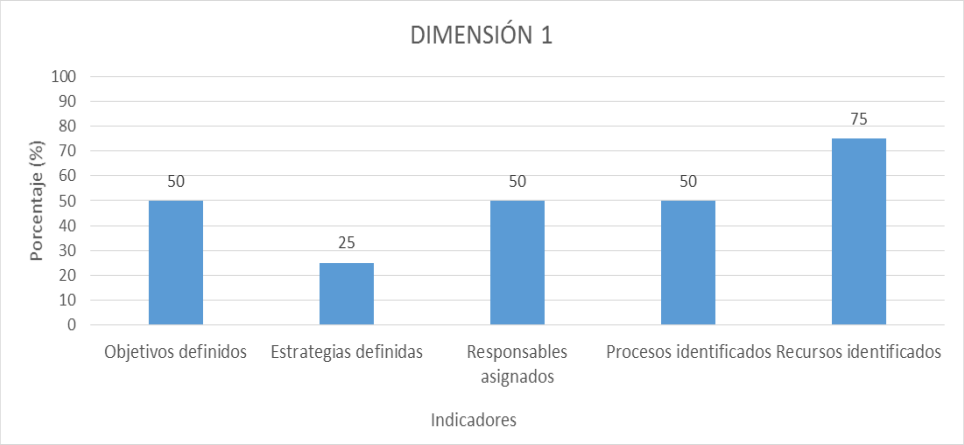


Figura 5. Cuadro de porcentaje del cumplimiento de la dimensión 1 de la variable gestión de riesgos
Fuente: Elaboración propia

Interpretación

En la Tabla se muestra el grado de cumplimiento de la dimensión 1 de la ISO 31000:2009 sobre la gestión de riesgos del Data Center, con un porcentaje total obtenido del 12,5 % del cumplimiento de la Norma ISO 31000:2009. Además se demuestra en la Figura 6 el cuadro de barras de los indicadores de la dimensión y su porcentaje correspondiendo de acuerdo a la evaluación realizada.

Tabla 28
Grado de cumplimiento de la dimensión 2 de la variable gestión de riesgos

RESULTADO DEL DIAGNÓSTICO DE LA DIMENSIÓN 2 DE LA VARIABLE GESTIÓN DE RIESGOS				
Dimensión	**Indicador**	**Descripción**	**Sub indicador**	**Porcentaje obtenido (%)**
D2 : IDENTIFICAR RIESGOS	I6	Riesgos internos	I6.1 Nivel de control de riesgos internos	2,5
			I6.2 Causas de los riesgos internos	1,25
			I6.3Consecuencias de los riesgos internos	1,25
	I7	Riesgos externos	I7.1 Nivel de control de riesgos externos	2,5
			I7.2 Causas de los riesgos externos	1,25
			I7.3 Consecuencias de los riesgos externos	3,75
	I8	Fuentes de riesgo		3,75
	I9	Zonas de impacto		1,25
Total de la dimensión 2				17,5

Fuente: Elaboración propia

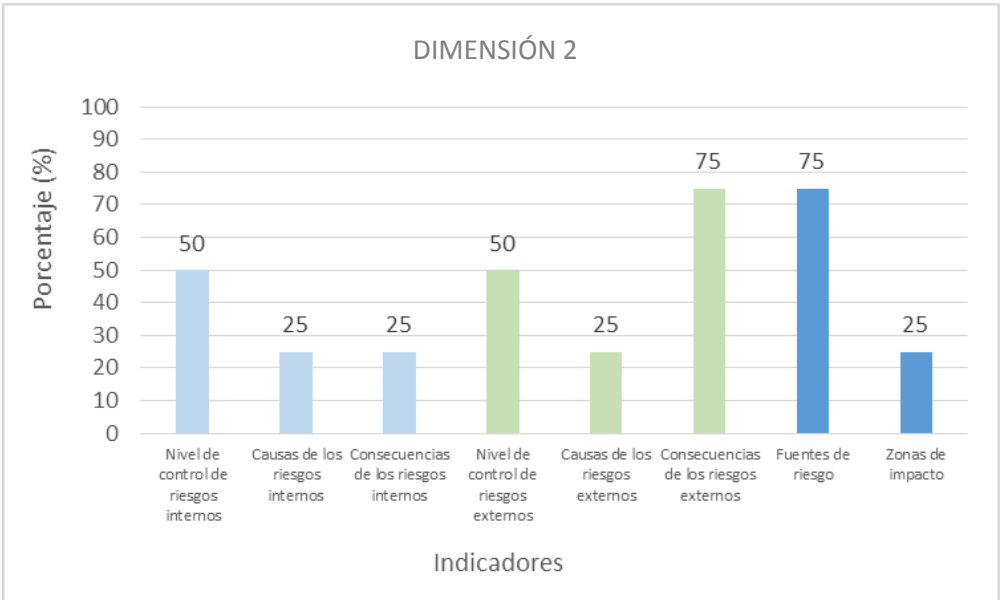


Figura 6. Cuadro de porcentaje del cumplimiento de la dimensión 2 de la variable gestión de riesgos
Fuente: Elaboración propia

Interpretación

En la Tabla se muestra el grado de cumplimiento de la dimensión 2 de la ISO 31000:2009 sobre la gestión de riesgos del Data Center, con un porcentaje total obtenido del 17,5 % del cumplimiento de la Norma ISO 31000:2009. Se observa además que existen sub indicadores para el indicador 6 que cuenta con el sub indicador I6.1 (nivel de control de riesgos internos), I6.2 (causas de los riesgos internos) y I6.3 (consecuencias de los riesgos internos) y para el indicador 7 sub indicador I7.1 (nivel de control de riesgos externos), I7.2 (causas de los riesgos externos) y I7.3 (consecuencias de los riesgos externos). Además se demuestra en la Figura 7 el cuadro de barras de los indicadores de la dimensión y su porcentaje correspondiendo de acuerdo a la evaluación realizada.

Tabla 29
Grado de cumplimiento de la dimensión 3 de la variable gestión de riesgos

RESULTADO DEL DIAGNÓSTICO DE LA DIMENSIÓN 3 DE LA VARIABLE GESTIÓN DE RIESGOS			
Dimensión	**Indicador**	**Descripción**	**Porcentaje obtenido (%)**
D3 : ANALIZAR RIESGOS	I10	Controles de gestión de riesgos	2,5
	I11	Probabilidad de ocurrencia	2,5
	I12	Causas	2,5
	I13	Consecuencias	3,75
	Total de la dimensión 3		11.25

Fuente: Elaboración propia

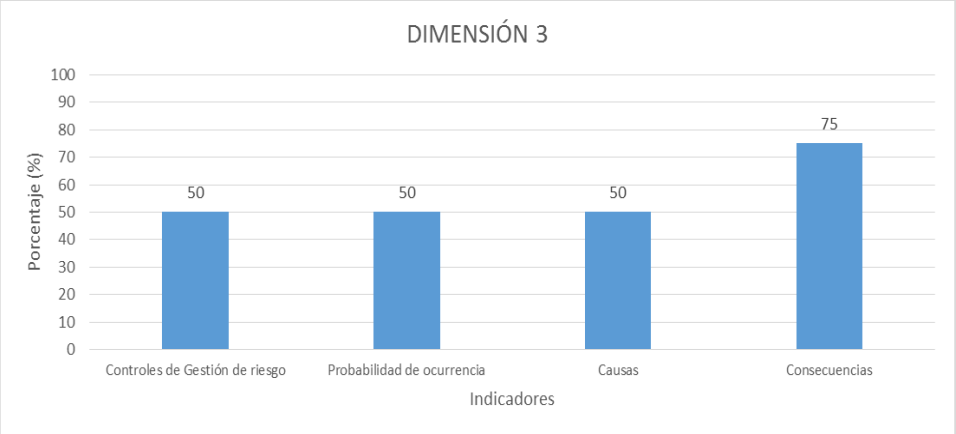


Figura 7. Cuadro de porcentaje del cumplimiento de la dimensión 3 de la variable gestión de riesgos
Fuente: Elaboración propia

Interpretación

En la Tabla se muestra el grado de cumplimiento de la dimensión 3 de la ISO 31000:2009 sobre la gestión de riesgos del Data Center, con un porcentaje total obtenido del 11,25 % del cumplimiento de la Norma ISO 31000:2009. Además se demuestra en la Figura 8 el cuadro de barras de los indicadores de la dimensión y su porcentaje correspondiendo de acuerdo a la evaluación realizada.

Tabla 30
Grado de cumplimiento de la dimensión 4 de la variable gestión de riesgos

RESULTADO DEL DIAGNÓSTICO DE LA DIMENSIÓN 4 DE LA VARIABLE GESTIÓN DE RIESGOS			
Dimensión	**Indicador**	**Descripción**	**Porcentaje obtenido (%)**
D4 : EVALUAR RIESGOS	I14	Nivel de riesgo	2,5
	I15	Riesgos priorizados	1,25
	I16	Toma de decisiones	2,5
Total de la dimensión 4			6,25

Fuente: Elaboración propia

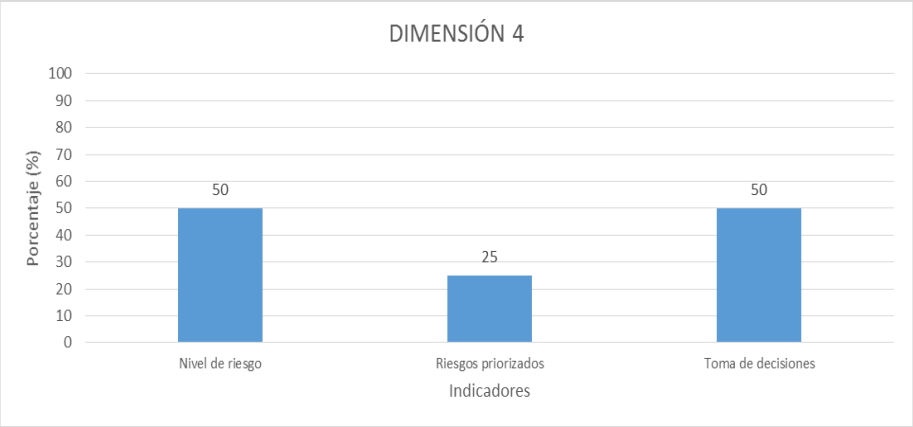


Figura 8. Cuadro de porcentaje del cumplimiento de la dimensión 4 de la variable gestión de riesgos
Fuente: Elaboración propia

Interpretación

En la Tabla se muestra el grado de cumplimiento de la dimensión 4 de la ISO 31000:2009 sobre la gestión de riesgos del Data Center, con un porcentaje total obtenido del 6,25 % del cumplimiento de la Norma ISO 31000:2009 siendo el porcentaje menor a comparación de las demás dimensiones. Además se demuestra en la Figura 9 el cuadro de barras de

los indicadores de la dimensión y su porcentaje correspondiente de acuerdo a la evaluación realizada.

ANÁLISIS DE RESULTADOS

Según Chillogallo & Zambrano (2016) en su trabajo de investigación “Elaboración de un modelo de gestión de riesgos de tecnologías de la información para la Fiscalía General del Estado” realizó una encuesta, la cual fue elaborada en base a las fases de la NTE-ISO 31000:2009 mostrando así en sus resultados para el cumplimiento de dicha norma en la institución en donde se realizó el estudio, muestra un porcentaje del 22,22 % de cumplimiento, teniendo en cuenta que se realizó el estudio para las siete fases como son establecimiento del contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento de riesgos, monitoreo y revisión y, comunicación y consultas.

En el presente trabajo de investigación se obtuvieron los resultados para la gestión de riesgos en el Data Center de la Municipalidad Distrital de Ilabaya en un porcentaje del 47,5 % de cumplimiento de la Norma ISO 31000:2009 teniendo en cuenta que se consideró las cuatro primeras fases, las cuales son las que se involucran para la propuesta realizada, con respecto a los resultados

obtenidos existe una diferencia entre los porcentajes obtenidos en ambos trabajos, extrayendo los porcentajes de las cuatro primeras fases de la investigación de Chillogallo & Zambrano (2016) se obtiene el promedio de 23,86 % significando que presentan debilidades en las fases consideradas, obtuvo el menor porcentaje en la fase de establecimiento del contexto permitiendo saber que no definen con claridad a los responsables ni las responsabilidades a cumplir, mientras que en el presente trabajo se tiene la fase de evaluación de riesgos con el menor porcentaje obtenido significando que no existe conocimiento de los riesgos priorizados, ni la comunicación adecuada con alta dirección para tomar las acciones necesarias en cuanto al presupuesto, personal disponible y demás recursos que involucraría el tratamiento de los mismos.

La metodología utilizada para obtener información para el estudio de la variable gestión de riesgos fue un cuestionario basado en las fases de la Norma ISO 31000:2009, y el criterio de evaluación se basó en calificar mediante una valoración de las actividades a tener en cuenta para una correcta gestión de riesgos según el estándar mencionado, siendo esta metodología comprensible para conocer el estado de cumplimiento de un sistema de gestión en una organización, tal como se aplicó en la investigación de Medina (2013).

La herramienta utilizada para obtener datos para el estudio de la variable, fue sometida a juicios de tres expertos, los cuales dieron sus recomendaciones para mejorar la obtención de los resultados y así realizar con precisión la recolección de datos. El cuestionario utilizado presenta un coeficiente Alfa de Cronbach de 0,889; por lo que se considera que la consistencia interna es buena y que el instrumento es fiable para medir el nivel de gestión de riesgos existente en el Data Center de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya.

CONCLUSIONES

- Se logró evaluar la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya, la evaluación se basó en la Norma ISO 31000:2009, obteniendo un 47,5 % de un correcto cumplimiento de la gestión de riesgos, es decir que existen aspectos deficientes que se deben mejorar y otros requisitos que deben ser implementados según la norma, lo cual expresa que actualmente la gestión de riesgos que viene siendo cumplida por la institución se encuentra en un nivel medio.

- Se logró evaluar el contexto respecto a la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya, obteniendo un 12,5 % del cumplimiento respecto al requerimiento que establece la Norma ISO 31000:2009, en consecuencia sus actividades actuales no están acordes con la norma en su totalidad.

- Se logró evaluar la identificación de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya, además de obtener un 17,5 % del cumplimiento respecto al requerimiento que establece la Norma ISO 31000:2009, demostrando que no se tiene una visión clara de los riesgos

existentes, sean internos o externos, así como las fuentes de riesgo y zonas de impacto.

- Se logró evaluar el análisis de los riesgos del Data Center de la Municipalidad Distrital de Ilabaya, obteniendo un nivel de cumplimiento del 11,25 % respecto al requerimiento que establece la Norma ISO 31000:2009, en consecuencia se deben implementar controles de gestión de riesgos para un mejor tratamiento de las causas, consecuencias y su probabilidad de ocurrencia.

- Se logró evaluar los riesgos valorados según el diagnóstico del cuestionario para la fase de evaluación de riesgos que involucra los riesgos priorizados y la toma de decisiones, de tal manera se alcanzó un 6,25 % del nivel de cumplimiento según la ISO 31000. Entre los riesgos priorizados existentes en el Data Center los cuales afectan a los activos siguientes como los Servidores Dell Power Edge R220, Switch Core, Cableados estructurados y Servidores para Host de Virtualización Blade IBM todos ellos con amenaza de Corte de Suministro Eléctrico y con susceptibilidad a las variaciones de voltaje, dichos riesgos se muestran en la Tabla .

RECOMENDACIONES

- Según la investigación realizada sobre el estudio de la evaluación de la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basándose en la Norma ISO 31000:2009, se recomienda seguir los alineamientos que brinda la norma, para mejorar este proceso actual, aunque no siempre será necesario utilizar todos los requerimientos de las normas internacionales y adecuarlas según sea el caso a estudiar o evaluar.

- Se recomienda tomar en cuenta las deficiencias y carencias encontradas para una correcta gestión de riesgos y reforzarlas con la propuesta para la mejora de la gestión de riesgos en el Data Center de la Municipalidad Distrital de Ilabaya, de tal manera tiene como objetivo completar y optimizar cada uno de sus pasos involucrados según la Norma ISO 31000:2009.

- Se recomienda continuar con el estudio de la evaluación de la gestión de riesgos con respecto a todos los criterios basados en la Norma ISO 31000:2009, a fin de contar con un sistema de gestión de riesgos totalmente implementado, como parte vital para iniciar la implementación de un Sistema de Seguridad de la Información el cual permita preservar la confidencialidad, integridad y disponibilidad de la información.

- Se recomienda mejorar el desempeño de los procesos externos e internos de la Municipalidad Distrital de Ilabaya con una óptima toma de decisiones sobre la gestión de los riesgos identificados, de los cuales deben ser partícipes los responsables que pertenecen al nivel gerencial.

- Según la propuesta planteada para la mejora de la gestión de riegos del Data Center de la Municipalidad Distrital de Ilabaya, se recomienda utilizarla y acondicionarla a los nuevos procesos o cambios que se puedan producir en la institución para que puedan continuar con los lineamientos de la norma y alcanzar sus objetivos.

REFERENCIAS BIBLIOGRÁFICAS

Arias, Y. L., Dias, M. L., & Vargas, J. A. (2014). *Elaboración de una Guía de Gestión de Riesgos Basados en la Norma NTC-ISO 31000 para el Proceso de Gestión de Incidentes y Peticiones de Servicio del Área de Mesa de Ayuda de Empresas de Servicios de Soporte de Tecnología en Colombia.* Colombia.

Arteaga, C. M., Villa, P. A., & Ladino, M. I. (2014). *Definición de una Metodología de Gestión de Riesgos para Entidades del Sector Público bajo el Estándar ISO 27001. Journal de Ciencia e Ingenieria*, pp 28-36.

Chillogallo, E. J., & Zambrano, V. H. (2016). *Elaboración de un Modelo de gestión de riesgos de Tecnologías de Información para la Fiscalia General del Estado. (Tesis de posgrado), Escúela Politécnica Nacional,* Ecuador.

CIIFEN.(2016). Centro Internacional para la Investigación del fenómeno del niño. Obtenido de www.ciifen.org

Corral , Y. (2009). *Validez y Confiabilidad de los Instrumentos de la Investigación para la Recolección de Datos. Revista Ciencias de la Educación*, volumen (33), pp 20.

Enriquez, & Hidalgo. (2015). *Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama. Revista Politécnica*.

Fundación Telefónica. (2016). *La COFA Observatorio Técnologico.* Obtenido de https://lacofa.fundaciontelefonica.com

Gil Ojeda, Y., & Vallejo Garcia, E. (2008). *Guia para la Identificación y Análisis de los Procesos de la Universidad de Málaga*.España

Hernandez, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación (Quinta Edición).* Mexico: McGraw-HILL/INTERAMERICANA EDITORES S.A. DE C.V.

International Organization for Standardization. (2016). *ISO.* Obtenido de ISO: http://www.iso.org

ISO73. (2009). *GUIDE 73 Risk management Vocabulary*. Obtenido de ISO: http://www.iso.org

José-Marti, I. C. (2013). *Proceso de Gestión de riesgo y Seguros en las empresas.* CASARES, Asesoría Actuarial y de Riesgos, S.L.

Macau, R. (2004). *TIC : Funciones de las tecnologias de la informacion y la comunicacion en las organizaciones. Revista de Universidad y Sociedad del Conocimiento, volumen* (1).

Medina Bocanegra, J. A. (2013). *Propuesta para Implementación del Sistema de Gestión de Calidad basado en la Norma ISO 9001:2008 en una Empresa del Sector Construcción.* Lima: “.

Monje, C. A. (2011). *Metodología de la Investigación Cuantitativa y Cualitativa.* Neiva.

Olano M., A. (2010). *Diseños de Investigación Educacional.* Lima.

Pérez, E., & Cristian Arias. (2011). *Diseño de un Sistema de Gestión de la Calidad basado en la Norma ISO 9001:2008 para una empresa que comercializa artículos de ferretería en la Ciudad de Guayaquil. Guayaquil*, Ecuador.

Pestana, F. M., & Stracuzzi, S. P. (2012). *Metodología de laInvestigación Cuantitativa (edicion 2012).* Caracas: Fedupel.

Pineda, E. B., De Canales, F. H., & Alvarado, E. L. (1994). *Metodología de la Investigación - 2da edición.* Washington: Novi Mundi.

Quintero, E. T., Ascanio, S. L., & Cardenas, Y. K. (2015). *Guía de Gestión de Riesgos para el Departamento de Sistemas de la Empresa Apuestas Cúcuta 75*. Colombia.

Real Academia Española. (2016). *Real Academia Española.* Obtenido de Real Academia Española: http://dle.rae.es

Serra, C. (2016). *ISO 31000:2009. Herramienta para evaluar la gestión de riesgos* . Obtenido de ISACA: http://www.isaca.org

Sotelo, M., Torres, J., & Rivera, J. (2012). *Un Proceso Práctico de Ánalisi de Riesgos de Activos de Información*.

Supo, J. (2015). *Como Empezar una Tesis, Primera edición.* Arequipa: BIOESTADISTICO EIRL.

ANEXOS

ANEXO 01 MATRIZ DE CONSISTENCIA

Tabla 31
Matriz de consistencia

Título: Evaluación de la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basada en la ISO 31000, Tacna 2016

Planteamiento del problema	Objetivos de la investigación	Variables	
Problema General	**Objetivo General**	**Variable :** gestión de riesgos	
		Dimensiones	**Indicadores**
¿Cómo es la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basada en la ISO 31000?	Evaluar la gestión de riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000.	D1: Establecer contexto del Data Center	I1: Objetivos definidos
			I2: Estrategias definidas
			I3: Responsables asignados
			I4 : Procesos identificados
			I5: Recursos identificados
Problemas específicos :	**Objetivos específicos:**	D2: Identificar riesgos del Data Center	I1: Riesgos internos
a) ¿Cómo es el contexto del Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?	a) Evaluar el contexto del Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000		I2: Riesgos externos
b) ¿Cómo es la identificación de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?	b) Evaluar la identificación de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000		I3: Fuentes de riesgo
c) ¿Cómo es el análisis de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?	c) Evaluar el análisis de los riesgos para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000		I4: Zonas de impacto
d) ¿Cómo es la evaluación de los riesgos priorizados para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000?	d) Evaluar los riesgos priorizados para el Data Center de la Municipalidad Distrital de Ilabaya basado en la ISO 31000	D3: Analizar riesgos en el Data Center	I1: Controles de gestión de riesgo
			I2: Probabilidad de ocurrencia
			I3 : Causas
			I4: Consecuencias
		D4: Evaluar riesgos del Data Center	I1: Riesgos priorizados
			I2 : Actividades de reducción
			I3: Toma de decisiones

Población	Técnica - Instrumento
El tamaño de la población es de N= 10 personas en la Sub Gerencia de Tecnologías de la Información y Comunicaciones	Encuesta – cuestionario
Muestra	**Diseño de la investigación**
Se trabajó con toda la población, donde n=N=10 personas de la Sub Gerencia de Tecnologías de la Información y Comunicaciones	Diseño no experimental – nivel descriptivo

Fuente: Elaboración propia

ANEXO 02

INSTRUMENTO APLICADO PARA LA VARIABLE: GESTIÓN DE RIESGOS

El siguiente cuestionario tiene por objetivo conocer el nivel de la gestión de riesgos en el Data Center con respecto a la Norma ISO 31000:2009

- Instrucciones: Marque con una aspa (x) o encierre en un círculo la opción de respuesta que usted considere más adecuada, solo seleccione una opción. No deje respuestas en blanco.

  En el siguiente cuadro se detalla las siguientes opciones como alternativas con su respectiva valorización con la cual se realizara el análisis de datos respectivo para el presente cuestionario.

Tabla 32
Criterios de evaluación para el cuestionario

Criterio de evaluación	Valorización (%)
(N) Nunca (MM) Muy malo (MB) Muy bajo	0
(CN) Casi nunca (B) Bajo	25
(AV) A veces (R) Regular	50
(CS) Casi siempre (A) Alto (F) Frecuente	75
(S) Siempre (MF) Muy frecuente (MA) Muy alto	100

Fuente: Elaboración propia

Establecer contexto

1. ¿Se definen claramente los **objetivos** para la gestión de riesgos sobre el Data Center de la institución?

   a) Siempre
   b) Casi siempre
   c) A veces
   d) Casi nunca
   e) Nunca

2. ¿Se proponen **estrategias** para la gestión de riesgos sobre el Data Center de la institución?

   a) Siempre
   b) Casi siempre
   c) A veces
   d) Casi nunca
   e) Nunca

3. ¿Se definen claramente a los **responsables** para la gestión de riesgos del Data Center de la organización?

   a) Siempre
   b) Casi siempre
   c) A veces
   d) Casi nunca
   e) Nunca

4. ¿Cumplen con los **procesos** necesarios para el correcto funcionamiento del Data Center de la institución?

   a) Siempre
   b) Casi siempre
   c) A veces
   d) Casi nunca
   e) Nunca

5. ¿Se identifican claramente los **recursos** que pueden ser afectados por los riesgos en el Data Center de la institución?

   a) Siempre
   b) Casi siempre
   c) A veces
   d) Casi nunca
   e) Nunca

Identificar riesgos

6. ¿Cómo es el nivel de control de **riesgos internos** en el Data Center de la institución?

   a) Muy bueno
   b) Bueno
   c) Regular
   d) Mala
   e) Muy mala

7. ¿Se identifican claramente las posibles **causas** de los **riesgos internos** en el Data Center de la institución?

a) Siempre
b) Casi siempre
c) A veces
d) Casi nunca
e) Nunca

8. ¿Se identifican claramente las posibles **consecuencias** de los **riesgos internos** en el Data Center de la institución?

a) Siempre
b) Casi siempre
c) A veces
d) Casi nunca
e) Nunca

9. ¿Cómo es el nivel de control de **riesgos externos** sobre el Data Center de la institución?

a) Muy bueno
b) Bueno
c) Regular
d) Mala
e) Muy mala

10. ¿Se identifican claramente las posibles **causas** de los **riesgos externos** sobre el Data Center de la institución?

a) Siempre
b) Casi Siempre
c) A veces
d) Casi nunca
e) Nunca

11. ¿Se identifican claramente las posibles **consecuencias** de los **riesgos externos** sobre el Data Center de la Institución?

a) Siempre
b) Casi siempre
c) A veces
d) Casi nunca
e) Nunca

12. ¿Se identifican claramente las **fuentes de riesgos** que pueden afectar el Data Center de la institución?

a) Siempre
b) Casi siempre
c) A veces
d) Casi nunca
e) Nunca

13. ¿Se identifican claramente las **zonas de impacto** que pueden ser afectadas por los riesgos en el Data Center de la institución?

a) Siempre
b) Casi siempre
c) A veces
d) Casi nunca
e) Nunca

Analizar riesgos

14. ¿Cómo es el nivel de adaptación de los **controles** de gestión de riesgos en el Data Center de la institución?

    a) Muy bueno
    b) Bueno
    c) Regular
    d) Mala
    e) Muy mala

15. ¿Cómo considera a la **probabilidad** de ocurrencia de los riesgos en el Data Center de la institución?

    a) Muy frecuente
    b) Frecuente
    c) A veces
    d) Casi nunca
    e) Nunca

16. ¿Cómo considera el **nivel de existencia** de las causas de los riesgos definidos sobre el Data Center?

    a) Muy alto
    b) Alto
    c) Regular
    d) Bajo
    e) Muy bajo

17. ¿Cómo considera el **nivel de impacto de las consecuencias** producidas por los riesgos definidos sobre el Data Center?

    a) Muy alto
    b) Alto
    c) Regular
    d) Bajo
    e) Muy bajo

Evaluar riesgos

18. ¿Cómo considera el **nivel de riesgo** en el Data Center de la institución?

    a) Muy alto
    b) Alto
    c) Regular
    d) Bajo
    e) Muy bajo

19. ¿Qué nivel de importancia se le da a las **actividades de reducción** de los riesgos?

    a) Muy alto
    b) Alto
    c) Regular
    d) Bajo
    e) Muy bajo

20. ¿**Se informa sobre los factores de riesgo a alta dirección** para la toma de decisiones correspondientes?

    a) Siempre
    b) Casi siempre
    c) A veces
    d) Casi nunca
    e) Nunca

Tabla 33
Datos del cuestionario

sujeto	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20
S1	3	3	4	4	3	3	4	4	3	4	4	4	4	3	3	3	3	2	3	3
S2	3	3	3	3	4	3	2	2	2	3	3	3	2	2	4	4	4	4	2	3
S3	4	2	4	4	2	3	3	3	3	4	4	4	3	3	3	3	3	3	4	4
S4	3	4	3	3	4	2	3	4	3	3	4	4	4	3	3	3	3	4	2	3
S5	3	2	4	2	3	4	2	3	4	2	4	4	4	4	3	3	4	3	2	4
S6	4	3	3	3	4	4	4	4	4	2	4	4	2	3	4	4	4	2	4	3
S7	4	2	3	4	4	4	2	2	3	4	4	4	4	4	2	4	4	2	4	4
S8	2	1	1	1	2	2	2	2	3	2	2	2	2	2	1	3	4	4	1	1
S9	2	2	3	3	3	3	3	2	3	3	2	2	2	3	5	4	4	3	2	3
S10	2	2	2	3	2	3	2	2	3	2	2	2	2	3	2	3	2	3	2	2

Fuente: Elaboración propia

ANEXO 04
CONFIABILIDAD DE INSTRUMENTO

Tabla 6
Resumen de respuestas del personal administrativo de la SGTIC

sujeto	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	total
S1	3	3	4	4	3	3	4	4	3	4	4	4	4	3	3	3	3	2	3	3	67
S2	3	3	3	3	4	3	2	2	2	3	3	3	2	2	4	4	4	4	2	3	59
S3	4	2	4	4	2	3	3	3	3	4	4	4	3	3	3	3	3	3	4	4	66
S4	3	4	3	3	4	2	3	4	3	3	4	4	4	3	3	3	3	4	2	3	65
S5	3	2	4	2	3	4	2	3	4	2	4	4	4	4	3	3	4	3	2	4	64
S6	4	3	3	3	4	4	4	4	4	2	4	4	2	3	4	4	4	2	4	3	69
S7	4	2	3	4	4	4	2	2	3	4	4	4	4	4	2	4	4	2	4	4	68
S8	2	1	1	1	2	2	2	2	3	2	2	2	2	2	1	3	4	4	1	1	40
S9	2	2	3	3	3	3	3	2	3	3	2	2	2	3	5	4	4	3	2	3	57
S10	2	2	2	3	2	3	2	2	3	2	2	2	2	3	2	3	2	3	2	2	46
varianza	0.7	0.7	0.9	0.9	0.8	0.5	0.7	0.8	0.3	0.8	0.9	0.9	1	0.4	1.3	0.3	0.5	0.7	1.2	0.9	

Fuente: Elaboración propia

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

Figura 9: Fórmula para cálculo de Coeficiente de Alfa de Cronbach
Fuente: Elaboración propia

Donde: K = número de ítems
S_i^2 = Sumatoria de varianzas independientes
S_t^2 = Varianza total

Tabla 7
Resultado de confiabilidad del cuestionario

Alfa de CRONBACH	Número de elementos
0.889	20

Fuente: Elaboración propia

ANEXO 05

RESULTADOS DE LOS INDICADORES

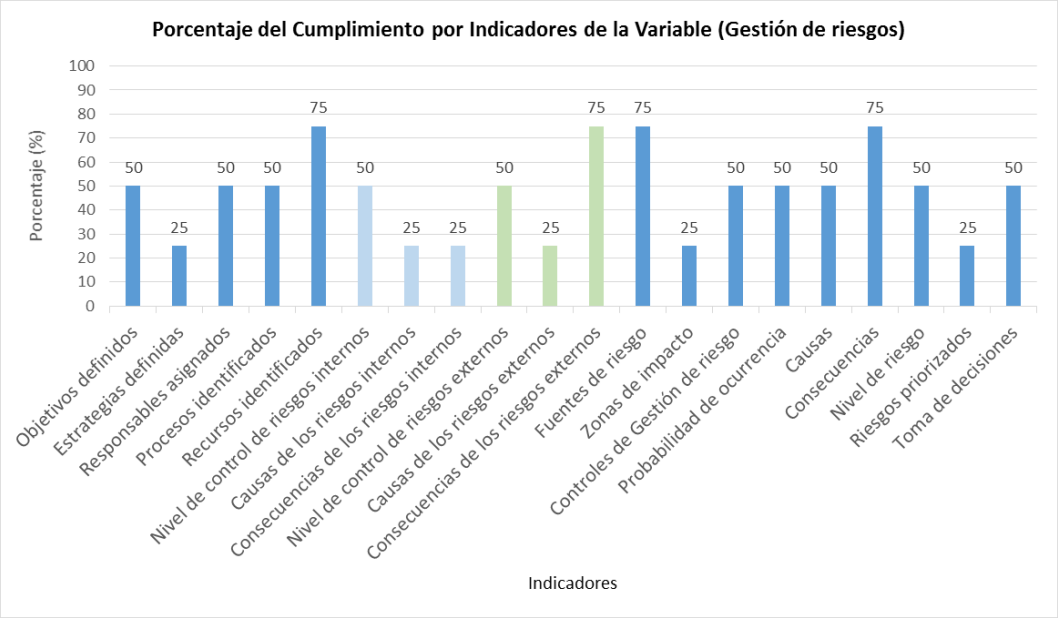


Figura 10. Grado de cumplimiento de la ISO 31000:2009 sobre la variable gestión de riesgos (por indicadores)
Fuente: Elaboración propia

ANEXO 06

FICHAS DE VALIDACIÓN DEL INSTRUMENTO

MATRIZ DE VALIDACIÓN DE INSTRUMENTO

NOMBRE DEL INSTRUMENTO: Cuestionario

OBJETIVO: Conocer el nivel de la Gestión de riesgos existente en el Data Center de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya.

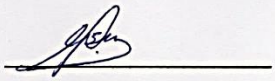
DIRIGIDO A: Personal administrativo de la Sub Gerencia de Tecnologías de la Información y Comunicaciones.

APELLIDOS Y NOMBRES DEL EVALUADOR:

GRADO ACADEMICO DEL EVALUADOR:

VALORACION:

CRITERIO DE EVALUACIÓN	ESCALA
(N) Nunca (MM) Muy Malo (MB) Muy bajo	1
(CN) Casi Nunca (B) Bajo	2
(AV) A veces (R) Regular	3
(CS) Casi siempre (A) Alto (F) Frecuente	4
(S) Siempre (MF) Muy Frecuente (MA) Muy Alto	5



FIRMA DEL EVALUADOR

Dr. Ernst F. Otto Manani

MATRIZ DE VALIDACIÓN

VARIABLE	DIMENSION	INDICADOR	ITEMS	CRITERIOS DE EVALUACION								OBSERVACION Y/O RECOMENDACIONES
				Relación entre la Variable y la Dimensión		Relación entre la Dimensión y el Indicador		Relación entre el Indicador y el Ítems		Relación entre el Ítems y la Opción de respuesta		
				SI	NO	SI	NO	SI	NO	SI	NO	
GESTION DE RIESGO	Establecer contexto	Objetivos definidos	¿Se definen claramente los objetivos para la gestión de riesgos sobre el Data Center de la Institución?	X		X		X		X		
		estrategias definidas	¿Se proponen estrategias para la Gestión de Riesgos sobre el Data Center de la Institución?			X		X		X		
		responsables asignados	¿Se definen claramente a los responsables para la gestión de riesgos del Data Center de la Organización?			X		X		X		
		procesos identificados	¿Cumplen con los procesos necesarios para el correcto funcionamiento del Data Center de la Institución?			X		X		X		
		recursos identificados	¿Se identifican claramente los recursos que pueden ser afectados por los riesgos en el Data center de la Institución?			X		X		X		
	Identificar riesgos	Riesgos internos	¿Cómo es el nivel de control de riesgos internos en el Data center de la Institución?	X		X		X		X		
			¿Se identifican claramente las posibles causas de los riesgos internos en el Data Center de la Institución?					X		X		
			¿Se identifican claramente las posibles consecuencias de los riesgos internos en el Data Center de la Institución?					X		X		
		Riesgos externos	¿Cómo es el nivel de control de riesgos externos sobre el Data center de la institución?			X		X		X		
			¿Se identifican claramente las posibles causas de los riesgos externos sobre el Data Center de la Institución?					X		X		
			¿Se identifican claramente las posibles consecuencias de los riesgos externos sobre el Data Center de la Institución?					X		X		
		Fuentes de riesgo	¿Se identifican claramente las fuentes de riesgos que pueden afectar el Data center de la Institución?			X		X		X		
		Zonas de Impacto	¿Se identifican claramente las zonas de impacto que pueden ser afectadas por los riesgos en el Data Center de la Institución?			X		X		X		
	Analizar riesgos	Controles de Gestión de riesgo	¿Cómo es el nivel de adaptación de los controles de gestión de riesgos en el Data Center de la Institución?	X		X		X		X		
		Probabilidad de Ocurrencia	¿Cómo considera a la probabilidad de ocurrencia de los riesgos en el Data Center de la Institución?			X		X		X		
		Causas	¿Cómo considera el nivel de existencia de las causas de los riesgos definidos sobre el Data Center?			X		X		X		
		Consecuencias	¿Cómo considera el nivel de impacto de las consecuencias producidas por los riesgos definidos sobre el Data Center?			X		X		X		
	Evaluar riesgos	Nivel de riesgo	¿Cómo considera el nivel de riesgo en el Data Center de la Institución?	X		X		X		X		
		Riesgos priorizados	¿Qué nivel de importancia se le da a las actividades de reducción de los riesgos?			X		X		X		
		Toma de decisiones	¿Se informa sobre los factores de riesgo a alta dirección para la toma de decisiones correspondientes?			X		X		X		

FIRMA DEL EVALUADOR

Dr. Gleny F. Osco Mamani

MATRIZ DE VALIDACIÓN DE INSTRUMENTO

NOMBRE DEL INSTRUMENTO: Cuestionario

OBJETIVO: Conocer el nivel de la Gestión de riesgos existe en el Data Center de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya.

DIRIGIDO A: Personal administrativo de la Sub Gerencia de Tecnologías de la Información y Comunicaciones.

APELLIDOS Y NOMBRES DEL EVALUADOR:

GRADO ACADEMICO DEL EVALUADOR:

VALORACION:

CRITERIO DE EVALUACIÓN	ESCALA
(N) Nunca (MM) Muy Malo (MB) Muy bajo	1
(CN) Casi Nunca (B) Bajo	2
(AV) A veces (R) Regular	3
(CS) Casi siempre (A) Alto (F) Frecuente	4
(S) Siempre (MF) Muy Frecuente (MA) Muy Alto	5

Ing. Johans Pimentel Zegarra
CIP. 149420

FIRMA DEL EVALUADOR

MATRIZ DE VALIDACIÓN

VARIABLE	DIMENSION	INDICADOR	ITEMS	CRITERIOS DE EVALUACION								OBSERVACION Y/O RECOMENDACIONES
				Relación entre la Variable y la Dimensión		Relación entre la Dimensión y el Indicador		Relación entre el Indicador y el Ítems		Relación entre el Ítems y la Opción de respuesta		
				SI	NO	SI	NO	SI	NO	SI	NO	
GESTION DE RIESGO	Establecer contexto	Objetivos definidos	¿Se definen claramente los objetivos para la gestión de riesgos sobre el Data Center de la Institución?	X		X		X		X		
		estrategias definidas	¿Se proponen estrategias para la Gestión de Riesgos sobre el Data Center de la Institución?			X		X		X		
		responsables asignados	¿Se definen claramente a los responsables para la gestión de riesgos del Data Center de la Organización?			X		X		X		
		procesos identificados	¿Cumplen con los procesos necesarios para el correcto funcionamiento del Data Center de la Institución?			X		X		X		
		recursos identificados	¿Se identifican claramente los recursos que pueden ser afectados por los riesgos en el Data center de la Institución?			X		X		X		
	Identificar riesgos	Riesgos internos	¿Cómo es el nivel de control de riesgos internos en el Data center de la Institución?	X		X		X		X		
			¿Se identifican claramente las posibles causas de los riesgos internos en el Data Center de la Institución?					X		X		
			¿Se identifican claramente las posibles consecuencias de los riesgos internos en el Data Center de la Institución?					X		X		
		Riesgos externos	¿Cómo es el nivel de control de riesgos externos sobre el Data center de la institución?			X		X		X		
			¿Se identifican claramente las posibles causas de los riesgos externos sobre el Data Center de la Institución?			X		X		X		
			¿Se identifican claramente las posibles consecuencias de los riesgos externos sobre el Data Center de la Institución?					X		X		
		Fuentes de riesgo	¿Se identifican claramente las fuentes de riesgos que pueden afectar el Data center de la Institución?			X		X		X		
		Zonas de Impacto	¿Se identifican claramente las zonas de impacto que pueden ser afectadas por los riesgos en el Data Center de la Institución?			X		X		X		
	Analizar riesgos	Controles de Gestión de riesgo	¿Cómo es el nivel de adaptación de los controles de gestión de riesgos en el Data Center de la Institución?	X		X		X		X		
		Probabilidad de Ocurrencia	¿Cómo considera a la probabilidad de ocurrencia de los riesgos en el Data Center de la Institución?			X		X		X		
		Causas	¿Cómo considera el nivel de existencia de las causas de los riesgos definidos sobre el Data Center?			X		X		X		
		Consecuencias	¿Cómo considera el nivel de impacto de las consecuencias producidas por los riesgos definidos sobre el Data Center?			X		X		X		
	Evaluar riesgos	Nivel de riesgo	¿Cómo considera el nivel de riesgo en el Data Center de la Institución?	X		X		X		X		
		Riesgos priorizados	¿Qué nivel de importancia se le da a las actividades de reducción de los riesgos?			X		X		X		
		Toma de decisiones	¿Se informa sobre los factores de riesgo a alta dirección para la toma de decisiones correspondientes?			X		X		X		

Mg. Jonans Pimentel Zegar
CIP. 149420

FIRMA DEL EVALUADOR

MATRIZ DE VALIDACIÓN DE INSTRUMENTO

NOMBRE DEL INSTRUMENTO: Cuestionario

OBJETIVO: Conocer el nivel de la Gestión de riesgos existe en el Data Center de la Sub Gerencia de Tecnologías de la Información y Comunicaciones de la Municipalidad Distrital de Ilabaya.

DIRIGIDO A: Personal administrativo de la Sub Gerencia de Tecnologías de la Información y Comunicaciones.

APELLIDOS Y NOMBRES DEL EVALUADOR:

GRADO ACADEMICO DEL EVALUADOR:

VALORACION:

CRITERIO DE EVALUACIÓN	ESCALA
(N) Nunca (MM) Muy Malo (MB) Muy bajo	1
(CN) Casi Nunca (B) Bajo	2
(AV) A veces (R) Regular	3
(CS) Casi siempre (A) Alto (F) Frecuente	4
(S) Siempre (MF) Muy Frecuente (MA) Muy Alto	5

Ing. CIP. ALBERTO JOHNATAN FLOR RODRIGUEZ
Registro 133642 - SISTEMAS

FIRMA DEL EVALUADOR

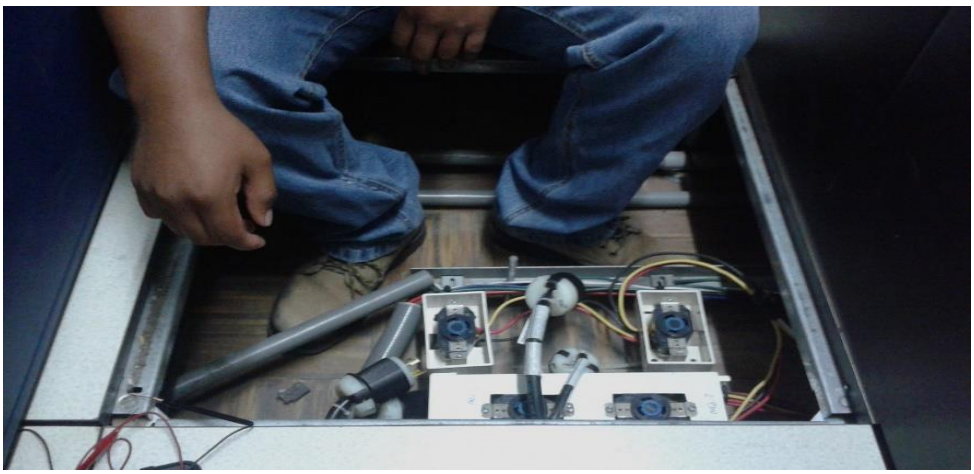
MATRIZ DE VALIDACIÓN

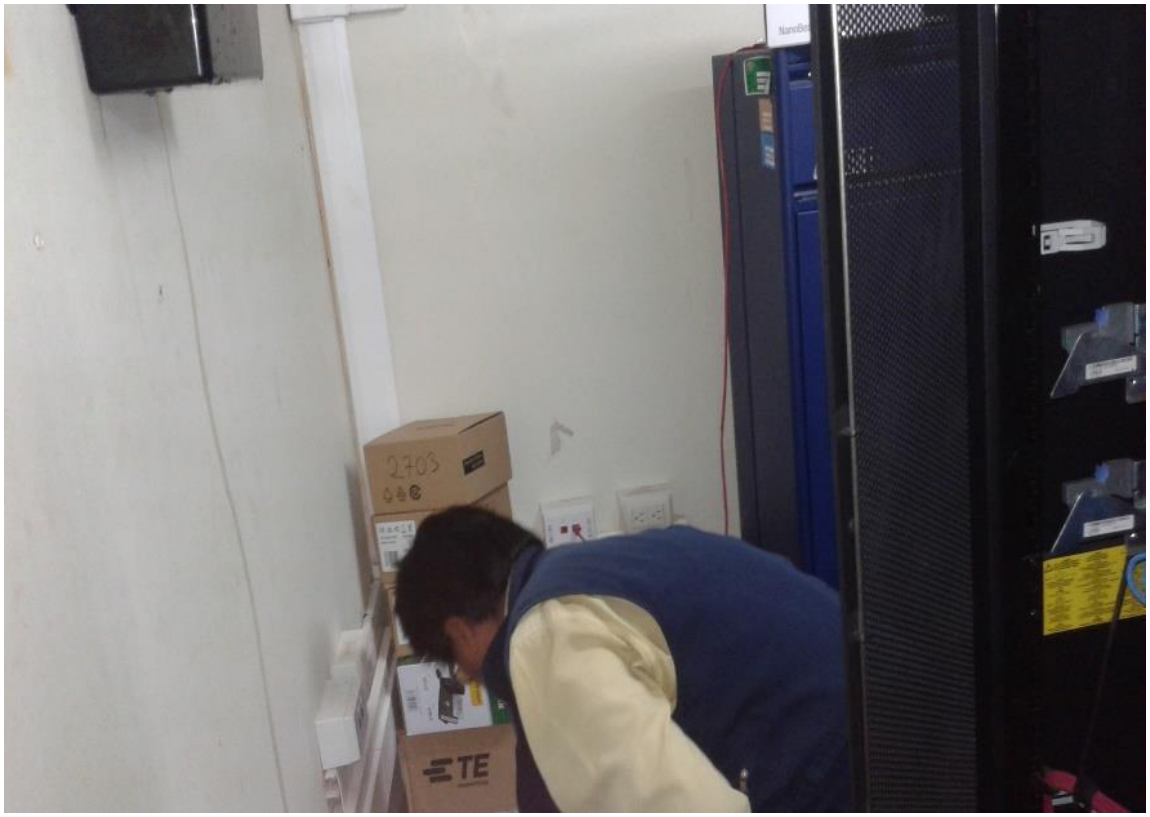
VARIABLE	DIMENSION	INDICADOR	ITEMS	CRITERIOS DE EVALUACION								OBSERVACION Y/O RECOMENDACIONES
				Relación entre la Variable y la Dimensión		Relación entre la Dimensión y el Indicador		Relación entre el Indicador y el Ítems		Relación entre el Ítems y la Opción de respuesta		
				SI	NO	SI	NO	SI	NO	SI	NO	
GESTION DE RIESGO	Establecer contexto	Objetivos definidos	¿Se definen claramente los objetivos para la gestión de riesgos sobre el Data Center de la Institución?	X		X		X		X		
		estrategias definidas	¿Se proponen estrategias para la Gestión de Riesgos sobre el Data Center de la Institución?			X		X		X		
		responsables asignados	¿Se definen claramente a los responsables para la gestión de riesgos del Data Center de la Organización?			X		X		X		
		procesos identificados	¿Cumplen con los procesos necesarios para el correcto funcionamiento del Data Center de la Institución?			X		X		X		
		recursos identificados	¿Se identifican claramente los recursos que pueden ser afectados por los riesgos en el Data center de la Institución?			X		X		X		
	Identificar riesgos	Riesgos internos	¿Cómo es el nivel de control de riesgos internos en el Data center de la Institución?	X		X		X		X		
			¿Se identifican claramente las posibles causas de los riesgos internos en el Data Center de la Institución?					X		X		
			¿Se identifican claramente las posibles consecuencias de los riesgos internos en el Data Center de la Institución?					X		X		
		Riesgos externos	¿Cómo es el nivel de control de riesgos externos sobre el Data center de la institución?			X		X		X		
			¿Se identifican claramente las posibles causas de los riesgos externos sobre el Data Center de la Institución?					X		X		
			¿Se identifican claramente las posibles consecuencias de los riesgos externos sobre el Data Center de la Institución?					X		X		
		Fuentes de riesgo	¿Se identifican claramente las fuentes de riesgos que pueden afectar el Data center de la Institución?			X		X		X		
		Zonas de Impacto	¿Se identifican claramente las zonas de impacto que pueden ser afectadas por los riesgos en el Data Center de la Institución?			X		X		X		
	Analizar riesgos	Controles de Gestión de riesgo	¿Cómo es el nivel de adaptación de los controles de gestión de riesgos en el Data Center de la Institución?	X		X		X		X		
		Probabilidad de Ocurrencia	¿Cómo considera a la probabilidad de ocurrencia de los riesgos en el Data Center de la Institución?			X		X		X		
		Causas	¿Cómo considera el nivel de existencia de las causas de los riesgos definidos sobre el Data Center?			X		X		X		
		Consecuencias	¿Cómo considera el nivel de impacto de las consecuencias producidas por los riesgos definidos sobre el Data Center?			X		X		X		
	Evaluar riesgos	Nivel de riesgo	¿Cómo considera el nivel de riesgo en el Data Center de la Institución?	X		X		X		X		
		Riesgos priorizados	¿Qué nivel de importancia se le da a las actividades de reducción de los riesgos?			X		X		X		
		Toma de decisiones	¿Se informa sobre los factores de riesgo a alta dirección para la toma de decisiones correspondientes?			X		X		X		

Ing. CIP. ALBERTO JOHNATAN FLOR RODRIGUEZ
Registro 133642 - SISTEMAS
FIRMA DEL EVALUADOR

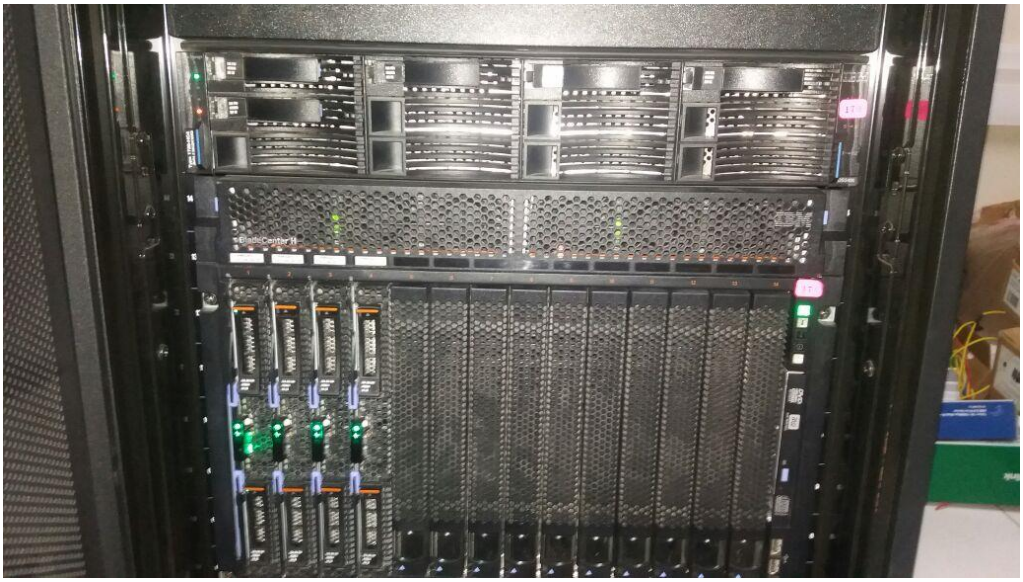
ANEXO 07

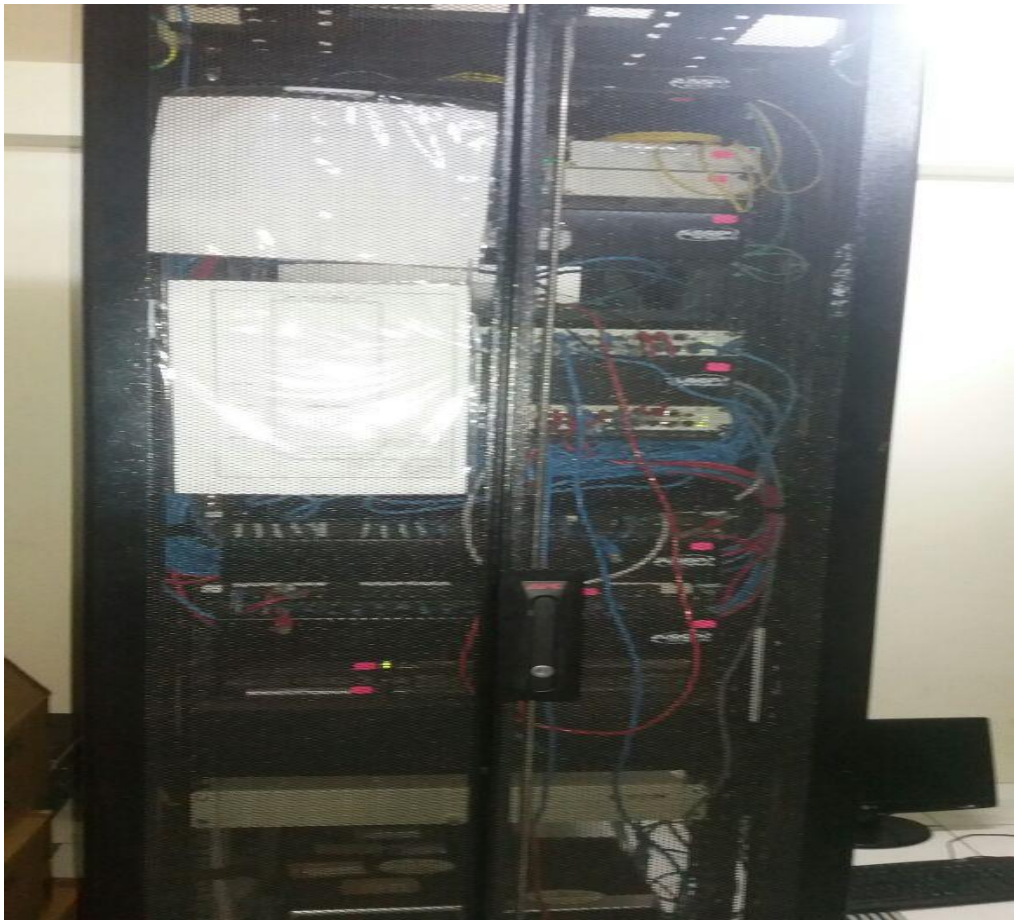
FOTOS




TE


GABINETE DE SERVIDORES S - 01





ANEXO 08

8.10. SUB GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La Sub Gerencia de Tecnologías de la Información y Comunicaciones, es la unidad orgánica a cargo de los sistemas de información, comunicación, infraestructura tecnológica y soporte técnico en la Municipalidad, responsable del desarrollo, análisis, diseño, programación y mantenimiento de toda la plataforma tecnológica de la Municipalidad y la implementación de la plataforma de tecnologías de la información y comunicaciones.

A. DIAGNÓSTICO SITUACIONAL

Cuadro N° 29. – Análisis FODA de la Sub Gerencia de Tecnologías de Información y Comunicaciones

FORTALEZAS	DEBILIDADES
• Personal con experiencia y capacidad técnica para la ejecución de sus labores en los diversos aspectos que conllevan las TICs en la Municipalidad (Desarrollo de software, Administración de Redes y Telecomunicaciones). • Disponibilidad de trabajo en equipo, integración y una adecuada delegación de tareas que propician el adecuado cumplimiento de las mismas. • Personal profesional y técnico flexible al cambio tecnológico; no es reacio a la implementación de nuevas tecnologías, incluso colabora para la mejora y la Propuesta de nuevas alternativas. • Equipos de despliegue de Red conectado y configurado de manera adecuada. • Red física de datos certificada por empresas líderes en su rubro a nivel nacional. • Cedes Municipales interconectadas por canales comunicación formales además de La inclusión de la telefonía interna intercedes.	• Carencia de asignación presupuestal para la atención a las necesidades y proyecciones del ámbito de Tecnologías de Información y comunicaciones en la Municipalidad Distrital de Ilabaya • Presupuesto nulo para la capacitación del personal informático, así como de los permisos respectivos para asistir a capacitaciones. • Capacidad limitada de almacenamiento para albergar información digital. • Índice elevado en las solicitudes de soporte.
OPORTUNIDADES	**AMENAZAS**
• Instalación de Empresas de telefonía e internet por fibra óptica. • La MDI cuenta con una partida presupuestal del canon minero para invertir en lo que respecta a Tecnología.	• Cortes intempestivos de energía eléctrica. • Cortes de Red e internet (radioenlaces) debido a factor climático.

Fuente: Sub Gerencia de Tecnologías de Información y Comunicaciones

B. CRONOGRAMA DE ACTIVIDADES

Cuadro N° 30.– Actividades del POI de la Sub Gerencia de Tecnologías de Información y Comunicaciones

UNIDAD ORGÁNICA	**SUB GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**
RESPONSABLE	**ING. LUIS ANGEL CALDERON BARIA**
MISIÓN	Somos una institución transparente con vocación de servicios de calidad, que promueve el desarrollo social, económico y tecnológico, en beneficio de la población de Ilabaya.
OBJETIVO ESTRATÉGICO	Promover el aprovechamiento de las tecnologías de información.

ITEM	DENOMINACIÓN	INDICADOR	PONDERACIÓN (%)	UNIDAD DE MEDIDA	METAS PROGRAMADAS SEMESTRE		META ANUAL
					1	2	
1	Mantenimiento de Sistemas de protección DATA CENTER puesta a tierra, alarmas, seguridad, aire acondicionado).	Número de Mantenimientos semestral	7%	Documento	1	1	2
2	Mantenimiento de equipos de contingencia (Grupos electrógeno, UPS, banco de baterías, paneles solares).	Número de Mantenimientos semestral	8%	Documento	1	1	2
3	Mantenimiento de hardware y software del parque informático de la MDI (mantenimiento y soporte parque informático de los diferentes anexos, colegios de la Jurisdicción).	Número de Mantenimientos mensual	7%	Documento	1	1	2
4	Mantenimiento de hardware y software de equipos de networking (Switch, Gabinetes, Ap, actualización de fireware, certificación).	Número de Mantenimientos semestral	9%	Documento	1	1	2
5	Mantenimiento preventivo y correctivo de equipos repetidoras (Radio enlaces, alineamiento, certificación).	Número de Mantenimientos de equipo	10%	Documento	1	1	2
6	Copias de seguridad de los sistemas de información (servidores de sistemas, página web, SIAF).	Número de backups diario	12%	Documento	480	480	960
7	Administración, Soporte Sistema Integrado de Administración Financiera, Sistema de Planillas, Sistema de Administración Municipal, Software Inventario Mobiliario Institucional, mantenimiento y soporte al Sistema de Control de Asistencia.	Número de atenciones diarias	12%	Documento	900	900	1800