

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



Presentado por

BACHILLER EDWIN LLASACCE BAUTISTA

**GESTIÓN DE RIESGOS TECNOLÓGICOS EN EL DATA
CENTER DE LA DIRECCIÓN SUB REGIONAL DE
SALUD CHANKA BASADO EN LA ISO 31000,
ANDAHUAYLAS 2022**

Asesor:

ING. EDWING ALCIDES MAQUERA FLORES

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO
DE SISTEMAS**

ANDAHUAYLAS – APURÍMAC – PERÚ

2023



APROBACION DEL ASESOR

Quién suscribe:
ING. EDWING ALCIDES MAQUERA FLORES
por la presente:

CERTIFICA,
Que, el Bachiller en **Ingeniería de Sistemas**, EDWIN LLASACCE BAUTISTA ha culminado satisfactoriamente el informe final de la tesis intitulada: "GESTION DE RIESGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022" para optar el Título Profesional de **Ingeniero de Sistemas**.

Andahuaylas, 13 febrero de 2023

Ing. Edwing Alcides Maquera Flores
Asesor

Bach. Edwin LLasacce Bautista
Tesista



FACULTAD DE INGENIERIA

**ACTA DE SUSTENTACION
DE TESIS**

En la Av. José María Arguedas del Local Académico SL01 (Ccoyahuacho) en el auditorio de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas ubicado en el distrito de San Jerónimo de la Provincia de Andahuaylas, siendo las 11:00 horas del día 03 de marzo del año 2023, se reunieron los docentes: Mg. Enrique Edgardo Condor Tinoco, Mag. Ruben Apaza Apaza, MSc. Richard Carrión Abollaneda, en condición de integrantes del Jurado Evaluador del Informe Final de Tesis intitulado: "GESTIÓN DE RIESGOS TECNOLÓGICOS EN EL DATA CENTER DE LA DIRECCIÓN SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022", cuyo autor es el Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA** y el asesor Ing. Edwin Alcides Maquera Flores, con el propósito de proceder a la sustentación y defensa de dicha tesis.


Luego de la sustentación y defensa de la tesis, el Jurado Evaluador **ACORDÓ: APROBAR** por **UNANIMIDAD** al Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA**, obteniendo la siguiente calificación y mención:

Nota escala vigesimal		Mención
Números	Letras	
13	TRECE	REGULAR

En señal de conformidad, se procedió a la firma de la presente acta en 03 ejemplares.


Mg. Enrique Edgardo Condor Tinoco
Presidente del Jurado Evaluador


Mag. Ruben Apaza Apaza
Primer Miembro del Jurado Evaluador


MSc. Richard Carrión Abollaneda
Segundo Miembro del Jurado Evaluador

ANEXO 31



APROBACIÓN DEL JURADO DICTAMINADOR

LA TESIS: "GESTIÓN DE RIESGOS TECNOLÓGICOS EN EL DATA CENTER DE LA DIRECCIÓN SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022"; para optar el Título Profesional de Ingeniero de Sistemas, ha sido evaluada por el Jurado Dictaminador conformado por:

PRESIDENTE: Mag. Enrique Edgardo Condor Tinoco
PRIMER MIEMBRO: Mag. Rubén Apaza Apaza
SEGUNDO MIEMBRO: MSc. Richard Carrión Abollaneda

Habiendo sido aprobado por UNANIMIDAD, en la ciudad de Andahuaylas el día 03 del mes de marzo de 2023

Andahuaylas, 21 de marzo de 2023.



MAG. ENRIQUE EDGARDO CONDOR TINOCO
PRESIDENTE DEL JURADO DICTAMINADOR



MAG. RUBEN APAZA APAZA
PRIMER MIEMBRO DEL JURADO DICTAMINADOR



MSC. RICHARD CARRION ABOLLANEDA
SEGUNDO MIEMBRO DEL JURADO DICTAMINADOR



INFORME DE ORIGINALIDAD

El que suscribe asesor del trabajo de investigación/tesis, titulada GESTION DE RIESGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022 presentado por Edwin LLasacce Bautista, con DNI 73471099, de la Escuela Profesional de Ingeniería de Sistemas, para optar el grado de título profesional de ingeniero de sistemas.

Informo que el documento ha sido sometido a revisión de originalidad, utilizando el software de control de similitud y detención de plagio Turnitin, conforme al reglamento vigente, verificándose un porcentaje de 14% de similitud.

Por tanto, en mi condición de asesor, firmo el presente informe en señal de conformidad y adjunto el reporte de software firmado.

Andahuaylas, 10 de marzo de 2023

Firma

Ing. Edwing Alcides Maquera Flores

DNI: 00509928

ORCID: 0000-0003-1441-4207

Se adjunta:

1. Reporte firmado, generado por el software.

NOMBRE DEL TRABAJO

**Informe Final ISO 31000 Llasacce Edwin
VF 04 TURNITIN.docx**

RECuento DE PALABRAS

24346 Words

RECuento DE CARACTERES

122770 Characters

RECuento DE PÁGINAS

100 Pages

TAMAÑO DEL ARCHIVO

2.1MB

FECHA DE ENTREGA

Mar 9, 2023 10:34 AM GMT-5

FECHA DEL INFORME

Mar 9, 2023 10:36 AM GMT-5

● **14% de similitud general**

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos:

- 14% Base de datos de Internet
- Base de datos de Crossref
- 1% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossref

● **Excluir del Reporte de Similitud**

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 15 palabras)



● 14% de similitud general

Principales fuentes encontradas en las siguientes bases de datos:

- 14% Base de datos de Internet
- Base de datos de Crossref
- 1% Base de datos de publicaciones
- Base de datos de contenido publicado de Cros

FUENTES PRINCIPALES

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	repositorio.unjbg.edu.pe Internet	7%
2	hdl.handle.net Internet	2%
3	dspace.ucuenca.edu.ec Internet	<1%
4	ri.ues.edu.sv Internet	<1%
5	blog.softexpert.com Internet	<1%
6	rossberg.net Internet	<1%
7	auto-q-consulting.com.mx Internet	<1%
8	1library.co Internet	<1%
9	repositorio.up.edu.pe Internet	<1%

Descripción general de fuentes

10	tesis.usat.edu.pe	Internet	<1%
11	gob.mx	Internet	<1%
12	repositorio.escuelamilitar.edu.pe	Internet	<1%
13	repositorio.uladech.edu.pe	Internet	<1%
14	myslide.es	Internet	<1%
15	repositorio.ug.edu.ec	Internet	<1%
16	amn.org.br	Internet	<1%
17	repositorio.unheval.edu.pe	Internet	<1%
18	es.slideshare.net	Internet	<1%
19	repositorio.sangregorio.edu.ec	Internet	<1%
20	bibing.us.es	Internet	<1%
21	docplayer.es	Internet	<1%





Descripción general de fuentes

22	argentina.gob.ar Internet	<1%
23	sedafop.gob.mx Internet	<1%
24	libres.uncg.edu Internet	<1%
25	storage.googleapis.com Internet	<1%
26	repositorio.unamba.edu.pe Internet	<1%
27	cybertesis.unmsm.edu.pe Internet	<1%
28	frasertechno.com Internet	<1%
29	repositorio.ucv.edu.pe Internet	<1%
30	repositorio.uwiener.edu.pe Internet	<1%
31	tesis.ipn.mx Internet	<1%
32	Pedro Pablo Poveda Orjuela. "Configuración de un modelo conceptual ..." Crossref posted content	<1%
33	bibdigital.epn.edu.ec Internet	<1%

Descripción general de fuentes

34	cdn.gob.pe Internet	<1%
35	gce-lter.marsci.uga.edu Internet	<1%
36	repositorio.utelesup.edu.pe Internet	<1%
37	marna.com.ve Internet	<1%
38	research.ng-london.org.uk Internet	<1%


Bach: Edwin Lasarce Bautista
DNI: 73471099


Ing. Edwing A. Mayuera Flores
DNI: 00504988

Dedicatoria

A Dios, por su perdurable bondad y proveer salud y amor, a mis padres por haberme forjado como la persona que soy y por ser los autores principales de mi vida, sin el apoyo de ellos no hubiese podido concluir con el presente trabajo y al apoyo emocional durante todo el proceso que escribía esta tesis.

Agradecimiento

Agradezco a mis padres que siempre han sido el motor que impulsa mis sueños y proyectos, tú que estuviste a mi lado en los días y noches más duros cuando estudiaba. Siempre has sido uno de mis mejores entrenadores vitales. Orgulloso de haberlos elegido como mis padres y que estén a mi lado en este momento tan importante.

INDICE

Dedicatoria	i
Agradecimiento	ii
Índice Tablas	vi
Índice Figuras	vii
RESUMEN	viii
ABSTRACT	ix
CHUMASQA	x
INTRODUCCION	xi
CAPITULO I: PROBLEMA DE INVESTIGACIÓN	1
1.1. Descripción del problema	1
1.2. Formulación del problema	3
1.2.1 Problema general.....	3
1.2.2 Problemas específicos	3
1.3. Limitaciones	4
1.4. Justificación.....	4
1.5. Objetivos	5
1.5.1 Objetivo general.....	5
1.5.2 Objetivos específicos	5
1.6. Hipótesis.....	6
CAPITULO II: ANTECEDENTES	7
2.1. Antecedentes a nivel internacional	7
2.2. Antecedentes a nivel nacional	10
CAPITULO III: MARCO TEÓRICO	14
3.1. Riesgo	14
3.1.1. Según el tipo de actividad	15
3.2. La gestión del riesgo.....	17
3.3. Vulnerabilidad.....	18
3.4. Consecuencia.....	18
3.5. Amenaza o Peligro	18
3.6. ISO 31000	18
3.6.1. Comunicación y consulta.....	21

3.6.2. Alcance, contexto y criterios.....	22
3.6.3. Definición del alcance	22
3.6.4. Evaluación de riesgos	25
3.6.5. Tratamiento de riesgos.....	36
3.6.6. Elaboración e implementación de planes de tratamiento de riesgos	37
3.6.7. Seguimiento y revisión	39
3.6.8. Grabación y elaboración de informes	40
3.6.9. Data center:.....	42
CAPITULO IV: METODOLÓGICO DE LA INVESTIGACIÓN	44
3.1. Tipo y nivel de investigación	44
3.2. Diseño de la investigación	44
3.3. Población.....	45
3.4. Muestra	45
3.5. Operacionalización de variable.....	46
3.6. Técnicas de instrumentos de acopio de datos	46
3.7. Validación y confiabilidad de instrumento	48
3.8. Análisis de datos	49
3.9. Diagnóstico de la variable gestión de riesgos	49
3.9.1. Establecer contexto.....	49
3.9.2. Evaluación de riesgos	51
3.10. Propuesta para mejorar la gestión de riesgos.....	56
3.10.1. Analizar Riesgos.....	57
3.10.2. Evaluación del Riesgos	62
CAPITULO V: RESULTADOS.....	64
4.1. Análisis descriptivo	64
4.1.1. Gestión de riesgos.....	64
4.1.2. Dimensiones de la gestión de riesgos	65
4.1.2.1. Establecer contexto	65
4.1.2.2. Identificación de riesgos	67
4.1.2.3. Analizar riesgos	68
4.1.2.4. Evaluar riesgos.....	69
CAPITULO VI: DISCUSIÓN	71
CONCLUSIONES.....	74

RECOMENDACIONES	75
REFERENCIAS BIBLIOGRÁFICAS	76
ANEXOS	79

Índice Tablas

Tabla 1: Población de la Dirección Sub Regional de Salud Chanka - Andahuaylas.....	45
Tabla 2: Operacionalización de variables	46
Tabla 3: Criterio de evaluación para la variable: gestión de riesgos	47
Tabla 4: Evaluación del resultado de la variable: gestión del riesgo	47
Tabla 5: Confiabilidad de los instrumentos	49
Tabla 6: Responsabilidades y responsables.....	49
Tabla 7: Establecimiento de contexto	50
Tabla 8: Identificación de activos.....	51
Tabla 9: Listado de eventualidades internas y externas	51
Tabla 10: Relación de activos tangibles e intangibles con respecto a las amenazas.....	52
Tabla 11: Identificación de vulnerabilidades	54
Tabla 12: Relación entre activos, amenazas y vulnerabilidades	55
Tabla 13: Apreciación de los activos	57
Tabla 14: Apreciación de activos del Data Center	58
Tabla 15: Valoración de amenazas	58
Tabla 16: Amenazas y su respectiva valoración	59
Tabla 17: Valoración de vulnerabilidades	59
Tabla 18: Vulnerabilidades y valoración	60
Tabla 19: Valoración de riesgos	61
Tabla 20: Valoración de riesgos	61
Tabla 21: El nivel de riesgo en los activos	63
Tabla 22: Procedimiento para el tratamiento de riesgos	63
Tabla 23: Gestión de riesgos según niveles de Frecuencia y porcentaje.....	64
Tabla 24: Resultados del diagnóstico por aspectos de la variable de gestión del riesgo.	64
Tabla 25: Dimensión establecer contexto de la variable gestión de riesgos	65
Tabla 26: Grado de cumplimiento de la dimensión establecer contexto de la variable gestión de riesgos	66
Tabla 27: Dimensión identificación de riesgos de la variable gestión de riesgos	67
Tabla 28: Grado de cumplimiento de la dimensión identificar riesgo de la variable gestión de riesgos	67
Tabla 29: Dimensión analizar riesgos de la variable gestión de riesgos	68
Tabla 30: Grado de cumplimiento de la dimensión analizar riesgo de la variable gestión de riesgos.....	69
Tabla 31: Dimensión evaluar riesgos de la variable gestión de riesgos	69
Tabla 32: Grado de cumplimiento de la dimensión evaluar riesgo de la variable gestión de riesgos.....	70

Índice Figuras

Figura 1: Riesgo es una Función de la Amenaza por Vulnerabilidad.....	14
Figura 2: Proceso para la gestión de riesgos	20
Figura 3: Fases para elaboración de propuesta	57
Figura 4: Fórmula para cálculo de Coeficiente de Alfa de Cronbach	87

RESUMEN

En la presente tesis tiene como fin la evaluación del data center de la Dirección Sub Regional de Salud Chanka Andahuaylas, basado en los conceptos y recomendaciones para la gestión de riesgos de la norma ISO 31000.

El diseño de la investigación es de tipo descriptivo simple; este diseño busca y recopila información actualizada sobre un escenario predeterminado o, más concretamente, busca información que ayude a tomar una decisión. El cuestionario fue aplicado a los miembros del personal administrativo y validado por tres expertos sirvió como herramienta de medición de la única variable de gestión de riesgos de la Dirección Sub Regional de Salud chanka Andahuaylas.

Los resultados del cuestionario aplicable indican que hay un 60,5% de conformidad con la norma ISO 31000 en el proceso de gestión de riesgos, También demuestra el proceso de gestión y la adhesión a los requisitos por dimensiones: Con el 14,58% del porcentaje total alcanzado, la dimensión establecer contexto, el 24,34% del porcentaje total, dimensión identificar riesgos, con el 12,08% del porcentaje total y el 9,53% del porcentaje total fueron alcanzados por las dimensiones analizar riesgos y evaluar riesgos, lo que indica un grado medio de conformidad con los criterios de la ISO 31000 para este proceso, la institución tiene un nivel medio de conformidad con la Norma ISO 31000.

De forma similar a como se llevó a cabo el trabajo de estudio, se realizó un análisis para demostrar la situación actual del data center de la Dirección Sub Regional de Salud Chanka Andahuaylas, en consecuencia, fue posible categorizar y definir claramente los activos y riesgos actuales para mejorar la evaluación de la gestión de riesgos y proporcionar conclusiones más útiles.

Palabras claves: Data center, gestión de riesgos.

ABSTRACT

The purpose of this thesis is the evaluation of the data center of Direction Sub Regional de Salud Chanka Andahuaylas, based on the ISO 31000 risk management - principles and guidelines.

A basic descriptive research design was used; this sort of design seeks and gathers current data on a predetermined circumstance, i.e., it aims to gather data in order to reach a choice. The instrument used to measure the only risk management variable was a questionnaire validated by three experts, which was applied to the administrative and technical personnel of the Sub Management of Information and Communication Technologies (SGTIC) of the Sub Regional Health Directorate of Andahuaylas.

The results obtained from the questionnaire applied show that there is a percentage of 60.5% of compliance with ISO 31000 on the risk management process, and also demonstrate compliance with the requirements by dimensions: dimension to establish context with 14.58% of the total percentage obtained, dimension to identify risks with 24.34% of the total percentage obtained, dimension to analyze risks with 12.08% of the total percentage obtained and dimension to evaluate risks with 9.53% of the total percentage obtained, demonstrating that this process is at an average level of compliance with ISO 31000 by the institution.

Likewise, in the research work an analysis is made that allowed to show the current state of the Data Center of the Direction Sub Regional de Salud Chanka Andahuaylas, in such a way it was possible to identify in a clear and classified way the existing assets and threats and to be able to carry out the evaluation of the risk management in an optimal way to obtain better results and conclusions.

Key words: Data center, risk management.

CHUMASQA

Kay tesispa munayninqa Dirección SubRegional de Salud Chanka Andahuaylaspa centro de datos nisqapi chaninchanapaqmi, ISO 31000 nisqa kamachikuyman hina - kamachikuykunata hinaspam kamachikuykunata.

Kay imayna ruwanapaq maskay nisqanme descriptivo simple nisqa, kay diseñoqa maskan hinaspam huñun kunan pacha willakuykunata ñawpaqmanta mascanampaq, chaymi maskan willakuykunata tariyta chaynapi tanteananpaq. Chay instrumento nisqawanmi tupukurqa sapallan variable de gestión de riesgo nisqa, chaymi karqa kimsa yachaqkunapa validasqa tapukuynin, chaytam churarqaku Iliq llankaq runakunaman chay Gestión de Tecnologías de Información y Comunicación (SGTIC) nisqapi, Dirección Sub Regional Salud chanka Andahuaylas nisqampi.

Chay tapukuy aplicasqamanta ruwasqakunam qawarichin sapa pachakmanta 60,5% ISO 31000 nisqawan huntasqa kayninta chay proceso de gestión de riesgos nisqapi, chaymantapas, dimensiones nisqaman hina kamachikuykunata huntakuyninmi qawarichikun: dimension establecer contexto nisqawan 14,58% llapan pachakmanta tarisqamanta, dimensión nisqa riesgokunata riqsichinku 24,34% llapan pachakmanta tarisqamanta, dimensión nisqa riesgokunata t'aqwirinku 12,08% llapan pachakmanta tarisqamanta hinallataq dimensión nisqa riesgokunata chaninchanku 9,53% llapan pachakmanta tarisqamanta, chaywanmi qawarichikun kay ruwayqa ISO nisqaman hina pata nisqapi kasqanmanta 31000 kaqlla nisqa institución ruwasqan.

Chaynallataqmi, investigacion llamkaypiqa huk analisis ruwakun, chaymi permitirqa qawachiyta kunan imayna kasqanmanta kay willay wasimanta Dirección Sub Regional de Salud Chanka Andahuaylas nisqapi, chaynapi sutillata riqsiyta hinaspam clasificayta chay activokunata hinaspam tutupakunay nisqakunata hinaspam aswan allin ruwaykunata, tukupaykunata ima tarinapaq, chay riesgokuna kamachin nisqa chaninchayta allinta ruwayta atinankupaq.

Sapaq simikuna:, riesgokuna kamachiy.

INTRODUCCION

A nivel mundial la incorporación de las tecnologías de información y comunicación (TIC) en la administración pública y privada se viene realizando constantemente desde que se constituyeron un elemento imprescindible para el funcionamiento de las organizaciones.

En la actualidad la información se ha convertido en un bien intangible, pero de mucha importancia para la organización, las organizaciones almacenan y concentran su información en los Data Center lugar donde se encuentran los servidores (aplicación, de base de datos, etc.) y partir de esta información almacenada en los Data Center las organizaciones toman decisiones hacia los objetivos trazados dentro de la visión y misión de la organización.

Es entonces que al entender la importancia de la información almacenada es que se hace necesario contar con un plan estratégico de la gestión de riesgos de la información, y esto se realiza a partir de la evaluación de riesgos tecnológicos de la data center a fin de evitar la pérdida de información como activo de la organización.

En el presente trabajo de investigación se propone realizar una evaluación de riesgos del Data Center de la Dirección Sub Regional de Salud Chanka – Andahuaylas, basado en la ISO 31000.

CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1 Descripción del problema

A escala mundial la incorporación de la tecnologías de información y comunicación (TIC) en la administración pública y privada se viene realizando constantemente desde que se constituyeron un elemento imprescindible para el funcionamiento de las organizaciones

Las TIC son cada vez más demandadas por los miembros de la sociedad de la información y el conocimiento. Las organizaciones no son diferentes, ya que producen información de forma regular y necesitan tecnologías de la información para manejarla de forma eficiente con el fin de coordinar sus objetivos con mejoras en sus operaciones y ahorro de costes, Las TIC deben estar en constante comunicación con el exterior, con sus clientes en tiempo real, y deben alcanzar un nivel competitivo para mantener su viabilidad a largo plazo en una sociedad en vías de globalización afirma Reyes Echeagaray (2016).

Las ventajas que hoy en día aportan las tecnologías de información y comunicación en las empresas que tienen implantado son principalmente aquellas que optimizan los procesos y favorecen el crecimiento organizacional.

Por tanto, el impacto de su eficiencia será mayor, es así que las tecnologías son de importancia para el crecimiento de las empresas, sin embargo, estas tecnologías no están libres a riesgos por las que pueden ser afectadas por diferentes amenazas y vulnerabilidades latentes.

La tecnología es un enorme facilitador, pero también conlleva muchos riesgos que pueden influir negativamente. En los tiempos que corren, el riesgo cibernético está en la "cima del pensamiento" en forma de robo de datos, cuentas robadas, archivos borrados y sistemas inutilizados o dañados. Las adquisiciones y fusiones pueden complicar

considerablemente el entorno informático de la organización. El riesgo de tecnología tiene implicaciones estratégicas, financieras, operacionales, regulatorias, y reputacionales.

A nivel nacional las instituciones privadas y públicas como las Direcciones de Salud tiene dentro de su estructura organizacional la unidad de estadística e informática responsable de apoyar la tecnología de la información como parte de su organización funcional. de apoyar las labores administrativas y Servicios de Salud mediante un adecuado servicio informático, soporte informático y distintas funciones propias de la oficina.

Dado que afecta directamente a las decisiones empresariales, la información es uno de los activos más valiosos de una empresa. Por este motivo, una parte importante de la información que poseen las instituciones se guarda en servidores cuyo mantenimiento corre a cargo de las oficinas de informática. el hecho de que la mayoría de ellas carezcan de una gestión suficiente de los peligros que ya existen y que podrían dañar la información. peligros actuales que podrían perjudicar a la organización o tal vez imposibilitar el cumplimiento de sus objetivos.

En la Dirección Sub Regional de Salud Chanka de Andahuaylas cuenta con un departamento de tecnologías de la información como parte de su estructura organizativa, y su propio centro de datos es una de sus instalaciones., en el cual se evidencia la deficiencia de la gestión de riesgos. se observaron las siguientes problemáticas: discontinuidad de mantenimiento de los equipos, además que desde el año 2014(año de creación del data center) se hace uso continuo de los equipos sin haber sido renovados a lo largo de su periodo de funcionamiento, los servidores del Data Center dependen de su sistema de inyección y extracción de aire ya que estos no cuentan con un sistema de aire acondicionado , esto puede generar que los equipos terminen averiados por la concentración de calor que genera los equipos dentro del ambiente del Data Center.

Para la protección de los perímetros físicos, la detección de intentos de entrada y/o la disuasión de intrusos en las instalaciones, la seguridad perimetral comprende la integración de componentes y sistemas, tanto electrónicos como mecánicos en su centro de datos mal denominada data center de la Dirección Sub Regional de Salud Chanka de Andahuaylas - Dirección Sub Regional de Salud Chanka no considera como prioridad la gestión de riesgos.

A medida que las áreas de la sede administrativa de la Dirección Sub Regional de Salud Chanka de - Andahuaylas fueron creciendo vegetativamente no consideró un crecimiento estructurado de TI, esto evidencia que el centro de datos no soportara la incorporación de servicios adicionales necesarios para el mejor desempeño de la organización.

El plan estratégico de tecnología de información considera en el marco estratégico de TI en el cuadro N° 09 anexo 02 como objetivo fortalecer el control interno y la seguridad de la información mediante el establecimiento de políticas en materia de TI, pero en su alineamiento estratégico del cuadro N°10 anexo 03 entre los objetivos TI y PETI no toma como prioridad la gestión de riesgos y ni tampoco en sus portafolios de proyectos de TI.

1.2 Formulación del problema

1.2.1 Problema general

¿Cómo es la gestión de riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basada en la ISO 31000, Andahuaylas-2022?

1.2.2 Problemas específicos

- a) ¿Cómo es el contexto del Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?
- b) ¿Cómo es la identificación de los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?

- c) ¿Cómo es el análisis de los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?
- d) ¿Cómo es la evaluación de los riesgos priorizados para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?

1.3 Limitaciones

La selección de la población se consideró sólo el personal de la Dirección Sub Regional De Salud Chanka – Andahuaylas formado por trabajadores del data center y profesionales administrativos y técnicos con conocimientos de informática.

Las fases de control de riesgos, comunicación y consulta no se tienen en cuenta para la investigación, ya que requerirían más tiempo, dinero, formación del personal y el permiso de la alta dirección.

1.4 Justificación

Las tecnologías de la información y la comunicación desempeñan actualmente un papel importante en las operaciones de las empresas y tienen un impacto directo en la competitividad y la productividad de las organizaciones. Por ello, se consideran recursos estratégicos cruciales para el crecimiento de cualquier empresa. Como cualquier otro recurso, son susceptibles de sufrir diversos peligros que pueden provocar la pérdida de datos, la interrupción del servicio, pérdidas monetarias, daños a la reputación e incluso pérdidas humanas.

Cualquier organización es vulnerable a amenazas como virus, fallos de software, caídas de la red, spyware, troyanos, robo de equipos y spam, por lo que es necesario evaluar estos riesgos y, a continuación, tomar las medidas oportunas para implantar controles que traten de garantizar unos niveles de riesgo aceptables con el fin de proteger la información, que es el principal activo de cualquier organización.

La seguridad es uno de los componentes más cruciales de la informática moderna. La Oficina Nacional de Gobierno Electrónico e informática – ONGEI de la Presidencia del Consejo de Ministros - PCM estable que las instituciones deben de contar con los siguientes documentos de gestión como es el Plan Operativo Informático – POI y el Plan Estratégico de Tecnologías de Información, dichos documentos de gestión establecen las actividades a realizar a mediano y largo plazo, los mismos que se deben de encontrar alineados al Plan Operativo Institucional y al Plan Estratégico Institucional enmarcados dentro de la visión y misión de la organización.

En la Dirección Sub Regional de Salud Chanka, no cuenta con ninguno de los dos documentos de gestión establecidos por la Oficina Nacional de Gobierno Electrónico e Informático – ONGEI como obligatorio por cuanto es necesario realizar una evaluación de riesgo del Data Center a fin de evitar perdida de información que perjudicaría desastrosamente a la organización, para ello se realizará la evaluación de riesgos mediante la norma (ISO 31000, 2018) que fortalecerá la gestión de las tecnologías de información incorporando de nuevos equipos (servidores, seguridad perimetral, sistemas de seguridad y contingencia establecidos en la TIRE) para la implementación de nuevos servicios sobre la plataforma del Data Center.

1.5 Objetivos

1.5.1 Objetivo general

Evaluar la propuesta estratégica basada en ISO 31000 en gestión de riesgos tecnológicos para el data center de la Dirección Sub Regional de Salud Chanka, Andahuaylas 2022”.

1.5.2 Objetivos específicos

- a) Evaluar el contexto del Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.

- b) Identificar los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.
- c) Analizar los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.
- d) Proponer los riesgos priorizados para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.

1.6 Hipótesis

En las investigaciones descriptivas, la hipótesis puede utilizarse ocasionalmente para predecir un punto de datos o un valor en una o más variables que se medirán u observarán (Hernández, Fernández, & Baptista, 2010)

El primer paso de la actividad científica, conocido como investigación descriptiva, permite organizar los hallazgos a partir de observaciones de comportamientos, características, causas, métodos y otras variables de fenómenos y hechos. Ese tipo de investigación no tiene hipótesis explícitas. (Pineda, De Canales, & Alvarado, 1994)

A partir de la información recogida, la investigación descriptiva organiza los rasgos, atributos o características de la realidad observada en relación con el problema investigado. Esto permite recoger los hallazgos observacionales en una exposición relacionada de las características del fenómeno estudiado de acuerdo con criterios que dan 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 cuantitativa la formulación de hipótesis. (Monje, 2011)

Teniendo en cuenta las afirmaciones anteriores, no se elaboró ninguna hipótesis para este estudio porque los hechos examinados nos permitieron cumplir los objetivos planteado del Data Center de la Dirección Sub Regional de Salud Chanka Andahuaylas como aporte del trabajo de investigación, que se encuentra en el Capítulo de desarrollo.

CAPITULO II: ANTECEDENTES

2.1. Antecedentes a nivel internacional

Rivero, Paulino (2017) “Diseño de un Modelo de Administración de Riesgos Aplicado a una Empresa Fabricante de Autopartes en la Ciudad de México” es el título de la tesis del autor. En el caso de estudio de la empresa fabricante de autopartes, donde permite la planeación y previsión de riesgos en la región atendida por las empresas antes mencionadas que demuestran el requerimiento, la compilación tiene como objetivo proponer un diseño para la evaluación y precisión de la gestión de riesgos utilizando diversas herramientas y técnicas. La investigación llega a la conclusión de que 31000 y 31010 son las mejores soluciones para emplear en la gestión de riesgos, ya que ambas son normas universales. Una trata de las recomendaciones generales para la gestión de riesgos, mientras que la otra se centra en los métodos de análisis y evaluación de riesgos. Este estudio está relacionado con un proyecto en curso porque tiene en cuenta la teoría que subyace a cómo se interpretan los riesgos en las empresas y cómo se gestionan esos riesgos de acuerdo con la norma ISO 31000. También proporciona una explicación clara de las seis categorías de técnicas de evaluación de riesgos enumeradas en la norma ISO 31010: 2009. Además, permite elegir los métodos de aplicación y evaluación en función de los requisitos de cada empresa.

(Chillogallo & Zambrano, 2016) en su tesis “Elaboración de un Modelo de Gestión de Riesgos de Tecnologías de Información para la Fiscalía General del Estado”. En esta investigación tiene como propósito que la Procuraduría General de la República debe asegurar que los ciudadanos reciban un servicio adecuado y oportuno, por lo que requiere de un modelo de gestión que garantice la prestación de los servicios técnicos mediante el uso de estándares y metodologías que se ajusten a las realidades institucionales. En este trabajo se construyó un modelo de gestión de riesgos informáticos. Ofrece

herramientas para la toma de decisiones, la eliminación de la discrecionalidad y la formalización de los procesos. Gracias a su utilización, la Dirección de Tecnologías de la Información pudo elaborar planes y estrategias sostenibles de gestión de riesgos.

Gonzales (2017) en su tesis "Gestión del riesgo empresarial en la atención del cliente: En el caso de la empresa de transportes Mi Chaperito, 2016". El objetivo principal de este estudio es evaluar en qué medida las empresas gestionan el riesgo cuando prestan servicios a sus clientes y cuando alcanzan sus objetivos estratégicos. Conclusiones: A la hora de implantar el SGR se debe tener en cuenta una metodología adecuada a las necesidades de las empresas, utilizando las cuatro fases del SGR más pertinentes para las empresas: identificación del riesgo, análisis cuantitativo y cualitativo, respuesta al riesgo, y seguimiento y control sobre la parte estratégica de la organización. Este estudio sirve de manual para el análisis cualitativo y cuantitativo del riesgo que se empleará de acuerdo con las necesidades de la empresa con el objetivo de potenciar la estrategia de la organización.

Acosta & Patiño (2017) El Sistema de Gestión de Seguridad de la Información (SGSI) tiene como objetivo proporcionar una adecuada gestión de la seguridad de la entidad, donde también se tenga en cuenta la gestión del riesgo, según su trabajo de investigación internacional titulado "Diseño del Sistema de Gestión de Seguridad de la Información (S.G.S.I.) para el Centro de Datos de la Personera de Bogotá D.C. bajo las normas NTC ISO-IEC 27001:2013 y NTC- ISO-IEC 27002:2013", si bien la reducción de riesgos en la Personera de Bogotá es el objetivo primordial de este estudio, también se busca establecer un vínculo entre la implementación del SGSI y la identificación de los riesgos, amenazas y vulnerabilidades a los que están expuestos los activos para tratarlos oportunamente y responder con prontitud ante cualquier incidente de seguridad; En conclusión, se establece que existe una relación entre las normas y directrices para el

tratamiento de riesgos y el SGSI, sirviendo las primeras como uno de los pilares para la creación del SGSI institucional, tras la identificación de amenazas e identificación de responsables, entre otros.

Ñañez (2019) en su trabajo de investigación nacional titulado “Modelo de Gestión de Riesgos De TI Basados En La Norma ISO/IEC 27005 Y Metodología Magerit para mejorar la Gestión de Seguridad de la Información en la Universidad Nacional Toribio Rodríguez de Mendoza - Chachapoyas Perú” planteó que al momento de la implementación de un SGSI se consideran actividades y tareas que abarcan según la ISO/IEC 27001 desde la planeación de su alcance hasta los planes de mejora continua, sin embargo el factor crítico a tomar en cuenta es la gestión de riesgos y su relación existente con el SGSI en sí, debido a esto la presente investigación se centró en el desarrollo de la gestión de riesgos de TI para mejorar la gestión de seguridad de la información. Para garantizar la continuidad de los procesos académicos y administrativos vitales de la universidad, esta investigación concluye que la gestión de riesgos informáticos debe estar relacionada con el sistema de seguridad de la información. También sugiere mantener una revisión periódica de las políticas del SGSI para evaluar su cumplimiento por parte del personal encargado de la seguridad y, simultáneamente, la eficacia de los riesgos informáticos relacionados con el SGSI.

Huayllani (2019) en su trabajo de investigación nacional titulado “Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019” planteó que el Ministerio de Salud cuenta con una reciente implementación de un Sistema de Gestión de Seguridad de la Información, así como con un Sistema de Gestión de Riesgos; sin embargo no existía una idea clara de los alcances que dichas implementaciones poseen, esto debido a que no se había realizado una evaluación de como el funcionamiento de uno estaba relacionado o no al funcionamiento del otro. Del mismo modo, el autor señala que otra cuestión que debe resolverse es la posible relación

entre estos dos sistemas para tener una base teórica más completa sobre cómo se comportan individualmente o en conjunto y, en consecuencia, poder gestionar de forma más eficaz y eficiente la información, el recurso más valioso para cualquier entidad pública o privada. Durante la evaluación y el análisis, se determinó que existe una asociación significativa y favorable entre las dos variables consideradas. Asimismo, se aconseja que ambos sistemas se sometan a evaluaciones periódicas con la flexibilidad necesaria para que cada uno de ellos pueda alcanzar sus objetivos.

Jara (2018) en su trabajo de investigación nacional titulado “Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018”, realizado en la Municipalidad Distrital de Carabayllo, se planteó que es necesario contar con información de calidad para la toma de decisiones, así como asegurar la disponibilidad, confidencialidad e integridad de la misma, por lo que el objetivo de la investigación es establecer la correlación existente entre el SGSI y el proceso de gestión de riesgo, como la funcionalidad de ambas permitan salvaguardar los activos de información, por lo que se concluye tras evidencias estadísticas la existencia de una correlación significativa entre ambas variables lo que permite que la gerencia de la Municipalidad defina de manera oportuna los controles para el tratamiento de riesgos según su criticidad.

2.2. Antecedentes a nivel nacional

Ccesa (2017) en su obra académica titulada “Diseño de un sistema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016”, expresa lo siguiente: La base de un sistema de gestión de la seguridad de la información es el análisis y la gestión de riesgos, ya que permite cuantificarlos. En otras palabras, es un indicador de incertidumbre medido por estadísticas. En este proyecto de investigación, la evaluación de riesgos, utilizando

MARGERIT V.3 como técnica de análisis y gestión de riesgos, permitió identificar y evaluar los activos, amenazas y peligros a los que está expuesta la Municipalidad Provincial de Huamanga. La documentación (sobre evaluación de riesgos) exigida por la NTP ISO/IEC 27001:2014 fue posible gracias a la implantación de MARGERIT. Las medidas de seguridad se crearon teniendo en cuenta los riesgos destacados para reducir los riesgos altos y medios (véase el cuadro 4.22).

Dulanto et. Al. (2017). En la tesis se encuentra la propuesta de diseño del cronograma laboral para la gestión del riesgo del Ejército Peruano. El objetivo de este estudio es desarrollar un marco de trabajo ideal, que tenga en cuenta diversos criterios organizativos, como el orden de trabajo, la asignación de roles y funciones, la designación de recursos y otros, para proporcionar los resultados deseados. Conclusiones: Para aplicar eficazmente la gestión de riesgos, es importante tener en cuenta el ámbito de trabajo de la organización, así como su interpretación en relación con su entorno. Esto se debe a que, si no hay una planificación o distribución ordenada de los recursos de la organización, el trabajo será un reto y el SGR no funcionará correctamente. Este trabajo contribuye a la investigación en curso para comprender que la gestión de riesgos puede mejorar los resultados si va acompañada de un entorno laboral ideal en la empresa, lo que significa que debe existir un plan con objetivos, normas y directrices claramente definidos. Además, debe darse prioridad al compromiso de todas las partes implicadas, ya que es crucial para el desarrollo y la aplicación de la gestión de riesgos.

Pinto (2017) La relación entre la administración y los riesgos de la SI en la institución policial sirvió de base para determinar su objetivo. La tesis tenía un diseño sencillo y una estructura transversal y no experimental. Se aplicó el enfoque estadístico correlacional. 117 profesores del centro encuestado constituían la población cuando se considera el grupo completo como muestra. La información interna, la información empresarial y las amenazas a la seguridad mostraban relaciones inversas

estadísticamente significativas y correlaciones algo elevadas entre ellas. Llegó a la conclusión de que se habían mencionado en relación con la gestión de riesgos y la SI, lo que confirmaba que existían paralelismos entre ambas.

Ayala (2017), tuvo como objetivo fijar el efecto de la implementación de la metodología del SGSI para el procedimiento que administra los riesgos. Empleo el método SGSI (denominado ISO 27001), que ayuda a mejorar el proceso de gestión. Consiguió reducir su medida equivalente de 3,72 a 3,09, exhibiendo un 17%, como resultado cuantitativo. Para identificar su disminución, se estableció la nivelación de los peligros más significativos. En este estudio, se constató que el 72% de los controles ausentes disminuyeron y el 76% de los controles presentes aumentaron.

Llontop (2018), su objetivo fue hacer un demo de un modelado que ha permitido hacer un trabajo de administración y prevención de TI, que sirvió para una mejora efectiva para el servicio de riesgos en entidades con ambientes virtualizadas. El enfoque se basó en la teoría de Westerman y en directrices como ISO 17799, ISO 27001 y la metodología MagerIT. Como resultado del procedimiento, se demostró posteriormente la viabilidad de la gestión de riesgos informáticos. Las conclusiones, que adoptaron un enfoque cuantitativo, se apoyaron en muestras estadísticas que se adquirieron en un formato numerado mediante una investigación directa basada en el conocimiento previo y un diseño comparativo descriptivo.

Otoya (2018), en su trabajo de investigación tuvo el objeto establecer el predominio para administrar el riesgo tecnológico para la prevención de los mismos, cuyo punto importante es la identificar el predominio que se gestiona en las amenazas tecnológicas, la misma manera reconocer el impacto potencial de ejecución de riesgos de TI. Se basó la metodología Margerit acoplada a la estandarización de la I.S.O 31000. (Revisada, 2016). (Primera ed.). Nos llevó a la gestión de riesgos desde un punto de análisis claro, una perspectiva bien organizada que nos permitió evaluar los riesgos.

Según el análisis del autor, la gestión de riesgos tecnológicos supera significativamente a otras estrategias de gestión de riesgos para el refuerzo seguro de toda la información, alcanzando un alto nivel con una valoración significativa de 0,035 y una dependencia de esta variable de seguridad del 44%.

CAPITULO III: MARCO TEÓRICO

3.1. Riesgo

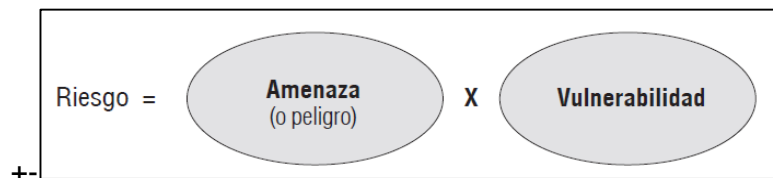
Según Jhuéz (2015) El riesgo es el resultado de la incertidumbre sobre los objetivos, teniendo en cuenta que un resultado es una desviación de las expectativas, ya sea positiva, negativa o ambas; y que los objetivos pueden tener varias facetas (como objetivos financieros, de salud y seguridad y medioambientales) y aplicarse a varios niveles (estratégico, de toda la organización, de proyecto, de producto y de proceso).

El riesgo se describe a nivel empresarial como la incertidumbre que se desarrolla a la hora de alcanzar un propósito. Se refiere esencialmente a condiciones desfavorables, incidentes o acontecimientos que obstaculizan la progresión regular de las operaciones de una empresa y que, en general, tienen ramificaciones financieras para sus responsables.

De acuerdo a Arenas, Lagos, & Hidalgo (2010) La idea de amenaza o riesgo es que se trata de un elemento de riesgo externo que está representado por la posible ocurrencia de una catástrofe natural que podría ocurrir en un lugar determinado y tener una cierta gravedad y duración.

Figura 1:

Riesgo es una Función de la Amenaza por Vulnerabilidad.



Nota: Amenazas ambientales y vulnerabilidad, <https://bit.ly/2G5tqcb>

(Arenas, Lagos, & Hidalgo, Los riesgos naturales en la planificación territorial, 2010) manifiesta que los peligros son inevitables, de ahí que los intentos de reducir el riesgo y las catástrofes deban concentrarse en disminuir la vulnerabilidad de nuestros asentamientos humanos.

3.1.1. Según el tipo de actividad

(Grupo ESGinnova, 2019) Todas las acciones entrañan algún riesgo. Algunos, sin embargo, tienen diversos grados de impacto en la forma en que las empresas desarrollan su actividad. Estos riesgos pueden clasificarse inicialmente de la manera que se indica a continuación:

- **Riesgo sistemático:** según (Grupo ESGinnova, 2019) este término describe los peligros que existen en todo un mercado o sistema económico. Pueden tener efectos de gran alcance en toda la comunidad empresarial, como ocurre, por ejemplo, en las grandes recesiones económicas de las que ninguna empresa puede recuperarse. Además, pueden provocar accidentes, conflictos y catástrofes naturales.
- **Riesgo no sistemático:** según (Grupo ESGinnova, 2019) los peligros asociados a la gestión financiera y operativa de cada empresa. Dicho de otro modo, en este caso falla una sola empresa, no el mercado o el entorno empresarial en su conjunto. La forma de gestionarlos varía en función de la actividad y la situación. Algunos ejemplos son las situaciones de crisis interna o una estrategia de crecimiento que no se llevó a cabo correctamente.
- **Según su naturaleza:** (Grupo ESGinnova, 2019) precisa que los peligros también pueden clasificarse en función de su tipo. En realidad, ésta es la forma más popular de clasificarlos. Es obvio que un riesgo legal o judicial no debe tratarse de forma similar a un riesgo económico. En ese sentido, la clasificación de los riesgos quedaría de la siguiente manera:
- **Riesgos financieros:** (Grupo ESGinnova, 2019) son todas aquellas que tienen que ver con la forma en que las empresas gestionan sus finanzas.

En otras palabras, actividades, transacciones y factores como la financiación, la expansión, la diversificación y la inversión que influyen en las finanzas empresariales. En esta categoría es posible distinguir algunos tipos:

- Riesgo de crédito.
 - Riesgo de tasas de interés.
 - Riesgo de mercado.
 - Riesgo gestión.
 - Riesgo de liquidez.
 - Riesgo de cambio.
- **Riesgos económicos:** (Grupo ESGinnova, 2019) En este contexto, alude a peligros potenciales relacionados con actividades económicas internas o externas. En el primer caso, nos referimos a los daños que puede sufrir una organización como consecuencia de decisiones internas. En el segundo caso, se trata de sucesos de origen externo. Cabe señalar que el riesgo económico difiere del riesgo financiero en que repercute en el valor de la gestión del riesgo en las organizaciones principalmente en términos de ventajas financieras para las empresas, mientras que el riesgo financiero se refiere a todos los recursos de que disponen las organizaciones.
 - **Riesgos ambientales:** (Grupo ESGinnova, 2019) Las empresas son vulnerables a estos riesgos cuando el entorno en el que operan es muy hostil o puede llegar a serlo. Pueden deberse a factores naturales o sociales. En el primer grupo podemos nombrar elementos como la temperatura, la altura, la presión atmosférica, las fallas geológicas, entre

otros. En el segundo, se tratan temas como la violencia y la desigualdad. En cualquier caso, es evidente que estos peligros no dependen de las empresas, por lo que su gestión exige estrategias preventivas más potentes.

- **Riesgos políticos:** (Grupo ESGinnova, 2019) Cada situación política del entorno en el que operan las empresas puede crear este riesgo. Gubernamental, legal y extralegal son las tres categorías. Los casos en los que las instituciones locales han tomado medidas, como un cambio de administración o un giro en la política comercial, entran dentro de la primera categoría. En la segunda, se tienen en cuenta acciones ilegales como el terrorismo, las revoluciones y el sabotaje.
- **Riesgos legales:** (Grupo ESGinnova, 2019) se refiere a las restricciones impuestas por leyes o reglamentos que pueden limitar la capacidad de una empresa para operar en un área determinada. Por ejemplo, algunas naciones tienen normas de mercado restrictivas que prohíben la actividad de determinadas empresas. Estos peligros suelen estar relacionados con los riesgos políticos.

3.2. La gestión del riesgo

Gómez Rivadeneira (2014) La gestión de riesgos puede definirse como el proceso de determinar la susceptibilidad de una población a un riesgo, analizar a continuación los efectos potenciales de ese riesgo sobre esa población, definir el grado de incertidumbre sobre la ocurrencia del suceso crítico que debe evitarse y desarrollar estrategias para disminuir el riesgo, la vulnerabilidad y hacer frente al suceso crítico en caso de que se produzca.

3.3. Vulnerabilidad

El Instituto Colombiano de Normas Técnicas y Certificación (2012) define Vulnerabilidad como las Propiedades intrínsecas de algo que resultan en la susceptibilidad a una fuente de riesgo que puede ocasionar un evento con una consecuencia.

3.4. Consecuencia

Según el Instituto Colombiano de Normas Técnicas y Certificación (2012) define consecuencia como el resultado de un evento que afecta a los objetivos.

3.5. Amenaza o Peligro

Zules Acosta (2013) Una amenaza es cualquier evento o condición física que tiene la potencialidad de causar muertes; lesiones, daño a la propiedad, infraestructura o al medio ambiente, paralización de negocios; en general cualquier tipo de daño o pérdida.

3.6. ISO 31000

Según Casares, Martí, & Lizarzaburu Bolaños (2016) Sirve de manual de aplicación para ayudar a las empresas a crear su propia estrategia de gestión de riesgos. Sin embargo, no es un requisito para la certificación. Las organizaciones pueden comparar sus procedimientos de gestión de riesgos con una norma internacionalmente aceptada para la gestión eficaz de riesgos y el gobierno corporativo mediante la aplicación de la norma ISO 31000. Se emplea con frecuencia para programas de auditoría de riesgos internos o externos.

En el contexto de esta norma de gestión de riesgos, riesgo se define como el efecto de la incertidumbre sobre los objetivos. La noción de riesgo está íntimamente ligada a la de incertidumbre.

El riesgo solo se puede definir de manera significativa en relación con los objetivos porque se relaciona con el efecto de la incertidumbre en los objetivos que tienen una consecuencia potencial, buena o mala, en su éxito.

No puede existir en el vacío. Debe existir en relación con el logro de sus objetivos. La definición más simple de riesgo es “incertidumbre que importa”. El riesgo puede afectar uno o más de sus objetivos, o lo que podría suceder.

En la medida de lo posible, sus objetivos deben ser:

- Específico;
- Mensurable ya sea cualitativa o cuantitativamente; alcanzable dentro de las limitaciones impuestas por el contexto; relevante para los objetivos o el contexto más amplios; y
- Alcanzable dentro de un marco de tiempo establecido.

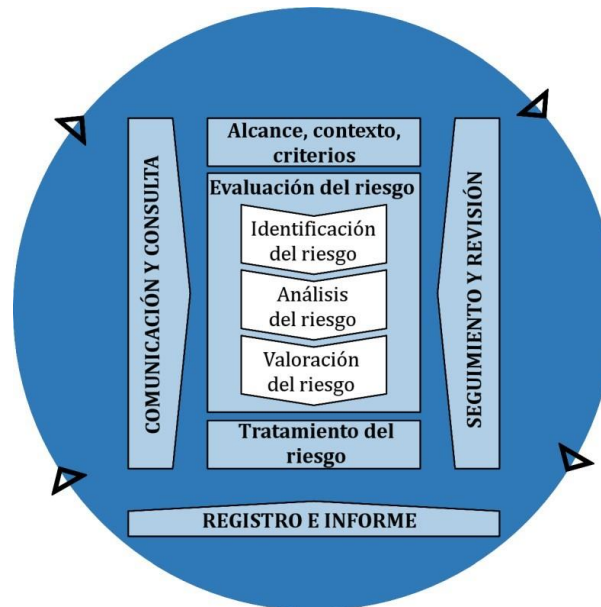
(ISO 31000, 2018) “Las organizaciones de todos los tipos y tamaños enfrentan factores e influencias externas e internas que hacen que sea incierto si lograrán sus objetivos.”

(ISO 31000, 2018) Se utiliza la gestión iterativa del riesgo. Ayuda a las organizaciones a desarrollar estrategias, alcanzar objetivos y tomar decisiones defendibles. Es esencial para dirigir una organización a todos los niveles y es un componente de la gobernanza y el liderazgo.

(ISO 31000, 2018) El proceso de gestión de riesgos es la base de la gestión de riesgos. En el proceso de gestión de riesgos se utilizan sistemáticamente actividades como la consulta y la comunicación, el establecimiento del contexto y la evaluación de riesgos, el tratamiento, el seguimiento, la revisión, el registro y la notificación.

Figura 2:

Proceso para la gestión de riesgos



Nota: Adaptado de norma *ISO 31000:2018*

(ISO 31000, 2018) Su marco de gestión de riesgos garantizará que el proceso de gestión de riesgos se integre en todas las operaciones de la organización, incluida la toma de decisiones, y que los cambios en los contextos interno y externo se registren suficientemente si se planifica y ejecuta correctamente. un grupo de elementos del marco de gestión de riesgos que sirven de marco organizativo y proporcionan disposiciones para crear, poner en práctica, supervisar, revisar y mejorar constantemente la gestión de riesgos en todos los ámbitos.

(ISO 31000, 2018) Sus iniciativas de gestión de riesgos tienen que incorporarse a la estructura, las operaciones y los procedimientos de una organización, así como a los procesos de gestión y toma de decisiones. Puede utilizarse a nivel estratégico, operativo, de programa o de proyecto..

(ISO 31000, 2018) La técnica de gestión de riesgos tiene una amplia gama de aplicaciones. Pero hay que adaptarla a los objetivos y ajustarla a las circunstancias internas y

externas de la aplicación. Durante el proceso de gestión de riesgos, hay que tener en cuenta que el comportamiento humano y la cultura son dinámicos y flexibles. Aunque las fases del proceso de gestión de riesgos se describen a veces como secuenciales, en realidad son iterativas.

3.6.1. Comunicación y consulta

Según la (ISO 31000, 2018) la comunicación y consulta efectivas son esenciales para garantizar que los responsables de identificar y gestionar los riesgos y aquellos con intereses creados entiendan la base sobre la cual se toman las decisiones informadas sobre el riesgo y las razones por las cuales se seleccionan acciones y tratamientos particulares.

Así mismo de la (ISO 31000, 2018) su objetivo de la comunicación y la consulta es ayudar a las partes interesadas a comprender el riesgo, los fundamentos de las decisiones y las causas de la necesidad de determinadas acciones. Proporcionar, intercambiar o adquirir información, así como conversar con las partes interesadas sobre la gestión de riesgos, es un proceso constante e iterativo. Una parte interesada es una persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.

(ISO 31000, 2018) La consulta es un proceso bidireccional de comunicación educada entre una persona u organización y sus interlocutores sobre una cuestión. Es una aportación a la toma de decisiones más que una toma de decisiones en colaboración. El intercambio de información objetiva, oportuna, pertinente, exacta e inteligible debe facilitarse mediante una estrecha cooperación entre las dos partes interesadas, respetando al mismo tiempo la integridad y confidencialidad de la información, así como el derecho de las personas a su intimidad. La información puede estar relacionada con la existencia, el tipo, el

formato, la probabilidad, la importancia, la evaluación, la aceptabilidad y la gestión del riesgo. Cada paso del proceso de gestión de riesgos debe implicar la interacción y el compromiso con las partes interesadas externas e internas pertinentes. La comunicación y la consulta efectivas mejoran la gestión de riesgos porque permiten a todas las partes e interesados comprender los puntos de vista de los demás y, cuando procede, participar activamente en el proceso de toma de decisiones.

3.6.2. Alcance, contexto y criterios

(Ángel Escorial Bonet, 2019) El propósito de establecer el alcance, el contexto y los criterios es personalizar el proceso de gestión de riesgos y permitir una gestión de riesgos eficaz.

3.6.3. Definición del alcance

(Excelencia, 2018) Se debe definir el alcance de sus actividades de gestión de riesgos. Dado que sus actividades de gestión de riesgos pueden aplicarse a diferentes niveles (estratégico, operativo, programa, proyecto u otras actividades), es importante tener claro el alcance que se está considerando, los objetivos relevantes a considerar y su alineación con sus objetivos. Al planificar el enfoque, las consideraciones incluyen:

- Objetivos y decisiones que hay que tomar.
- Resultados esperados de las actividades.
- Tiempo, ubicación, inclusiones y exclusiones específicas.
- Herramientas y técnicas apropiadas de evaluación de riesgos.
- Recursos requeridos, responsabilidades y registros a llevar.
- Relaciones con otros proyectos, procesos y actividades.

3.6.3.1. Contexto externo e interno

Según (Ángel Escorial Bonet, 2019) el contexto externo e interno es el entorno en el que buscas definir y lograr tus objetivos. El contexto de sus actividades de gestión de riesgos debe establecerse a partir de la comprensión del entorno externo e interno en el que opera. Debe reflejar el entorno específico al que se aplicarán las actividades de gestión de riesgos.

(Ángel Escorial Bonet, 2019) Establecer el contexto establece la estructura y los cimientos dentro de los cuales se debe realizar la evaluación de riesgos. Asegura que las razones para llevar a cabo la evaluación de riesgos sean claras. También proporciona el telón de fondo de las circunstancias contra las cuales se pueden identificar y evaluar los riesgos. Así mismo Comprender el contexto es importante porque:

- La gestión de riesgos tiene lugar en el contexto de sus objetivos y actividades.
- Sus factores individuales, de equipo u organizacionales pueden ser una fuente de incertidumbre, riesgo y oportunidad.
- El propósito y el alcance del proceso de gestión de riesgos pueden estar interrelacionados con sus objetivos.

3.6.3.2. Definición de criterios de riesgo

(Borsalli, 2021) Debe especificar la cantidad y el tipo de riesgo que puede tomar o no, en relación con sus objetivos. Los criterios de riesgo son los términos de referencia contra los cuales se determina la importancia de un riesgo. Es un conjunto de criterios para:

- Decidir si se puede aceptar un riesgo o una oportunidad en la búsqueda de sus objetivos.

- A veces denominado apetito de riesgo, especifica una técnica para determinar la magnitud del riesgo, o un parámetro relacionado con el riesgo, junto con un límite más allá del cual el riesgo se vuelve inaceptable.
- La aceptabilidad del riesgo también se puede definir especificando la variación aceptable en las medidas específicas de desempeño vinculadas a los objetivos.
- Se pueden especificar diferentes criterios según el tipo de consecuencia. Por ejemplo, los criterios para aceptar el riesgo financiero pueden diferir de los definidos para el riesgo para la vida humana.

3.6.3.3. Evaluar la importancia de un riesgo.

(Ángel Escorial Bonet, 2019) Una evaluación de la importancia de un riesgo en comparación con otros riesgos a menudo se basa en una estimación de la magnitud del riesgo en comparación con criterios que están directamente relacionados con los umbrales establecidos en torno a sus objetivos.

La comparación con estos criterios puede informarle en qué riesgos debe enfocarse para el tratamiento, en función de su potencial para impulsar los resultados fuera de los umbrales establecidos en torno a los objetivos.

- La magnitud del riesgo rara vez es el único criterio relevante para las decisiones sobre la importancia de un riesgo. Otros factores relevantes pueden incluir la sostenibilidad (por ejemplo, el resultado final triple) y la resiliencia, los criterios éticos y legales, la eficacia de los controles, el impacto máximo si los controles no están presentes o fallan, el momento de las consecuencias, los costos de los controles y las opiniones de las partes interesadas. Decidir entre opciones.

- Una organización se enfrentará a muchas decisiones en las que varios objetivos, a menudo en competencia, se verán potencialmente afectados, y hay posibles resultados adversos y posibles beneficios a considerar. Para tales decisiones, es posible que se deban cumplir varios criterios y que se requieran compensaciones entre objetivos contrapuestos.
- Deben identificarse los criterios relevantes para la decisión. Se debe decidir y contabilizar cómo se ponderarán los criterios o se realizarán las compensaciones.
- Al establecer los criterios, se debe considerar la posibilidad de que los costos y los beneficios puedan diferir para las diferentes partes interesadas.
- Debe decidirse la forma en que se van a tener en cuenta las diferentes formas de incertidumbre.

3.6.4. Evaluación de riesgos

(Ángel Escorial Bonet, 2019) La evaluación de riesgos es el proceso general de:

- Identificación de riesgos: un proceso de encontrar, reconocer y describir riesgos.
- Análisis de riesgo: un proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- Evaluación de riesgos: un proceso de comparación de los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

La evaluación de riesgos debe llevarse a cabo de forma sistemática, iterativa y colaborativa. Esta actividad se basa en el conocimiento y las opiniones de las partes interesadas. Debe utilizar la mejor información disponible, complementada con más indagaciones según sea necesario.

Una evaluación de riesgos exitosa depende de una comunicación y consulta efectivas con las partes interesadas internas y externas.

Involucrar a las partes interesadas durante la actividad de evaluación de riesgos ayudará a:

- Asegurar que los intereses de las partes interesadas sean bien entendidos y considerados.
- Reunir diferentes áreas de especialización para identificar y analizar el riesgo.
- Garantizar que los diferentes puntos de vista e inquietudes se consideren adecuadamente al evaluar los riesgos.
- Asegurar que los riesgos, problemas y oportunidades se identifiquen adecuadamente.

(Ángel Escorial Bonet, 2019) La actividad de evaluación de riesgos proporciona a los responsables de la toma de decisiones y a las partes interesadas una comprensión de las incertidumbres, los riesgos y las oportunidades que podrían afectar el logro de sus objetivos y la adecuación y eficacia de los controles ya establecidos.

(Excelencia, 2018) Los resultados de la actividad de evaluación de riesgos son insumos para los procesos de toma de decisiones y proporcionan la base para las decisiones sobre el enfoque más apropiado que se utilizará para tratar los riesgos o aprovechar la oportunidad.

IEC 31010:2019 Gestión de riesgos — Una norma internacional para la evaluación de riesgos conocida como Métodos de Evaluación de Riesgos ofrece directrices adicionales sobre la selección y el uso de varios enfoques que pueden

utilizarse para mejorar la forma en que se tiene en cuenta la incertidumbre y para comprender mejor las incertidumbres, los riesgos y las oportunidades.

Las técnicas descritas en el estándar proporcionan un medio para mejorar la comprensión de la incertidumbre y sus implicaciones para sus decisiones y acciones. Puede ayudarlo a tomar decisiones cuando existe incertidumbre, para brindar información sobre riesgos particulares y como parte de un proceso para administrar el riesgo.

IEC 31010:2019 clasifica las técnicas según su aplicación principal en la evaluación de riesgos, a saber:

- Obtener puntos de vista de las partes interesadas y expertos (Cláusula B.1);
- Identificar el riesgo;
- Determinar fuentes y causas (o impulsores de riesgo);
- Analizar los controles existentes;
- Comprender las consecuencias y la probabilidad;
- Analizar dependencias e interacciones;
- Proporcionar medidas de riesgo;
- Evaluar la importancia de un riesgo;
- Seleccionar entre opciones; y registro y presentación de informes.

3.6.4.1. Identificación de riesgos

(Copyright, 2022) Encontrar, identificar y describir los riesgos que podrían ayudarlo u obstaculizarle en la consecución de sus objetivos es el objetivo de la identificación de riesgos. La identificación de riesgos permite tener en cuenta explícitamente la incertidumbre. Dependiendo del contexto y el alcance de la

evaluación, cualquier fuente de incertidumbre y sus consecuencias tanto positivas como negativas pueden ser significativas.

(Copyright, 2022) La identificación de riesgos implica la identificación de fuentes de riesgo, eventos, sus causas (impulsores del riesgo) y sus posibles consecuencias. Una fuente de riesgo es un elemento que solo o en combinación tiene el potencial intrínseco de dar lugar a un riesgo. Un evento (o incidente o accidente) es una ocurrencia o cambio de un conjunto particular de circunstancias. Puede ser una o más ocurrencias y puede tener varias causas.

Identificar lo que podría suceder (incertidumbres conocidas) o qué situaciones existen que podrían afectar el logro de los objetivos y resultados.

Esto incluye identificar los riesgos que están asociados con no aprovechar una oportunidad. Este es el riesgo de no hacer nada y potencialmente perder una oportunidad de mejorar el desempeño.

(Excelencia, 2018) define que, al identificar el riesgo, considere lo siguiente:

- ¿Qué podría pasar? ¿Qué podría salir mal? ¿Qué podría impedir el logro de los objetivos? ¿Qué riesgos podrían amenazar los resultados previstos?
- ¿Cómo podría suceder? ¿Es probable que el riesgo ocurra o vuelva a ocurrir? Si es así, ¿qué podría causar que ocurra el evento de riesgo? ¿Dónde podría ocurrir? ¿Es probable que el riesgo ocurra en cualquier lugar, en cualquier entorno o lugar? ¿O es un riesgo que depende de su ubicación, área física o actividad?
- ¿Por qué podría suceder? ¿Qué factores deberían estar presentes para que el evento de riesgo vuelva a ocurrir? Comprender por qué un evento de riesgo puede ocurrir o repetirse.

- ¿Cuál podría ser la consecuencia? Si el evento de riesgo llegara a ocurrir,
- ¿qué consecuencias tendría o podría tener sobre el objetivo y el resultado? ¿Se sentirán las consecuencias a nivel local o afectará a toda la organización?
- ¿Quién influye o puede influir en el resultado? ¿Cuánto está bajo su control o influencia? Asegúrese de que quienes tienen delegaciones, control, anuencia, recursos y presupuestos estén informados. Esto se vuelve más importante cuando se consideran los tratamientos para el riesgo.

Quién es el propietario del riesgo: un propietario del riesgo es una persona o entidad con la responsabilidad y la autoridad para gestionar el riesgo y coordinar actividades con los propietarios de control y tratamiento.

La información pertinente, adecuada y actualizada es importante para identificar los riesgos.

(Ángel Escorial Bonet, 2019) Los siguientes factores, y la relación entre estos factores, deben ser considerados durante la actividad de identificación de riesgos:

- fuentes tangibles e intangibles de riesgo;
- causas (factores de riesgo) y eventos;
- amenazas y oportunidades;
- vulnerabilidades y capacidades;
- cambios en el contexto externo e interno;
- indicadores de
- incertidumbres y riesgos emergentes;

- la naturaleza y el valor de los activos y recursos;
- consecuencias y su impacto en los objetivos;
- limitaciones del conocimiento y confiabilidad de la información; factores relacionados con el tiempo; y
- sesgos, suposiciones y creencias de los involucrados.

(Ángel Escorial Bonet, 2019) Se debe tener en cuenta que puede haber más de un tipo de resultado, lo que puede resultar en una variedad de consecuencias tangibles o intangibles. Una vez que se identifique un riesgo, identifique cualquier control existente, como características de diseño, personas, procesos y sistemas.

3.6.4.2. Análisis de riesgo

(Excelencia, 2018) El objetivo del análisis de riesgos es comprender la naturaleza del riesgo identificado y sus características, incluido, en su caso, el nivel de riesgo. La magnitud de un riesgo o combinación de peligros se describe en términos de combinación de resultados y su probabilidad para determinar el grado de riesgo, también conocido como calificación de riesgo.

(Ángel Escorial Bonet, 2019) Al realizar un análisis de riesgos, se tienen muy en cuenta factores como las incertidumbres, las fuentes, las causas (impulsores del riesgo), las repercusiones, la probabilidad, los sucesos, los escenarios, los controles y su eficacia. En un suceso pueden intervenir muchas causas, efectos y objetivos.

(Copyright, 2022) En función del objetivo del estudio, de la accesibilidad y validez de los datos y de los recursos de que se disponga, el análisis de riesgos puede llevarse a cabo con diversos grados de complejidad y detalle. Dependiendo de la situación y del uso previsto, puede utilizar metodologías de análisis

cualitativas, cuantitativas o una combinación de éstas. El análisis de riesgos debe considerar factores tales como:

- La probabilidad de eventos y consecuencias;
- La naturaleza y magnitud de las consecuencias;
- Complejidad y conectividad;
- Factores relacionados con el tiempo y la volatilidad;
- La eficacia de los controles existentes; y
- Sensibilidad y niveles de confianza.

(Ángel Escorial Bonet, 2019) El riesgo puede estar relacionado con una serie de consecuencias que repercuten en diversos objetivos. Las consecuencias están sujetas a evolución. Por ejemplo, cuanto más tiempo persista un fallo, más efectos perjudiciales pueden derivarse. En ocasiones, las consecuencias pueden derivarse de la exposición a determinados factores de riesgo.

La probabilidad puede referirse a la probabilidad de un evento o la probabilidad de una consecuencia especificada. El parámetro al que se aplica un valor de probabilidad debe establecerse explícitamente. El evento o consecuencia cuya probabilidad se afirma debe definirse con claridad y precisión.

Suele haber muchas interacciones y dependencias entre incertidumbres, riesgos y oportunidades. Por ejemplo, múltiples consecuencias pueden surgir de una sola causa o una consecuencia particular puede tener múltiples causas.

Los controles existentes y su eficacia deben tenerse en cuenta durante esta actividad de análisis de riesgos, ya que el nivel de riesgo dependerá de su adecuación y eficacia.

El control es algo que ya existe y que está reduciendo el riesgo. A menudo se presenta como resultado de una situación o incidente anterior. Hay tres categorías de controles:

- Preventivo: para reducir la probabilidad de que ocurra una situación, incluidas políticas y procedimientos, aprobaciones, autorizaciones, controles policiales y capacitación. Estos controles generalmente se enfocan en las causas o impulsores de un evento de riesgo.
- Detective: para identificar fallas en el entorno de control actual, incluidas revisiones de desempeño, conciliaciones, auditorías e investigaciones.
- Correctivo: para reducir la consecuencia y rectificar una falla después de que se haya descubierto, incluidos los planes de gestión de crisis y continuidad comercial, seguros y planes de recuperación ante desastres. Estos controles generalmente apuntan a las posibles consecuencias de un evento de riesgo.

El riesgo se ve afectado por la efectividad general de cualquier control que esté implementado. Se deben considerar los siguientes aspectos de los controles:

- El mecanismo por el cual los controles están destinados a modificar el riesgo; si los controles están implementados, son capaces de operar según lo previsto y están logrando los resultados esperados;
- Si existen deficiencias en el diseño de los controles o en la forma en que se aplican;
- Si hay lagunas en los controles;
- Si los controles funcionan de forma independiente o si necesitan funcionar colectivamente para ser efectivos;

- Si existen factores, condiciones, vulnerabilidades o circunstancias que pueden reducir o eliminar la efectividad del control, incluidas las fallas de causa común; y
- Si los propios controles introducen riesgos adicionales.

Cualquier suposición hecha durante el análisis de riesgos sobre el efecto real y la confiabilidad de los controles debe validarse cuando sea posible, con énfasis en los controles individuales o combinaciones que se supone que tienen un efecto modificador sustancial. Esto debe considerar la información obtenida a través del monitoreo y revisión de controles de rutina.

En muchos casos estas situaciones o incidentes surgen, no por falta de controles, sino por fallas en los controles existentes.

La verdadera clave para administrar los riesgos de manera efectiva es asegurarse de que sus controles existentes sean efectivos al considerar lo siguiente:

- ¿Cuáles son los controles existentes para un evento de riesgo en particular?
- ¿Son esos controles capaces de manejar o tratar adecuadamente el evento de riesgo para que sea controlado a un nivel que sea tolerable o aceptable?

(Ángel Escorial Bonet, 2019) Su actividad de análisis de riesgos puede verse influenciada por cualquier divergencia de opiniones, sesgos, percepciones de riesgo y juicios.

(ISO 31000, 2018) Influencias adicionales son la calidad de la información utilizada, las suposiciones y exclusiones realizadas, cualquier limitación de las

técnicas y cómo se ejecutan. Estas influencias deben ser consideradas, documentadas y comunicadas a los tomadores de decisiones.

(Excelencia, 2018) La actividad de análisis de riesgos proporciona información para la evaluación de riesgos, para las decisiones sobre si es necesario tratar el riesgo y cómo, y sobre la estrategia y los métodos de tratamiento de riesgo más apropiados. Los resultados brindan información para las decisiones, dónde se toman las decisiones y las opciones involucran diferentes tipos y niveles de riesgo.

3.6.4.3. Evaluación de riesgo

(MBA, 2018) El propósito de la evaluación de riesgos es apoyar las decisiones. La evaluación de riesgos implica comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos para determinar dónde se requieren acciones adicionales. Esta actividad utiliza la comprensión del riesgo obtenida durante el análisis de riesgo para tomar decisiones informadas sobre el riesgo sobre posibles acciones futuras. Las consideraciones éticas, legales, financieras y de otro tipo, incluidas las percepciones de riesgo, también son insumos en el proceso de toma de decisiones. Esto puede conducir a una decisión de:

- No hagas nada más;
- Considerar opciones de tratamiento de riesgos;
- Empezar más análisis para comprender mejor el riesgo;
- Mantener los controles existentes; o
- Reconsiderar los objetivos.

(ISO 31000, 2018) La información de la identificación y el análisis de riesgos se puede utilizar para concluir si el riesgo debe aceptarse y la importancia

comparativa del riesgo en relación con los objetivos y los umbrales de rendimiento. Esto proporciona información sobre las decisiones sobre si un riesgo es aceptable o requiere tratamiento y cualquier prioridad para el tratamiento. A la hora de tomar decisiones, hay que tener en cuenta el contexto general y los efectos reales y percibidos sobre las partes interesadas externas e internas.

(ISO 31000, 2018) Un riesgo puede ser aceptable o tolerable en las siguientes circunstancias:

- No hay tratamiento disponible;
- Los costos del tratamiento son prohibitivos o antieconómicos;
- El nivel de riesgo es bajo y no justifica el uso de recursos para tratar el riesgo;
- Las oportunidades involucradas superan significativamente las amenazas;
- Se ha tomado una decisión consciente de no tratarlo.

Los factores distintos a la magnitud del riesgo que se pueden tener en cuenta al decidir las prioridades incluyen:

- Otras medidas asociadas al riesgo como las consecuencias máximas o esperadas o la eficacia de los controles;
- Las características cualitativas de los hechos o sus posibles consecuencias;
- Las opiniones y percepciones de las partes interesadas;
- El costo y la viabilidad del tratamiento adicional en comparación con la mejora obtenida; o

Interacciones entre riesgos, incluidos los efectos de los tratamientos sobre otros riesgos.

(Excelencia, 2018) El resultado de la evaluación de riesgos debe registrarse, comunicarse y luego validarse en los niveles apropiados de la organización. Una vez que se han evaluado los riesgos y se han decidido los tratamientos, la actividad de evaluación de riesgos se puede repetir para verificar que los tratamientos propuestos no hayan creado riesgos adversos adicionales y que el riesgo restante después del tratamiento esté dentro de su apetito por el riesgo.

3.6.5. Tratamiento de riesgos

(Ángel Escorial Bonet, 2019) El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo. Habiendo completado una evaluación de riesgos, tratar un riesgo implica seleccionar e implementar una o más opciones de tratamiento que cambiarán la probabilidad de ocurrencia, las consecuencias del riesgo o ambas. El tratamiento del riesgo implica un proceso iterativo de:

- formular y seleccionar opciones de tratamiento de riesgos;
- planificar e implementar el tratamiento de riesgos;
- evaluar la efectividad de ese tratamiento;
- decidir si el riesgo restante es aceptable; y
- si no es aceptable, tomar más tratamiento.

(ISO 31000, 2018) Seleccionar la opción de tratamiento de riesgos más adecuada implica equilibrar los beneficios potenciales derivados en relación con el logro de los objetivos frente a los costos, el esfuerzo o las desventajas de la implementación.

(ISO 31000, 2018) Las opciones de tratamiento del riesgo no son necesariamente excluyentes entre sí ni apropiadas en todas las circunstancias. Las opciones para tratar el riesgo pueden incluir una o más de las siguientes:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo;

- Tomar o aumentar el riesgo para aprovechar una oportunidad;
- Eliminar la fuente de riesgo; cambiar la probabilidad;
- Cambiar las consecuencias;
- Compartir el riesgo (por ejemplo, a través de contratos, compra de seguros); o
- Retener el riesgo mediante una decisión informada.

(Ángel Escorial Bonet, 2019) Si el objetivo es reducir la probabilidad del riesgo, es posible que deba ajustar su enfoque. Cambiar con éxito el enfoque dependerá de la identificación de las causas del riesgo y los vínculos causales entre el riesgo y sus consecuencias, los cuales deberían haber sido identificados en la actividad de evaluación de riesgos.

(Copyright, 2022) Si el objetivo es reducir las consecuencias del riesgo, es posible que se requiera un plan de contingencia para responder al riesgo. Esta planificación puede llevarse a cabo en combinación con otros controles. Es decir, incluso si se han tomado medidas para minimizar la probabilidad del riesgo, aún puede valer la pena tener un plan para reducir las consecuencias del riesgo.

(ISO 31000, 2018) Si el objetivo es compartir el riesgo, puede ser útil involucrar a otra parte, como una aseguradora o un contratista. El riesgo se puede compartir contractualmente, de mutuo acuerdo y de diversas formas que satisfagan las necesidades y los requisitos de todas las partes. Dichos arreglos deben registrarse formalmente, ya sea a través de un contrato, un acuerdo o una carta formal. Compartir el riesgo no elimina la obligación y la responsabilidad de gestionar el riesgo. Un riesgo no puede ser transferido a otra parte.

3.6.6. Elaboración e implementación de planes de tratamiento de riesgos

Una vez que se han identificado las opciones de tratamiento y se han seleccionado los tratamientos apropiados para su implementación por parte de los propietarios del

tratamiento, se pueden preparar planes de tratamiento para monitorear el progreso de la implementación.

(Ángel Escorial Bonet, 2019) El propósito de los planes de tratamiento de riesgos es especificar cómo se implementarán las opciones de tratamiento elegidas. Aquí es donde los involucrados entienden los arreglos y se puede monitorear el progreso contra el plan.

(ISO 31000, 2018) El plan de tratamiento debe identificar el orden en que se debe implementar el tratamiento de riesgos. Los planes deben integrarse en los planes y procesos de gestión, en consulta con las partes interesadas apropiadas. La información proporcionada en el plan de tratamiento debe incluir:

- Justificación para la selección de las opciones de tratamiento, incluidos los beneficios esperados que se obtendrán;
- Aquellos que son responsables de aprobar e implementar el plan;
- Acciones propuestas;
- Los recursos necesarios, incluidas las contingencias;
- Medidas de desempeño;
- Restricciones y supuestos;
- Arreglos para la presentación de informes y el seguimiento; y
- Cuándo se espera emprender y completar las acciones.

(ISO 31000, 2018) Al implementar tratamientos, considere las siguientes preguntas:

- ¿Los tratamientos parecen tener el efecto deseado? ¿Detendrán o reducirán lo que se supone que deben detener o reducir?
- ¿Los controles desencadenarán otros riesgos? Por ejemplo, un sistema de rociadores para contrarrestar un incendio puede causar daños por

agua, presentando un riesgo diferente que requiere consideración o gestión (consecuencias no deseadas).

- ¿Los tratamientos son beneficiosos o rentables? ¿El costo de implementar el tratamiento supera el costo atribuido al riesgo que ocurre sin el control establecido? En general, ¿el costo de implementar el tratamiento es razonable para este riesgo?
- Incluso si los controles existentes se califican como "efectivos", puede considerar implementar tratamientos adicionales para fortalecer aún más su efectividad.

(MBA, 2018) Una vez que se implementan los tratamientos, la calificación de riesgo residual generalmente debe ser más baja que la calificación de riesgo original. El nivel de riesgo residual se refiere a la probabilidad y consecuencia de que el riesgo ocurra después de que el riesgo haya sido tratado.

Los riesgos residuales deben documentarse, monitorearse y revisarse. En su caso, los tratamientos adicionales pueden ser prudentes.

Sin embargo, aun cuando se haya tratado un riesgo y se hayan implementado controles, es posible que el riesgo no se elimine o que permanezca alto.

3.6.7. Seguimiento y revisión

(Excelencia, 2018) El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso. Las dos acciones clave:

- Supervisar e identificar el cambio del nivel de desempeño requerido o esperado.
- Revisar la idoneidad, adecuación y eficacia del proceso de gestión de riesgos, riesgos, controles y tratamientos para alcanzar los objetivos

establecidos. Esto incluye determinar si él ha cambiado el entorno operativo y si han surgido nuevos riesgos.

(ISO 31000, 2018) El monitoreo continuo y la revisión periódica del proceso de gestión de riesgos y sus resultados deben ser una parte planificada de sus actividades de gestión de riesgos, con responsabilidades claramente definidas. Como parte del proceso de gestión de riesgos, los riesgos, controles y tratamientos deben monitorearse y revisarse periódicamente para verificar que:

- Las suposiciones sobre las incertidumbres, los riesgos y las oportunidades siguen siendo válidas.
- Se están logrando los resultados y el desempeño esperados. Los resultados de las evaluaciones de riesgo están en línea con la experiencia o las expectativas.
- Las técnicas de evaluación de riesgos se aplican correctamente y funcionan con eficacia.
- Los tratamientos de riesgo son efectivos.

(ISO 31000, 2018) El monitoreo y la revisión deben realizarse a través de sus actividades de gestión de riesgos. Incluye la planificación, la recopilación y el análisis de información, el registro de resultados y el suministro de comentarios. Los resultados del seguimiento y la revisión deben incorporarse en sus actividades de gestión, medición e informes del rendimiento.

3.6.8. Grabación y elaboración de informes

(ISO 31000, 2018) Las actividades de gestión de riesgos y sus resultados deben documentarse e informarse a través de los mecanismos apropiados. El registro y la presentación de informes tienen como objetivo:

- Comunicar las actividades de gestión de riesgos y los resultados en toda la organización;
- Proporcionar información para la toma de decisiones;
- Mejorar las actividades de gestión de riesgos; y
- Ayudar a la interacción con las partes interesadas, incluidos aquellos con responsabilidad y rendición de cuentas para las actividades de gestión de riesgos.

(Ángel Escorial Bonet, 2019) Las decisiones relacionadas con la creación, retención y manejo de información documentada deben considerar, entre otros, su uso, la sensibilidad de la información y el contexto externo e interno. La presentación de informes es una parte integral del gobierno de una organización. Debería mejorar la calidad del diálogo con las partes interesadas y apoyar a los órganos superiores de gestión y supervisión en el cumplimiento de sus responsabilidades. Los factores a considerar para la presentación de informes incluyen, pero no se limitan a:

- las diferentes partes interesadas y sus necesidades y requisitos de información específicos;
- costo, frecuencia y puntualidad de los informes; método de presentación de informes; y
- relevancia de la información para los objetivos y la toma de decisiones.

El propósito de los registros es:

- Comunicar información sobre el riesgo a los responsables de la toma de decisiones y otras partes interesadas, incluidos los reguladores.
- Proporcionar un registro y justificación de la razón de ser de las decisiones tomadas.
- Conservar los resultados de la evaluación para uso y referencia futuros.
- Realice un seguimiento del rendimiento y las tendencias.

- Brindar confianza de que las incertidumbres, los riesgos y las oportunidades se entienden y se gestionan adecuadamente.
- Habilitar la verificación de la evaluación. Proporcionar un registro de auditoría.

3.6.9. Data center:

Según Bautista Díaz (2017) El objetivo de un centro de datos, también conocido como CPD (Centro de Proceso de Datos), es contener todos los equipos técnicos de una empresa garantizando su seguridad y fiabilidad. Un centro de datos posee ciertas cualidades físicas, como refrigeración, protección y redundancia. Todos estos factores garantizan la accesibilidad de los servicios de red. Es un lugar crucial para las empresas, ya que alberga los activos más valiosos de la organización y también sirve como unidad de negocio crucial con un alto valor.

De acuerdo a Tongo Evangelista (2017) clasifica en:

a) Una parte sustancial de la industria de las telecomunicaciones se sirve de centros de datos de Internet, que son instalaciones construidas por empresas para ofrecer tanto servicios de Internet como servicios de datos (alojamiento y hosting) a sus clientes. Centros de datos corporativos: Estas instalaciones están diseñadas para ofrecer servicios de datos a una sola empresa, permitiendo conexiones entre los numerosos servidores internos de la red de una organización e internet. Niveles de redundancia El Uptime Institute (18) realiza esta determinación, que se basa en la disponibilidad y redundancia del centro de datos, tal y como indican sus 4 niveles TIER:

- Infraestructura básica TIER I: Esta infraestructura es utilizada por pequeñas empresas y carece de redundancia en cualquiera de sus partes, lo que la hace vulnerable a cortes de servicio en caso de fallo de un componente.

- Infraestructura de nivel II TIER II con dispositivos redundantes: Esta infraestructura tiene componentes redundantes, normalmente en los aspectos eléctrico y de refrigeración, lo que la hace menos propensa a las interrupciones que el nivel I.
- Infraestructura mantenible concurrente TIER III: Todos los equipos de telecomunicaciones deben tener fuente de alimentación redundante, y dispone de dos canales de alimentación y refrigeración, uno de ellos activo. Esta infraestructura permite la reparación sin afectar al servicio.
- La infraestructura tolerante a fallos consiste en un centro de datos con sistemas separados TIER IV: varios componentes redundantes y canales de distribución continuamente activos.

CAPITULO IV: METODOLOGÍCO DE LA INVESTIGACIÓN

3.1. Tipo y nivel de investigación

El método cuantitativo, según Hernández et al. (2014), se basa en los escritos de Auguste Comte y Émile Durkheim. La investigación cuantitativa sostiene que el conocimiento debe ser objetivo y que éste se produce mediante un proceso deductivo en el que se evalúan hipótesis previamente articuladas utilizando medicación numérica y análisis estadísticos inferenciales. Este método suele estar vinculado al positivismo y a las convenciones y prácticas de las ciencias científicas. Este enfoque basa su investigación en casos “tipo”, con la intención de obtener resultados que permitan hacer generalizaciones (Bryman, 2004).

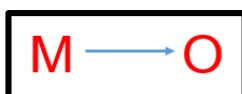
Según (Hernández, Fernández, & Baptista, 2010), la investigación es de carácter fundamental, conduce a la búsqueda de nueva información y áreas de estudio sin objetivos prácticos claros. Se suma a nuestra comprensión de la ciencia y se centra en el descubrimiento de nuevas reglas y conceptos.

El enfoque de la investigación es de tipo cuantitativo de tipo básico y nivel descriptivo.

3.2. Diseño de la investigación

El diseño de investigación 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 considero un diseño no experimental de corte transversal y de carácter de descriptivo simple.



Fuente: Diseño de Investigación Educativa (Atilio G. Olano Martínez, 2010)

M: Representa una muestra representativa del personal de la Dirección Subregional de Salud de Chanka Andahuaylas.

O: Refleja los datos recogidos de la muestra

La investigación, que sólo se centró en la recopilación de datos actuales sobre el tema estudiado, debe tenerse en cuenta debido a los fundamentos antes mencionados (Hernández Sampieri, 2014)

3.3. Población

La población es definida por el autor Arias (2006) como un conjunto finito o infinito de elementos con características homogéneas que serán el foco de una investigación, restringida por el tema y los objetivos del estudio.

Para el presente estudio está comprendida por el personal administrativo que laboran en la Dirección Sub Regional de Salud Chanka.

Tabla 1:

Población de la Dirección Sub Regional de Salud Chanka - Andahuaylas

Descripción	Cantidad
Jefe de oficina	1
Soporte informático	2
Asistente técnico	1
Asistente administrativo	1
Personal Administrativo de DISA	59
Total	64

Fuente: recursos humanos de la dirección sub regional de Salud Chanka andahuaylas

3.4. Muestra

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)

Para la investigación se consideró los trabajadores de área de informática y los usuarios que interactúan con los sistemas de la Dirección Sub Regional de Salud Chanka la cantidad de 64 trabajadores.

3.5. Operacionalización de variable

La variable del estudio de investigación es unico:

Variable Independiente: gestión de riesgos

Operacionalizacion de Variables

Tabla 2:

Operacionalización de variables

DEFINICION CONCEPTUAL	DIMENSIONES	INDICADORES	ITEMS
Gestión de Riesgos Es el proceso de identificar, evaluar y gestionar las fuentes de riesgos a lo largo de la vida del proyecto asumiendo riesgos durante la duración de un proyecto y en apoyo de sus objetivos.	D1: Establecer contexto	Objetivos definidos	1
		Estrategias definidas	2
		Responsables asignados	4
		Procesos identificados	3
		Recursos identificados	5
	D2: Identificar riesgos	Riesgos internos	6, 7, 8
		Riesgos externos	9, 10, 11
		Fuentes de Riesgos	12
		Zonas de Impacto	13
		Controles de Gestión de Riesgo	14
	D3: Analizar Riesgos en el Data Center	Probabilidad de Ocurrencia	15
		Causas	16
		Consecuencias	17
		Nivel de riesgos	18
		Prioridad de riegos	19
	D4: Evaluación de Riesgos del Data Center	Toma de Decisiones	20

Fuente: elaboración propia

3.6. Técnicas de instrumentos de acopio de datos

Según Trespalcios Gutiérrez, Vázquez Casielles, Bello Acebrón et al (2005), las encuestas son herramientas de investigación descriptiva que requieren decidir de antemano qué preguntas se harán, a quién se elegirá como muestra representativa de la población, cuáles serán las respuestas y cómo se recogerá la información.

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.

El cuestionario es la herramienta cuantitativa más popular utilizada para recopilar información, con la intención de poder cuantificar y generalizar la información y estandarizar los

procedimientos de entrevista (Vara, 2012); para la investigación el cuestionario para la variable 01 gestión de riesgo con de 20 ítems con sus respectivas dimensiones.

Tabla 3:

Criterio de evaluación para la variable: gestión de riesgos

CRITERIOS DE EVALUCIÓN	ESCALA
Nunca (N)	1
Casi Nunca (CN)	2
A Veces (AV)	3
Casi Siempre (CS)	4
Siempre (S)	5

Fuente: elaboración propia acopia de acuerdo a escala Likert

De este modo, se evaluó el grado de conformidad de la gestión de riesgos con la normativa (ISO 31000,2018).

Debemos mencionar también que para el presente trabajo de investigación para ubicar el porcentaje de cumplimiento de la norma en los resultados se utilizara la siguiente valoración

Tabla 4:

Evaluación del resultado de la variable: gestión del riesgo

Escala de Valoración	Porcentaje de escala (%)	Descripción
[B] Bajo	00 – 33	cumplimiento inadecuado de la gestión de riesgos (nivel bajo)
[M] Medio	33 – 66	cumplimiento de la gestión de riesgos (nivel medio)
[A] Alto	66 - 100	cumplimiento de la gestión de riesgo (nivel alto)

Nota: niveles de valoración de la variable de gestión de riesgos, (Ángel Escorial Bonet, 2019)

Se diagnosticó que el personal administrativo de la Sub Dirección Regional de Salud Chanka tiene conformidad indirecta con la norma ISO 31000: 2018 en un determinado nivel porcentual.

De acuerdo con la evaluación correspondiente de la tabla, la cual fue evaluada a criterio de los encuestados (personal administrativo de la Dirección Sub Regional de Salud Chanka Andahuaylas y personal administrativo que interactúa con los sistemas de información), las cuatro dimensiones de la variable de gestión de riesgos con respecto a la norma ISO 31000:2018 fueron evaluadas de la siguiente manera: dimensión uno (establecer contexto), dimensión dos (identificar riesgos), dimensión tres (analizar riesgos) y dimensión cuatro (evaluar riesgos).

3.7. Validación y confiabilidad de instrumento

3.7.1. Validación

Como señala Chávez (2001) la validez es una herramienta para medir la eficacia de lo que se espera. Hernández et al. (2010) Defina la validez como la relación en que un instrumento está realmente diseñado para medir la que se quiere medir. Esto nos permite concluir que la efectividad de una herramienta está directamente relacionada con el propósito de la herramienta.

El formulario debe ser apto de efectuar inferencias exitosas entre la unidad de medida utilizada y los hechos o anómalos que surgen de la realidad analizada, como lo muestran Hernández y otros (2003). En este sentido para validar el contenido del cuestionario, se encomendó copias a tres (3) expertos quienes lo revisaron y brindaron opinión favorable.

3.7.2. Confiabilidad del instrumento

Hernández et al. (2010) la confiabilidad de una herramienta de medida está definida por distintas técnicas y se refiere a la medida en que su uso reiterado en el mismo objetivo ocasiona los semejantes resultados.

Además, afirman que existen varios métodos para computar la confiabilidad de un dispositivo de medida. Todos usan ecuaciones que producen coeficientes de confiabilidad

que pueden variar entre 0 (que representa confiabilidad cero) y 1 (que representa confiabilidad máxima). Es decir, cuanto más cerca de cero (0), mayor es el error de medición.

Para precisar la confiabilidad del cuestionario, se utilizó el software SPSS versión 25, mediante el Alfa de Cronbach en cual se encuentra en el anexo 05, obteniéndose los resultados siguientes:

Tabla 5:

Confiabilidad de los instrumentos

Variables	Nº de Ítems	Nº de elementos	Alfa de Cronbach
Gestión de riesgos	20	28	0.81

Fuente: elaboración Propia

3.8. Análisis de datos

Los procedimientos utilizados para realizar el estudio de los datos comprendieron dos etapas, primeramente, se utilizó el método descriptivo, que comprendió la recopilación y tabulación de la información de la investigación, se usó hoja de cálculo y software estadístico, en el cual se ingresó y proceso los datos y se obtuvo toda la información.

3.9. Diagnóstico de la variable gestión de riesgos

3.9.1. Establecer contexto

(Ángel Escorial Bonet, 2019) definición de obligaciones y responsabilidades

Tabla 6:

Responsabilidades y responsables

Áreas	Responsables	Responsabilidad
Jefe de oficina	Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Elaboración de un método de respuesta a incidentes • Cuadro de requerimientos de TI para los productos o servicios
Desarrollador de sistemas	Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Informes de administración de las bases de datos de la institución • Procedimiento 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	Marcial Parcco Gutiérrez Frank Chiquilla Minaya	<ul style="list-style-type: none"> • Informes de la administración de la infraestructura tecnológica de la institución • Reportes de administración y mantenimiento de los equipos informáticos • Reportes de la administración de los sistema de cableado estructurado
Mantenimiento y registro	Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Actualización del software • Implementación de protocolos de suso de equipos y de sistemas informáticos
Seguridades informáticas	Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Plan seguridad informática • Evaluación de los planes de recuperación ataques externos • Monitoreo de la red para prevenir eventualidades

Fuente: Elaboración propia

Servicio prestado por el área de informática a partir del Data center de la DISA Andahuaylas al personal administrativo a nivel de equipos y servicios

Tabla 7:

Establecimiento de contexto

Establecimiento del contexto para el Data Center	
Definición: Gestión de riesgos para el Data Center de la DISA - Andahuaylas.	
Objetivos: Determinar la capacidad de respuesta del personal del área de informática ante un eventualidades	
Responsables	Responsabilidades asignadas
Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Preparación de un plan de respuesta y contingencia • TDR para los requerimientos de TI para bienes y/o servicios. • Informes de administración de las BD de los sistemas de la DISA • Plan de mantenimiento de Activos Tangibles • Plan de mantenimiento de Activos Intangibles. • Informes sobre control de acceso a la sistemas informáticos privilegios. • Reportes de cumplimiento de protocolos informáticos en la DISA
Marcial Parcco Gutiérrez Frank Chiquilla Minaya	<ul style="list-style-type: none"> • Informes de la administración activos tangibles tecnológica de la DISA • Reportes de administración y mantenimiento activos tangibles. • Reportes de la administración del cableado estructurado.
Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Establecer la propuesta de actualización del software y licencias de software. • Informes de la aplicación de protocolos de uso activos tecnológicos
Ing. Pompeyo Rojas Mesco	<ul style="list-style-type: none"> • Plan de seguridad perimetral • Informes de evaluación de los planes de recuperación ante eventualidades externas. • Reportes de monitoreo de la red prevención de eventualidades.
ALCANCE El presente estudio se enfoca sobre el servicio tecnológico, específicamente sobre los activos tangibles e intangibles que se encuentren el Data Center.	

Fuente: Elaboración propia

3.9.2. Evaluación de riesgos

3.9.2.1. Identificación de activos tangibles e intangibles

Tabla 8:

Identificación de activos

Activo	Descripción	TIPO DE ACTIVO			CANTIDAD
		HARDW AREE	SOFTWA RE	REDES	
001	servidor Dell PowerEdge R220	x			1
002	Switch Core	x			1
003	sistemas Operativos de servidores (Windows server 2012, Windows servir 2008)		x		2
004	Gestor de Base de datos (SQL server 2008 R2, Fox Pro, Postgre SQL)		x		2
005	Aplicativo Sistema de Administración Financiera -SIAF		x		1
006	Aplicativo Sistema de Gestión Administrativa - SIGA		x		1
007	Cableado Estructurado				
008	Cámaras de Seguridad	x			5
009	Sistema Eléctrico			x	1
010	Sistema de Alimentación Ininterrumpida (UPS)	x			1

Fuente: Elaboración Propia

3.9.2.2. Identificación de amenazas

Tabla 9:

Listado de eventualidades internas y externas

Código	Amenaza	Origen
AM01	Fuego	Deliberadas, accidental
AM02	Desastre Natural	Natural
AM03	Contaminación	Deliberadas, accidental
AM04	Averías	Deliberadas, accidental
AM05	Corte de Suministro Eléctrico	Deliberadas, Accidental, Programada
AM06	Ambiente no temperado	Deliberadas, Accidental
AM07	Errores del administrador	Accidental y/o desconocimiento
AM08	Abuso de privilegios de acceso	Deliberadas
AM09	Acceso no autorizado	Deliberadas
AM10	Manipulación de activos tangibles	Perdida de equipos
AM11	perdida de activos tangibles	Deliberadas
AM12	Desaprobación de servicio	Deliberadas
AM13	Baja de información	Deliberadas
AM14	Modificación de información	Deliberadas
AM15	Manejo del sistema	Deliberadas

AM16	Envío de información incoherente	Accidental, Deliberado
AM17	Vulnerabilidades de los aplicativos	Accidental
AM18	Indisponibilidad del personal	Accidental, Deliberado

Fuente: Elaboración propia

3.9.2.3. Relación de activos tangibles e intangibles con respecto a las amenazas

Tabla 10:

Relación de activos tangibles e intangibles con respecto a las amenazas

Cód. activo	Cód. amenaza	Cuadro de la amenaza	Naturaleza				Activo		
			NATURAL DELIBERADA	ACCIDENTAL	HARDWARE	SOFTWARE	REDES	ESTRUCTURA	
001	AM01	Fuego	X	X	X				
001	AM02	Desastre natural	X		X				
001	AM03	Contaminación			X	X			
001	AM04	Averías		X	X	X			
001	AM05	Corte de provisión eléctrico			X	X			
001	AM06	Contextos inoportunas de temperatura o humedad			X	X			
001	AM07	Caídas del administrador			X	X			
001	AM08	Iniquidad de libertades de accesos			X	X			
001	AM09	Atajo no acreditado 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	AM01	Fuego		X	X	X			
002	AM02	Desastre natural	X		X				
002	AM03	Contaminación			X	X			
002	AM04	Averías			X	X			
002	AM05	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	AM09	Acceso no autorizado a los recursos del sistema					X		
004	AM04	Averías			X		X		
004	AM07	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	AM04	Averías		x	X
005	AM07	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	AM04	Averías		x	X
006	AM07	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	AM04	Averías		x	X
007	AM07	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	AM01	Fuego	x	x	x
008	AM05	Corte suministro eléctrico		x	x
009	AM06	Condiciones inadecuadas de temperatura o humedad		x	x
010	AM05	Corte suministro eléctrico		x	x
010	AM06	Condiciones inadecuadas de temperatura o humedad		x	x
010	AM07	Errores del administrador		x	x

Nota: Esta tabla muestra una lista de activos junto con una clasificación de amenaza probables basada en el origen de la amenaza adoptado de la norma (ISO 31000, 2018).

Fuente: Elaboración Propia

3.9.2.4. Identificación de vulnerabilidades

Tabla 11:

Identificación de vulnerabilidades

Tipos de activos	Código	Vulnerabilidad	Resultado de la vulnerabilidad
Hardware	VH01	Mantenimiento insuficiente	Pérdida
	VH02	Difidencia a la humedad, el polvo y la suciedad	Pérdida
	VH03	Difidencia a las variaciones de voltaje	Interrupción
	VH04	Difidencia a las variaciones de temperatura	Interrupción
	VH05	Acumulación sin protección	Pérdida
	VH6	Trayecto de un eficiente control de cambios en la configuración	Modificación
	VH7	Separación de esquemas de reemplazo	Pérdida
Software	VS01	Separación o insuficiencia de pruebas de software	Interrupción
	VS02	Software ajeno o inmaduro	Interrupción
	VS03	Configuración incorrecta de cuantificaciones	Modificación
	VS04	Igualdades de contraseñas sin protección	Revelación
	VS05	Gestión incompleta de las contraseñas	Revelación
	VS06	Deserción de "terminación de la sesión" cuando se abandona la estación de trabajo	Modificación
	VS07	reutilización de los medios de almacenamiento sin borrado adecuado	Revelación
	VS08	Interfaz de usuario complicada	Modificación
	VS09	Ausencia de expediente	Modificación
	VS10	Plazos incorrectas	Modificación
	VS11	Deserción de mecanismos de identificación y autenticación.	Revelación
	VS12	Deserción de copias de respaldo	Pérdida
	VS13	Ausencia de protección física	Pérdida
	VS14	Falla en la producción de informes de gestión	Interrupción
	VS15	Retribución errada de los derechos de acceso	Revelación
Redes	VR01	Deserción de pruebas de envío o recepción de mensajes	Pérdida
	VR02	Conexión deficiente de los cables de red.	Interrupción
	VR03	Difidencia a las variaciones de voltaje	Interrupción
	VR04	Gestión incorrecta de la red	Interrupción
	VR05	Conexiones de red pública sin resguardo	Revelación
	VR06	Susceptibilidad a las variaciones de temperatura	Interrupción
Estructura de la organización	VE01	Deserción del personal	Interrupción
	VE02	Deserción protocolo para la autorización de publicación en la web	Revelación

Nota: en esta tabla se muestra las vulnerabilidades que tiene el data center de la Dirección Sub Regional de Salud Chanka Andahuaylas tomada de: (Ángel Escorial Bonet, 2019)

3.9.2.5. Evaluación de activos tangibles e intangibles con respecto a las amenazas y vulnerabilidades

Tabla 12:

Relación entre activos, amenazas y vulnerabilidades

Código activo	Código amenaza	Código vulnerabilidad	Resultados de la vulnerabilidades
001	AM01	VH03	Interrupción
001	AM02	VH02	Pérdida
001	AM03	VH02	Pérdida
001	AM04	VH06	Modificación
001	AM05	VH03	Interrupción
001	AM06	VH04	Interrupción
001	AM07	VH06	Modificación
001	AM08	VH06	Modificación
001	AM09	VH06	Modificación
001	AM10	VH06	Modificación
001	AM12	VH07	Pérdida
002	AM01	VH03	Interrupción
002	AM02	VH02	Pérdida
002	AM03	VH02	Pérdida
002	AM04	VH06	Modificación
002	AM05	VH03	Interrupción
002	AM10	VH06	Modificación
002	AM11	VH05	Pérdida
003	AM12	VH07	Pérdida
003	AM09	VH06	Modificación
004	AM04	VS02	Interrupción
004	AM07	VS03	Modificación
004	AM14	VS12	Pérdida
004	AM15	VS11	Revelación
004	AM16	VS11	Revelación
005	AM04	VS02	Interrupción
005	AM07	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	AM04	VS02	Interrupción
006	AM07	VS03	Modificación
006	AM17	VS11	Modificación
006	AM14	VS12	Pérdida
006	AM18	VS15	Revelación
006	AM19	VS01	Interrupción
006	AM15	VS11	Modificación
007	AM04	VS02	Interrupción
007	AM07	VS03	Modificación
007	AM17	VS11	Modificación
007	AM14	VS12	Pérdida
007	AM18	VS15	Revelación

007	AM19	VS01	Interrupción
007	AM15	VS11	Modificación
008	AM01	VR06	Interrupción
008	AM05	VR03	Revelación
009	AM06	VH03	Interrupción
009	AM05	VR03	Interrupción
010	AM06	VH04	Interrupción
010	AM07	VH06	Modificación
010	AM01	VH03	Interrupción
010	AM02	VH02	Pérdida
010	AM03	VH02	Pérdida
010	AM04	VH06	Modificación

Nota: la tabla muestra la relación de activos, amenazas y vulnerabilidades según las políticas de los responsables del centro de datos de la DISA, que apoyaron en todo momento su clasificación. En relación con las amenazas descubiertas, se indican las vulnerabilidades. evaluación y clasificación evaluación y clasificación. Fuente: Elaboración propia

3.10. Propuesta para mejorar la gestión de riesgos

El objetivo de la propuesta es lograr que el data center de la Dirección Sub Regional de Salud Chanka - Andahuaylas con base en los requisitos de la Norma 31000: 2018, que se refieren a la preservación del logro de los objetivos de la institución, puede identificar y tomar conciencia de sus activos más importantes, además de determinar las amenazas a las que están expuestos, las causas que pueden causar el impacto y las consecuencias que se pueden generar si no se conoce la realidad actual del cargo (Joaquin, 2016).

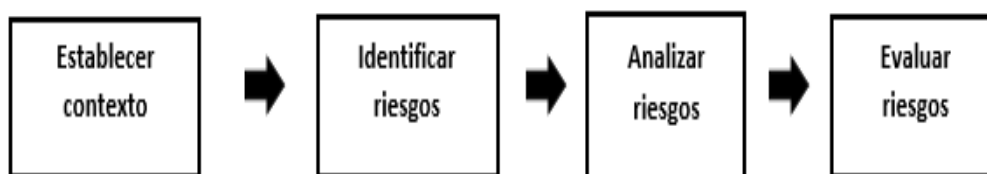
(Joaquin, 2016) las respuestas del cuestionario son cruciales porque demuestran el estado actual de la gestión de riesgos basada en las normas de la ISO 31000: 2018, lo que demuestra indirectamente el grado de cumplimiento de la norma correspondiente.

Con base en la norma ISO 31000, las acciones sugeridas para identificar, analizar y evaluar periódicamente los riesgos son las que proporcionarán el mejor desempeño posible de la gestión de riesgos en el centro de datos de la institución. Además, complementará algunas actividades que faltan (Joaquin, 2016).

(Joaquin, 2016) Las etapas de esta investigación se ajustan a los parámetros fijados para la variable de estudio del proyecto, como son el establecimiento de los antecedentes, la identificación de los riesgos, el análisis de los riesgos y la evaluación de los riesgos.

Figura 3:

Fases para elaboración de propuesta



Nota: La figura 3 muestra las fases de la gestión de riesgos que sirvieron de base para comprender el estado actual del Centro de Datos de la Dirección Sub Regional de Salud Chanka – Andahuaylas tomado (Joaquin, 2016, pág. 59)

La adopción de la siguiente metodología propuesta para llevar a cabo el análisis y la evaluación de sus riesgos basada en la Norma ISO 31000 es una de las propuestas para el centro de datos de la Dirección Sub Regional de Salud Chanka Andahuaylas (Joaquin, 2016).

3.10.1. Analizar Riesgos

(Joaquin, 2016) “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”.

Tabla 13:

Apreciación de los activos

Escala de valoración	Valor	Representación
MB: Muy bajo	0	Activo que no influye para el funcionamiento de la Central Datos
B: Bajo	1	Activo de baja importante para el funcionamiento de la Central Datos
M: Medio	2	Activo importante para el funcionamiento de la Central Datos
A: Alto	3	Activo altamente importante para el funcionamiento de la Central Datos
MA: Muy alto	4	Activo de vital importancia para el correcto funcionamiento de la Central Datos

Nota: la tabla 13 muestra la estaca de valoración de activos de data center de la Oficina de informática de la Dirección Sub Regional Salud Chanka Andahuaylas adoptado de (Joaquin, 2016)

Tabla 14:

Apreciación de activos del Data Center

ACTIVO	REPRESENTACIÓN	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	Sistema de Administración Financiera - SIAF	Muy alto
006	Sistema de Gestión Administrativa - SIGA	Alto
007	Aire acondicionado (no cuenta)	Alto
008	Cableado estructurado	Muy alto
009	Cámaras de video vigilancia	Bajo
010	Red eléctrica	Muy alto
011	Sistemas de alimentación ininterrumpida (UPS)	Alto
012	Administración de data center	Muy alto
013	Responsable de soporte de activos y redes	Muy alto
014	Backup de los sistemas	Muy Alto

Nota: valoración del nivel de importación de los activos del data center tomado de (Joaquin, 2016).

Tabla 15:

Valoración de amenazas

Grado de valoración	Valor	Descripción
B: Baja	0	La amenaza de presencia (muy baja)
M: Medio	1	La amenaza se presenta regular
A: Alto	2	La amenaza es muy continuamente

Fuente: Elaboración propia

(Joaquin, 2016) “Así mismo, se le asigna un criterio de valoración a las amenazas identificadas”.

Tabla 16:

Amenazas y su respectiva valoración

Código	Amenaza	Valoración
AM01	Fuego	0
AM02	Desastre natural	0
AM03	Contaminación	1
AM04	Averías	1
AM05	Corte de suministro eléctrico	1
AM06	Ambiente Temperado	2
AM07	Errores del administrador	0
AM08	Abuso de privilegios de acceso	0
AM09	Acceso no autorizado	0
AM10	Manipulación de los activos tangibles	0
AM11	Pérdida de activos tangibles	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 incoherente	0
AM18	Vulnerabilidades de los aplicativos	1
AM19	Indisponibilidad del personal	0

Nota: esta tabla muestra la valoración de amenazas y su valoración del data center de la Dirección Sub Regional de Salud Chaka Andahuaylas adoptado de (Joaquin, 2016) y (Ángel Escorial Bonet, 2019).

Tabla 17:*Valoración de vulnerabilidades*

Escala de Valoración	Valor	Descripción
B: Bajo	0	Puede postergarse
M: Medio	1	Debe tratarse a la brevedad
A: Alto	2	Debe tratarse inmediatamente

Fuente: Elaboración propia

Tabla 18:*Vulnerabilidades y valoración*

Tipos de activos	Código	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
	VH06	Ausencia de un eficiente control de cambios en la configuración	2
	VH07	Ausencia de esquemas de reemplazo	2
SOFTWARE	VS01	Ausencia de pruebas de software	0
	VS02	Software nuevo o en prueba	0
	VS03	Configuración incorrecta de parámetros	2
	VS04	Tabla 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 autenticación de usuario	2
	VS12	Ausencia de copias Backup	2
	VS13	Ausencia de protección al Data Center	0
	VS14	Falla en la emisión de informes de gestión	0
	VS15	Asignación errada de privilegios de acceso	2
REDES	VR01	Ausencia de pruebas de testeo de red	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 expuestas	2
	VR06	Variaciones de temperatura en los activos	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

Nota: valoración y vulneración de los activos en relación a las vulnerabilidades del data center adoptado de acuerdo a la guía del (Ángel Escorial Bonet, 2019)

3.10.1.1. Nivel de evaluación del riesgo

Tabla 19:

Valoración de riesgos

Escala de Valoración	Valor	Descripción
B: Bajo	0-2	Puede postergarse
M: Medio	3-5	Debe tratarse a la brevedad
A: Alto	6-8	Debe tratarse inmediatamente

Fuente: tomado del informe final de (Joaquin, 2016) y de la guía de la (ISO 31000, 2018).

Según (Joaquin, 2016) “Al haber consolidado la información como los activos, amenazas y vulnerabilidades con sus respectivas valoraciones permitió mostrar el riesgo según los resultados calculados”.

Tabla 20:

Valoración 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	3	AM4	0	VH03	2	8
008	3	AM6	1	VH03	2	8
009	4	AM1	0	VR06	1	5
009	4	AM5	2	VR03	2	8
010	1	AM6	1	VH03	2	4
011	4	AM5	2	VR03	2	8
011	4	AM6	1	VR06	1	6
011	4	AM7	0	VR04	0	4
012	3	AM6	1	VH04	1	5
012	3	AM7	0	VH06	2	5
012	3	AM1	0	VH03	2	5
012	3	AM2	0	VH02	1	4
012	3	AM3	1	VH02	1	5
012	3	AM4	1	VH06	2	6
013	4	AM19	0	VE01	1	5
013	4	AM20	0	VE02	1	5
014	4	AM19	0	VE01	1	5
014	4	AM20	0	VH02	1	5

Nota: la tabla muestra datos sobre recursos, amenazas y vulnerabilidades, fue factible obtener la suma, sumando estos valores asignados para las vulnerabilidades, lo que indica el riesgo basado en los resultados estimados. Los resultados de los cálculos se muestran en la tabla adoptado de la (ISO 31000, 2018).

3.10.2. Evaluación del Riesgos

Con la ayuda del análisis realizado sobre los activos y sus amenazas y vulnerabilidades asociadas, fue posible calificar los riesgos, señalar los activos que suponen un alto riesgo y mostrar los activos de alto riesgo y críticos con la puntuación más alta obtenida en función de su valoración, lo que permitió determinar el estado actual de los activos del Centro de Datos y

cuándo deberían tomarse las medidas adecuadas para hacer frente a estos riesgos (Ángel Escorial Bonet, 2019).

Tabla 21:

El nivel de riesgo en los activos

Nº	CÓDIGO	DETALLE	NIVEL DE RIESGO
1	001	Servidores Dell PowerEdge R220	Alto
	AM05	Corte de suministro eléctrico	
	VH03	Susceptibilidad a las variaciones de voltaje	
2	002	Switch Core	Alto
	AM05	Corte de suministro eléctrico	
	VH03	Susceptibilidad a las variaciones de voltaje	
3	10	Cableado estructurado	Alto
	AM05	Corte de suministro eléctrico	
	VH03	Susceptibilidad a las variaciones de voltaje	

Fuente: Elaboración propia

(Ángel Escorial Bonet, 2019) Se han identificado los principales peligros, por lo que se recomienda que el área de informática y estadística de la DISURCH tome acciones para enfrentarlos. La Norma ISO 31000:2018 sugiere las siguientes alternativas:

Tabla 22:

Procedimiento para el tratamiento de riesgos

Opción	Descripción
1	Evitar el riesgo previendo actividades que da lugar al riesgo
2	Analizar el riesgo para poder aprovechar una oportunidad
3	Eliminar la causa del riesgo
4	Valuar la probabilidad
5	prever las consecuencias
6	Compartir el riesgo (considerando contratos y financiamiento de riesgo)
7	Retener el riesgo mediante una decisión informada

Fuente: adoptado de la Norma (ISO 31000, 2018)

Según la norma (ISO 31000, 2018) elegir la mejor solución de tratamiento de riesgos implica sopesar los beneficios de cumplir los requisitos legales, normativos y de otro tipo frente a los costes y el trabajo de implementación que conlleva.

CAPITULO V: RESULTADOS

4.1. Análisis descriptivo

4.1.1. Gestión de riesgos

Tabla 23:

Gestión de riesgos según niveles de Frecuencia y porcentaje.

		Frecuencia	Porcentaje (%)
Válidos	Bajo	6	9,4
	Regular	57	89,1
	Alto	1	1,6
	Total	64	100,0

Fuente: Elaboración propia

De la tabla 23 podemos deducir que el 57 encuestados consideran que la Dirección Sub Regional de Salud Chanka adopta la gestión de riesgos del data center de manera regular es decir el 89.1%, 9.4% considera que la gestión de riesgos es adoptada de manera baja y 1.6% considera que la implementación de la gestión de riesgos de la ISO 31000 en un nivel alto.

Tabla 24:

Resultados del diagnóstico por aspectos de la variable de gestión del riesgo.

Dimensión	Detalle	Porcentaje del cumplimiento (%)
Dimensión 1	Establecer contexto	14.58
Dimensión 2	Identificar riesgos	24.34
Dimensión 3	Analizar riesgos	12.08
Dimensión 4	Evaluar riesgos	9.53
Porcentaje total		60.5

Fuente: Adoptado de la Norma (ISO 31000, 2018)

La tabla nos indica que el 14.58% establece el contexto sobre el funcionamiento de una data center, es decir tiene los objetivos definidos, establece estrategias de gestión sobre la información con la que cuenta, además cuenta con los responsables en las áreas pertinentes a gestión de información identifica los procesos que dentro de lo que se refiere al funcionamiento de la data center y tiene claro los recursos con los que cuenta la institución.

De igual manera el 24.34% identifica los riesgos internos, los riesgos externos, las probables fuentes de riesgos y zonas de impacto.

El 12.08% analiza los riesgos, es decir analiza los controles de gestión de riesgo, la probabilidad de ocurrencia, las causas que la pueden generar y sus consecuencias.

El 9.53% evalúa el riesgo es decir el nivel de riesgo, la priorización de los riesgos ya toma de decisiones.

Existe un 60.5% de cumplimiento global de la norma ISO 31000 para la gestión de riesgos del Centro de Datos, según el resumen del diagnóstico del grado de cumplimiento por indicadores de la norma ISO 31000 por indicadores en el Centro de Datos perteneciente a la Dirección Sub Regional de Salud de Andahuaylas. Esto indica que existen aspectos deficientes que deben ser mejorados y otros requisitos que deben ser implementados, de acuerdo a la norma, para que el Data center pueda ser más cumplidor.

4.1.2. Dimensiones de la gestión de riesgos

4.1.2.1. Establecer contexto

Tabla 25:

Dimensión establecer contexto de la variable gestión de riesgos

		Frecuencia	Porcentaje (%)
Válidos	Bajo	7	10,9
	Regular	57	89,1
	Total	64	100,0

Fuente: Elaboración propia

De la tabla (25) se demuestra que 57 encuestados que si se considera el establecimiento del contexto de la ISO 31000 es decir un 89.1% considera la adopción en un nivel regular y 10.9% considera la adopción de la ISO 31000 en un nivel bajo.

Tabla 26:

Grado de cumplimiento de la dimensión establecer contexto de la variable gestión de riesgos

Dimensión	Indicador	Detalle	Porcentaje logrado (%)
D01 : ESTABLECER CONTEXTO	I1	Objetivos definidos	2.41
	I2	Estrategias definidas	3.61
	I3	Responsables asignados	2.59
	I4	Procesos identificados	3.36
	I5	Recursos identificados	2.61
Total dimensión			14.58

Fuente: adoptado de la norma (ISO 31000, 2018)

Con un porcentaje total de 14,58% adquirido para el cumplimiento de la norma (ISO 31000, 2018), la tabla 26 ilustra el nivel de cumplimiento de la dimensión a la que se hace referencia al definir el contexto de la gestión de riesgos del centro de datos.

La tabla (26) establece el contexto sobre el funcionamiento de un data center, es decir tiene considerado los objetivos definidos en un 2.41%, como también establece estrategias de gestión de riesgos en un 3.61% sobre la información con la que cuenta, además cuenta con los responsables en las áreas pertinentes 2.59%, tampoco es ajeno la identificación de los procesos en un 3.36% dentro de lo que se refiere al funcionamiento del data center y tiene claro los recursos con los que cuenta 2.61%.

4.1.2.2. Identificación de riesgos

Tabla 27:

Dimensión identificación de riesgos de la variable gestión de riesgos

		Frecuencia	Porcentaje
Válidos	Bajo	56	87,5
	Regular	6	9,4
	Alto	2	3,1
	Total	64	100,0

Fuente: Elaboración propia

De la tabla (27) referido a la dimensión identificación de riesgos establece que 87.5% es decir 56 encuestados consideran que la identificación de los riesgos es muy bajo, 6 encuestados es decir 9.4% considera que la identificación de riesgos es regular y dos que significa el 3.1% refiere que la identificación de riesgos es de nivel alto con respecto a las ISO 31000.

Tabla 28:

Grado de cumplimiento de la dimensión identificar riesgo de la variable gestión de riesgos

Dimensión	Indicador	Detalle	Ítems	alcanzado (%)
D02 : IDENTIFICAR RIESGOS	16	Riesgos internos	16.1 Nivel de control de riesgos internos	3.61
			16.2 Causas de los riesgos internos	2.48
			16.3 Consecuencias de los riesgos internos	3.38
	17	Riesgos externos	17.1 Nivel de control de riesgos externos	2.92
			17.2 Causas de los riesgos externos	3.61
			17.3 Consecuencias de los riesgos externos	2.66

18	Fuentes de riesgo	3.48
19	Zonas de impacto	2.20
Total de la dimensión 02		24.34

Fuente: Elaboración propia en base a los procesos de la norma (ISO 31000, 2018)

De la tabla (28) que refiere al grado de cumplimiento de la dimensión identificar riesgo de la variable gestión de riesgos esta se encuentra en un 24.34% de cumplimiento de la dimensión identificación de riesgos de la gestión de riesgos de la ISO 31000.

Esta dimensión se encuentra definida por 4 indicadores y como también sub indicadores mismo que concluye en los siguiente, sobre el indicador riesgos internos obtuvo un 9.47%, pero aquí debemos mencionar que los sub indicadores el 3.61% refiere al control de riesgos internos, un 2.48% refiere ala las identificación de las causas internas y 3.38% considera considera la consecuencias de los riesgos internos. Ahora con respecto riesgos externos tienen 9.19% del cumplimiento de la dimensión, en donde de los sub indicadores nivel de control de riesgos externos es de 2.92%, el 3.61% corresponde la identificación de las causas de la externos y un 2.66% corresponde a la identificación de las consecuencias de los riegos externos. Ahora con lo que respecta al indicador identificación de las fuentes de riesgo es de un 3.48% y a la identificación de las zonas de impacto es de 2.20%.

4.1.2.3. Analizar riesgos

Tabla 29:

Dimensión analizar riesgos de la variable gestión de riesgos

		Frecuencia	Porcentaje
Válidos	Bajo	14	21,9
	Regular	50	78,1
	Total	64	100,0

Fuente: Elaboración propia

De la tabla veinte nueve (29) de la dimensión analizar riesgos de la variable gestión de riesgos indica que 50 encuestados refieren que el análisis de riesgo es regular en un 78.1% y el 21.9% refiere que el análisis de riesgos es de nivel bajo.

Tabla 30:

Grado de cumplimiento de la dimensión analizar riesgo de la variable gestión de riesgos

Dimensión	Indicador	Detalle	Porcentaje alcanzado (%)
	I10	Controles de gestión de riesgos	3,67
D03 :	I11	Probabilidad de ocurrencia	2,38
ANALIZAR	I12	Causas	3,59
RIESGOS	I13	Consecuencias	2,44
Total de la dimensión 03			12.08

Fuente: Elaboración propia en base a los procesos de la norma (ISO 31000, 2018)

De la tabla treinta (30) que refiere al grado de cumplimiento de la dimensión análisis de riesgo de la variable gestión de riesgos obtuvo un 12.08% de cumplimiento de la dimensión, ahora de los indicadores el 3.36% fue al control de gestión de riesgos, el 2.38% corresponde a la probabilidad de ocurrencia, el 3.59% corresponde a las causas y 2.44% corresponde a las consecuencias de análisis de riesgos.

4.1.2.4. Evaluar riesgos

Tabla 31:

Dimensión evaluar riesgos de la variable gestión de riesgos

		Frecuencia	Porcentaje
Válidos	Bajo	55	85,9
	Regular	9	14,1
	Total	64	100,0

Fuente: Elaboración propia

En la tabla treinta y uno (31) de la dimensión evaluación de riesgos 55 encuestados consideran la evaluación de riesgos en un nivel bajo es decir un 85.9% y 14.1% es decir 9 encuestados considera la evaluación en un nivel regular

Tabla 32:

Grado de cumplimiento de la dimensión evaluar riesgo de la variable gestión de riesgos

Dimensión	Indicador	Detalle	Porcentaje alcanzado (%)
D04 :	I14	Nivel de riesgo	3,66
EVALUAR	I15	Riesgos priorizados	2,27
RIESGOS	I16	Toma de decisiones	3,61
Total de la dimensión 04			9,53

Fuente: Elaboración propia en base a la norma (ISO 31000, 2018).

De la tabla treinta dos (32) que refiere un 9.53% grado de cumplimiento de la dimensión evaluar riesgo de la variable gestión de riesgos, asimismo, el 3.66% refiere a la evaluación del nivel de riesgo ahora la priorización se da en un 2.27% y a la toma de decisiones un 3.61%

CAPITULO VI: DISCUSIÓN

Dado que se tomaron en cuenta las cuatro primeras fases, que son las involucradas en la propuesta, en este trabajo de investigación se obtuvieron los resultados para la gestión de riesgos en el centro de datos de la Dirección Sub Regional de Salud Chanka Andahuaylas de 60.5% de cumplimiento de acuerdo a la norma (ISO 31000, 2018). Sin embargo, existe una diferencia entre los porcentajes obtenidos en ambos trabajos cuando se extraen los porcentajes de las cuatro primeras fases de la propuesta de Chillogallo & Zambrano (2016) en este trabajo, la fase de evaluación de riesgos obtuvo el porcentaje más bajo de 23.86%, lo que indica que no se ha informado adecuadamente a la alta dirección sobre los riesgos priorizados ni sobre cómo proceder en términos de presupuesto, personal y otros recursos. El porcentaje más bajo se obtuvo en la fase de establecimiento del contexto, lo que nos permite saber que no se han definido claramente los responsables ni las responsabilidades que deben cumplirse.

Tres expertos evaluaron el método utilizado para recoger los datos de la variable investigación y aportaron ideas sobre cómo adquirir mejor los resultados y captar con mayor precisión los datos. Para medir el nivel de gestión de riesgos en el Centro de Datos de la Dirección Sub Regional de Salud Chanka Andahuaylas, se determinó que el cuestionario utilizado tuvo un coeficiente Alfa de Cronbach de 0.81. En consecuencia, se considera que la consistencia interna es buena y el instrumento es confiable.

Malpartida (2018) determinó que los riesgos durante la etapa de desarrollo, 35% corresponden a eventualidades técnicas, el 29% corresponden a eventualidades de gestión, el 13% corresponden a los riesgos comerciales y un 23% corresponde a riesgos de factores externos, esto demuestra la correspondencia directa que existe entre la administración de riesgos y que además este estudio demostró que aplicando la gestión de riesgos adecuadamente en la ejecución produjo un 2% de adicional de tiempo y como también de costo.

Por su parte, estos descubrimientos son análogos a los de Taghipour et al. (2016) quienes consiguieron como consecuencia que de los once riesgos descritos se establecieron dos riesgos

a casos técnicos, dos a aspectos profesionales, uno a riesgos meteorológicos y cinco por inseguridades financieras; igualmente, señalaron que la mayor incidencia de riesgos está vinculada a los costos por metas del proyecto, que son los indicadores provocadores en los proyectos.

Quito (2017) concluye que la identificación de los riesgos, se listaron en los siguientes aspectos: el responsable, el área usuaria, coordinación entre las partes y la toma de decisiones y cada una de ellas con su descripción de riesgos considerando el nivel de prioridad y de intervención en el proyecto.

Gianelly (2021) evidencia que, efectuada la tipificación de los riesgos, asevera, de la lista de riesgos identificados, mediante entrevista y juicio de expertos se logró identificar 51 de los 60 riesgos que se presentaron en la etapa inicial del proyecto, como también mediante el uso de la matriz FODA herramienta que permitió analizar y mitigar los eventuales riesgos.

Morales (2018) ultima que en la eficiencia de la administración de riesgos se visualiza que el número de riesgos descritos y subsiguientemente tratados antes del procedimiento o uso de la metodología PMBOK dio como consecuencia: 30 eventualidades reconocidos mínimo y máximo de 43 eventualidades reconocidas, pero posteriormente del procedimiento o con el uso de la metodología PMBOK se posee como efecto un 71 acaecimientos mínimo y un máximo de 90 acaecimientos descritas optimizando la efectividad en el reconocimiento y gestión del riesgo sucedido; demostrando que el uso de la metodología PMBOK ocasiona un ascenso en la efectividad del 35.87% a un 82.73% en la administración del riesgo en el proceso de implementación de software.

Quito (2017) precisa que las estrategias para la respuesta a riesgos se implementan a partir de la identificación de los posibles factores generadores de riesgo, y para ello es necesario contar con un listado con orden de prioridad. Con la finalidad de mitigar eventualidades y darle sostenibilidad al proyecto.

Malpartida (2018) precisa que mediante el análisis e identificación de los riesgos permite elaborar un plan de riesgos que permita contrarrestar las amenazas en la estructura de desglose de trabajo, permitiendo definir y cumplir con los objetivos del proyecto de inversión

Quito (2017) concluye que mediante la implementación del PMBOCK la administración de riesgos en los proyectos, ayudaran considerablemente a evitar y/o reducir adicionales de tiempo y presupuesto en el cumplimiento de los objetivos de los proyectos.

Gudiel (2021) concluye después de analizar los resultados obtenidos a partir de la entrevista a los expertos, permitió afirmar que el manejo de control de riesgos en la ejecución del proyecto no ha sido la más idónea, puesto que no se previó las eventualidades y factores, las que ocasionaron adicionales de tiempo y como también adicionales de presupuesto de lo establecido del expediente técnico.

En la investigación de Morales (2018) mostro que un total el 82% de encuestados posee una comprensión entre elemental y avanzado de la guía del PMBOK y un total del 84% de encuestados tiene comprensión de la administración de riesgos en la actividad de implementación de un aplicativo, lo que supuestamente es positivo y vaticinaría agrado del cliente, no se demuestra en el entorno pero se demuestra en el producto de proyectos a nivel mundial sobre el tema.

Según la pesquisa donde los números nos manifiesta lo inaceptable que estamos en efectividad de casos de éxito en proyectos: pues poco más de 16% de casos de éxito, 31% de proyectos rescindidos y 52% de proyectos sobre dimensionados presupuestalmente. Demostrando la insuficiencia de nosotros los expertos en TIC de plantear y poner en práctica nuevas perspectivas de gestión. (Torres, 2012 citado en Morales, 2018)

CONCLUSIONES

1. En base a la Norma (ISO 31000, 2018), se evaluó la gestión de riesgos para el Centro de Datos de la Dirección Sub Regional de Salud Chanka Andahuaylas, obteniendo un 60.5% de cumplimiento regular, indicando que aún existen algunas áreas por mejorar y actividades adicionales que se deben realizar de acuerdo a la norma, lo que indica que actualmente la gestión de riesgos se cumple en un nivel medio.
2. El Data Center de la Dirección Subregional de Salud de Chanka Andahuaylas se sometió a una evaluación de su marco de gestión de riesgos y obtuvo una calificación de 14.58% de cumplimiento con el requisito establecido por la norma (ISO 31000, 2018), por lo que sus operaciones actuales no cumplen plenamente con la norma.
3. La evaluación de riesgos para el Centro de Datos de la Dirección Subregional de Salud de Chanka Andahuaylas reveló que sólo se cumple con el 24.34% de los requisitos de la norma (ISO 31000, 2018), lo que indica que no se tiene un claro conocimiento de los riesgos que se presentan actualmente, ya sean internos o externos, así como de las fuentes de riesgo y zonas de impacto.
4. Dado que el análisis de riesgos de la Dirección Sub Regional de Salud de Chanka Andahuaylas se logro evaluar y se encontró que cumple en un 12.08% con los requisitos de la Norma (ISO 31000, 2018), se deben establecer controles de gestión de riesgos para una mejor comprensión de las causas, efectos y probabilidad de ocurrencia.
5. Fue factible analizar los riesgos determinados con base en el diagnóstico del cuestionario para la fase de evaluación de riesgos, incluyendo los riesgos priorizados y la toma de decisiones, alcanzando un 9,53% del nivel de cumplimiento de la norma (ISO 31000, 2018). Servidores, Núcleo de Conmutación, Cableado Estructurado, y todos ellos con la amenaza de Cortes de Energía y vulnerabilidad a cambios de voltaje están entre los principales riesgos presentes en el Data Center que influyen en estos activos.

RECOMENDACIONES

1. De acuerdo con los resultados del estudio sobre la evaluación de la gestión de riesgos, se recomienda adherirse a las alineaciones previstas por la norma (ISO 31000, 2018). Para mejorar los procedimientos actuales de cualquier institución, será necesario utilizar todos los requisitos de las normas internacionales y adaptarlos según sea necesario para la mejora continua de la organización (Ramírez Castro & Ortiz Bayona, 2011)
2. Con el fin de optimizar las operaciones de la organización mediante el uso de (ISO 31000, 2018), se recomienda tener en cuenta las debilidades y deficiencias descubiertas para una adecuada gestión de riesgos y reforzarlas con la sugerencia de mejorar la gestión de riesgos.
3. Para empezar a implantar un sistema de seguridad de la información que permita proteger la confidencialidad, integridad y disponibilidad de la información, se recomienda seguir estudiando la evaluación de la gestión de riesgos con respecto a todos los criterios basados en la norma (ISO 31000, 2018), el resultado será un sistema de gestión de riesgos totalmente implantado.
4. Se recomienda mejorar la eficacia de los procesos internos y externos de la organización mediante la mejor gestión de los riesgos identificados, en la que deben participar los responsables a nivel directivo.
5. Se recomienda que la institución emplee la propuesta realizada para la mejora de la gestión de riesgos y la adapte a los nuevos procedimientos o cambios que puedan surgir, de forma que puedan seguir cumpliendo los requisitos de la norma y alcanzar sus objetivos institucionales.

REFERENCIAS BIBLIOGRÁFICAS

- Ángel Escorial Bonet, J. E. (12 de julio de 2019). Guía para la aplicación de UNE-ISO 31000:2018. España.
- Arenas, F., Lagos, M., & Hidalgo, R. (Octubre de 2010). *Los riesgos naturales en la planificación territorial*. Chile: Pontificia Universidad Católica de Chile.
- Arenas, F., Lagos, M., & Hidalgo, R. (10 de 2010). Los riesgos naturales en la planificación Territorial. *Temas de la agenda política*, 14.
- Arias Reyes, Y. L., Díaz Rodríguez, M. L., & Vargas Carvajal, 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 servicio de soporte de tecnología en Colombia*. Bogotá: Universidad Católica de Colombia .
- Bautista Díaz, C. R. (2017). *Decisiones gerenciales para la optimización energética de un data center*. Bogotá: Universidad Militar Nueva Granada.
- Bolaños, I. C.-M. (2016). *Introducción a la Gestión Integral de Riesgos Empresariales, Enfoque ISO 31000*. Lima, Perú: Platinum Editorial S.A.C.
- Borsalli, B. (6 de diciembre de 2021). *8 pasos para la gestión de riesgos de SSO*. Obtenido de <https://blog.softexpert.com/es/gestion-riesgos-ss0/#:~:text=La%20organizaci%C3%B3n%20debe%20especificar%20la,espec%C3%A9ficos%20de%20la%20actividad%20considerada>.
- Casares, I., Martí, S. J., & Lizaraburu Bolaños, E. (2016). *Introducción a la gestión Integral de riesgos empresariales Enfoque: ISO 31000*. Lima: Platinum Editorial S.A.C.
- Cesa Quincho, M. (2017). *Diseño de un sistema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la municipalidad provincial de Huamanga, 2016*. Huamanga: Universidad Nacional de San Cristobal de Huamanga.
- Chillo Gallo, E. J., & Zambrano, V. H. (2016). *Elaboración de un Modelo de Gestión de Riesgos de Tecnologías de Información para la Fiscalía General del Estado*. Quito, Ecuador.
- Copyright, S. C. (2022). *ISO 31000:2018 – Proceso para la Gestión de Riesgo*. Obtenido de <https://spcgroup.com.mx/iso310002018-proceso-para-la-gestion-de-riesgos/#:~:text=El%20prop%C3%B3sito%20de%20la%20identificaci%C3%B3n,An%C3%A1lisis%20del%20riesgo>.
- Excelencia, E. E. (19 de abril de 2018). *Cómo definir el alcance, contexto y criterios de riesgo en ISO 31000*. Obtenido de <https://www.escuelaeuropeaexcelencia.com/2018/04/como-definir-el-alcance-contexto-y-criterios-de-riesgo-en-iso-31000/>

- Gómez Rivadeneira, A. (2014). Marco conceptual y legal sobre la gestión. *Monitor Estratégico*, 1-8.
- Grupo ESGInnova. (12 de agosto de 2019). *ISOTools Excellence*. Obtenido de Plataforma Tecnológica para la Gestión de Excelencia: <https://www.isotools.org/2019/08/12/definicion-del-riesgos-empresariales-y-principales-tipos/>
- Hernández Sampieri, R. (2014). *Metodología de la Investigación*. Mexico: Editores S.A de C.V.
- Hernandez, R., Fernández, C., & Baptista, P. (2010). *Metodología de la Investigación (Quinta Edición)*. Mexico: McGraw-HILL/INTERAMERICANA EDITORES S.A. DE C.V.
- Instituto Colombiano de Normas Técnicas y Certificación. (2012). *Compendio de normas de Gestión del Riesgo*. Colombia: ICONTEC.
- ISO 31000. (2018). ISO 31000:2018 . *Gestión del riesgo - Directrices*. Obtenido de <https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es>
- ISO73. (2009). GUIDE 73 Risk management - Vocabulary.
- Jhuéz , J. (2015). Metodologías para la gestión de riesgo. *J.JHuéz Internacional*, 46.
- Joaquin, M. O. (2016). *Evaluación de la gestión de riesgos para el data center de la municipalidad distrital de ilabaya basada en la ISO 31000*. Universidad Nacional Jorge Basadre, Tacna. Facultad de Ingeniería. Obtenido de http://repositorio.unjbg.edu.pe/bitstream/handle/UNJBG/3186/1406_2018_condori_joaquin_mo_fain_informatica.pdf?sequence=1&isAllowed=y
- MBA, N. F. (12 de junio de 2018). *Cuatro pasos para la evaluación de riesgos según Norma ISO 31000 2018*. Obtenido de Control Interno: <https://www.auditool.org/blog/control-interno/cuatro-pasos-para-la-evaluacion-de-riesgos-segun-norma-iso-31000-2018>
- Monje, C. A. (2011). *Metodología de la Investigación Cuantitativa y Cualitativa*. Neiva.
- Monje, C. A. (2011). *Metodología de la Investigación Cuantitativa y Cualitativa*. Neiva .
- Olano M., A. (2010). *Diseños de Investigación Educativa*. Lima.
- Pineda, E. B., De Canales, F. H., & Alvarado, E. L. (1994). *Metodología de la Investigación - 2da edición*. Washington: Novi Mundi.
- Pineda, E. B., De Canales, F. H., & Alvarado, E. L. (1994). *Metodología de la Investigación - 2da edición*. Washington: Novi Mundi.
- Ramírez Castro, A., & Ortiz Bayona, Z. (2011). *Gestión de Riesgo tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios* . Bogota: Universidad Distrital Francisco José de Caldas.

- Reyes Echeagaray, D. A. (2016). *Tecnologías de Información y comunicación de las Organizaciones*. Mexico: Universidad Nacional Autónoma de México .
- Ríos Villafuerte, J. (2014). *Diseño de un sistema de gestión de seguridad de información para una central privada de información de riesgos*. Lima: Pontificia Universidad Católica del Perú.
- Tongo Evangelista, Y. Y. (2017). *Diagnóstico Situacional del Data Center bajo cumplimiento normativo y de estándar en el Hospital II ESSALUD de Huaraz 2017*. Huaraz: Universidad Católica los Ángeles de Chimbote.
- Trespalacios Gutiérrez, J., Vázquez Casielles, R., & Bello Acebrón, L. (2005). *Investigación de mercados* . Caracas: International Thomson Editores.
- Zules Acosta, F. A. (2013). *Desarrollo de prototipo de Ontología para representación del conocimiento sobre caracterización y monitoreo de amenazas del volcán Tungurahua en el Cantón Baños*. Ecuador: Escuela Politécnica Nacional.

ANEXOS

Anexo 01: Matriz de consistencia

Título: Gestión de Riesgos Tecnológicos en el Data Center de la Dirección Sub Regional de Salud Chanka Basado En La ISO 31000, Andahuaylas 2022			
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 Dirección Sub Regional de Salud Chanka basada en la ISO 31000?	Evaluar la gestión de riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000.	D01: Establecer contexto del Data Center	I1: Objetivos definidos I2: Estrategias definidas I3: Responsables asignados I4 : Procesos identificados I5: Recursos identificados
Problemas específicos:	Objetivos específicos:		
a) ¿Cómo es el contexto del Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?	a) Evaluar el contexto del Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.	D02: Identificar riesgos del Data Center	I1: Riesgos internos I2: Riesgos externos I3: Fuentes de riesgo I4: Zonas de impacto
b) ¿Cómo es la identificación de los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?	b) Evaluar la identificación de los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.	D03: Analizar riesgos en el Data Center	I1: Controles de gestión de riesgo I2: Probabilidad de ocurrencia I3 : Causas I4: Consecuencias
c) ¿Cómo es el análisis de los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?	c) Evaluar el análisis de los riesgos para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.	D04: Evaluar riesgos del Data Center	I1: Riesgos priorizados I2 : Actividades de reducción I3: Toma de decisiones
d) ¿Cómo es la evaluación de los riesgos priorizados para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018?	d) Evaluar los riesgos priorizados para el Data Center de la Dirección Sub Regional de Salud Chanka basado en la ISO 31000: 2018.		
	Población	Técnica - Instrumento	
	El tamaño de la población es el total de personas en la Dirección Sub Regional de Salud Chanka	Encuesta – cuestionario	
	Muestra	Diseño de la investigación	
	Se trabajo con los trabajadores administrativos que interactuan con las TICS (64)	Diseño no experimental – nivel descriptivo - Basico	

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, 2018)

- Instrucciones: Marque con un 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 realizará el análisis de datos respectivo para el presente cuestionario.

1	2	3	4	5
Nunca	Casi Nunca	A veces	Casi siempre	Siempre

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 les 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

Anexo 03:

Datos de la encuesta

N° Encuestados	GESTION DE RIESGOS																			
	PLANIFICACION					IDENTIFICACION								ANALISIS DE RIESGO					EVALUAR RIESGO	
	ITEM 1	ITEM 2	ITEM 3	ITEM 4	ITEM 5	ITEM 6	ITEM 7	ITEM 8	ITEM 9	ITEM 10	ITEM 11	ITEM 12	ITEM 13	ITEM 14	ITEM 15	ITEM 16	ITEM 17	ITEM 18	ITEM 19	ITEM 20
EC - 1	3	3	3	1	1	3	1	3	3	1	1	3	3	3	3	3	3	3	1	1
EC - 2	2	0	3	0	1	3	1	3	3	2	1	3	1	1	1	3	3	3	3	3
EC - 3	3	3	3	3	1	3	1	3	3	1	3	3	3	3	1	3	3	3	1	3
EC - 4	3	1	3	1	1	1	1	1	3	1	1	3	3	3	3	3	1	1	3	3
EC - 5	3	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 6	3	3	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	1	3
EC - 7	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 8	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 9	3	1	3	3	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 10	3	3	3	3	3	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3
EC - 11	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 12	3	3	3	3	3	3	3	3	3	2	3	1	0	1	3	3	3	3	3	3
EC - 13	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 14	2	3	3	3	3	3	3	3	3	2	3	3	3	3	0	3	3	3	3	1
EC - 15	3	3	3	3	3	1	3	1	1	3	3	3	3	3	3	3	3	3	3	3
EC - 16	2	3	3	3	1	1	3	3	3	2	3	0	1	1	0	3	3	3	3	1
EC - 17	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 18	3	3	3	3	5	5	3	3	3	5	3	3	3	5	3	3	3	3	3	3
EC - 19	3	3	3	3	3	3	1	3	2	3	1	3	3	1	3	3	3	3	3	3
EC - 20	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
EC - 21	3	3	3	3	3	3	3	3	2	1	3	3	3	3	3	3	3	3	3	3
EC - 22	2	0	0	0	3	3	3	3	3	2	3	3	3	1	3	3	3	3	0	3
EC - 23	2	3	2	3	2	3	3	3	4	4	3	4	2	4	2	5	3	4	1	4
EC - 24	2	4	4	3	4	3	2	3	4	4	2	2	2	5	3	5	3	4	3	4
EC - 25	2	5	2	3	2	3	2	3	3	5	3	3	2	5	2	5	2	5	2	5
EC - 26	2	3	3	3	3	3	3	3	2	4	3	3	2	5	3	3	2	5	2	5
EC - 27	2	4	2	3	2	3	2	3	3	4	3	4	3	5	3	3	2	4	2	4
EC - 28	2	5	2	4	2	4	2	4	3	5	3	5	2	5	2	5	2	5	2	5
EC - 29	2	4	3	4	3	4	3	4	2	4	2	4	2	4	2	5	2	4	2	5
EC - 30	2	5	2	4	2	5	2	4	3	4	2	3	2	4	2	4	2	4	2	4
EC - 31	2	5	3	5	3	5	3	4	3	4	2	4	1	5	2	4	2	4	2	4
EC - 32	2	5	2	5	2	4	2	4	3	4	2	4	1	5	2	3	2	3	1	4
EC - 33	3	3	2	4	3	4	2	4	3	4	3	4	2	4	2	4	2	4	2	4
EC - 34	2	4	3	5	3	5	3	5	3	5	2	4	2	4	2	3	2	4	2	3
EC - 35	2	4	3	4	3	4	2	4	3	4	3	4	2	4	3	3	3	4	3	3
EC - 36	3	5	2	4	2	4	3	4	3	5	3	5	2	4	2	3	2	4	2	3
EC - 37	2	4	3	4	3	4	2	4	3	4	3	4	2	4	2	4	2	4	2	3
EC - 38	3	5	2	4	3	3	3	3	3	3	3	3	2	3	2	3	2	3	2	3
EC - 39	2	5	2	3	3	4	3	3	3	5	3	4	2	4	2	4	2	4	2	4

EC - 40	2	5	3	4	3	4	3	4	3	4	3	4	2	4	3	3	2	4	3	4
EC - 41	3	4	2	4	2	4	3	4	3	5	3	5	2	3	2	4	2	4	2	4
EC - 42	2	5	3	4	3	4	3	4	3	5	3	5	2	3	3	4	3	4	3	4
EC - 43	2	4	3	4	3	4	2	5	3	5	3	5	2	4	2	4	2	4	2	4
EC - 44	3	4	3	3	3	5	2	4	3	4	3	4	2	4	3	4	2	5	3	5
EC - 45	2	5	3	4	2	4	2	4	3	5	3	5	2	4	2	4	2	4	2	4
EC - 46	3	4	2	4	3	4	2	4	3	4	3	4	2	4	2	4	2	4	2	4
EC - 47	2	5	2	4	2	4	2	4	3	4	3	4	3	4	2	4	2	4	2	4
EC - 48	2	3	3	3	3	4	1	3	3	4	3	4	3	4	3	4	2	4	2	4
EC - 49	2	5	2	4	3	5	2	3	3	4	3	4	2	4	2	4	2	4	3	5
EC - 50	2	5	3	4	3	8	5	4	3	5	3	4	2	4	3	4	3	4	3	5
EC - 51	3	3	2	4	3	3	3	3	3	4	2	4	2	4	2	4	3	4	2	4
EC - 52	2	2	2	2	2	5	2	2	2	2	2	2	2	2	2	2	2	2	2	2
EC - 53	2	3	2	3	2	3	3	3	4	4	3	4	2	4	2	5	3	4	1	4
EC - 54	2	4	4	3	4	3	2	3	4	4	2	2	2	5	3	5	3	4	3	4
EC - 55	2	5	2	3	2	3	2	3	3	5	3	3	2	5	2	5	2	5	2	5
EC - 56	2	3	3	3	3	3	3	3	2	4	3	3	2	5	3	3	2	5	2	5
EC - 57	2	4	2	3	2	3	2	3	3	4	3	4	3	5	3	3	2	4	2	4
EC - 58	2	5	2	4	2	4	2	4	3	5	3	5	2	5	2	5	2	5	2	5
EC - 59	2	4	3	4	3	4	3	4	2	4	2	4	2	4	2	5	2	4	2	5
EC - 60	2	5	2	4	2	5	2	4	3	4	2	3	2	4	2	4	2	4	2	4
EC - 61	2	5	3	5	3	5	3	4	3	4	2	4	1	5	2	4	2	4	2	4
EC - 62	2	5	2	5	2	4	2	4	3	4	2	4	1	5	2	3	2	3	1	4
EC - 63	3	3	2	4	3	4	2	4	3	4	3	4	2	4	2	4	2	4	2	4
EC - 64	2	4	3	5	3	5	3	5	3	5	2	4	2	4	2	3	2	4	2	3

Anexo 05:

Confiabilidad del instrumento

Datos para la prueba piloto

N° Encuestados	GESTION DE RIESGOS																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	3	3	3	1	1	3	1	3	3	1	1	3	3	3	3	3	3	3	1	1
2	2	0	3	0	1	3	1	3	3	2	1	3	1	1	1	3	3	3	3	3
3	3	3	3	3	1	3	1	3	3	1	3	3	3	3	1	3	3	3	1	3
4	3	1	3	1	1	1	1	1	3	1	1	3	3	3	3	3	1	1	3	3
5	3	1	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
6	3	3	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3	3	1	3
7	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
8	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
9	3	1	3	3	1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
10	3	3	3	3	3	3	3	3	3	3	3	3	1	3	3	3	3	3	3	3
11	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
12	3	3	3	3	3	3	3	3	3	2	3	1	0	1	3	3	3	3	3	3
13	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
14	2	3	3	3	3	3	3	3	3	2	3	3	3	3	0	3	3	3	3	1
15	3	3	3	3	3	1	3	1	1	3	3	3	3	3	3	3	3	3	3	3
16	2	3	3	3	1	1	3	3	3	2	3	0	1	1	0	3	3	3	3	1
17	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
18	3	3	3	3	5	5	3	3	3	5	3	3	3	5	3	3	3	3	3	3
19	3	3	3	3	3	3	1	3	2	3	1	3	3	1	3	3	3	3	3	3
20	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
21	3	3	3	3	3	3	3	3	2	1	3	3	3	3	3	3	3	3	3	3
22	2	0	0	0	3	3	3	3	3	2	3	3	3	1	3	3	3	3	0	3
S.C.C	62	54	61	56	56	62	56	62	62	53	58	61	57	58	56	66	64	64	57	60
P.M.A	2.82	2.45	2.77	2.55	2.55	2.82	2.55	2.82	2.82	2.41	2.64	2.77	2.59	2.64	2.55	3	2.91	2.91	2.59	2.73
D.S.T.	0.39	1.06	0.75	1.01	1.06	0.85	0.86	0.59	0.50	1.01	0.79	0.75	0.91	1.00	1.01	0.00	0.43	0.43	0.91	0.70
Varianza	0.16	1.12	0.56	1.02	1.12	0.73	0.74	0.35	0.25	1.02	0.62	0.56	0.82	1.00	1.02	0.00	0.18	0.18	0.82	0.49

Figura 4:

Fórmula para cálculo de Coeficiente de Alfa de Cronbach

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

Fuente: Elaboración propia

Dónde: K = número de ítems
 S_i² = Sumatoria de varianzas independientes
 S_t² = Varianza total

Resultado de confiabilidad del cuestionario

Alfa de CRONBACH	Número de elementos
0.81	22

Fuente: adoptado de (Hernandez, Fernández, & Baptista, 2010)

Anexo 06:

Validación de instrumento

CONSTANCIA DE VALIDACIÓN DE INSTRUMENTO

Yo, Roussevel Anderson Ticana Ortiz, con Documento Nacional de Identidad N° 73143778, de profesión Ingeniero de Sistemas, grado académico Ingeniero de Sistemas, con código de colegiatura 298580, labor que ejerzo actualmente como Resp. de Estadística Farmacia en la Red de Salud Abancay - Gobierno Regional Apurímac

Por medio de la presente hago constar que he revisado con fines de Validación el Instrumento denominado **Encuesta de aplicación**, cuyo propósito es medir la **Variable Gestión de Riesgo**, a los efectos de su aplicación a los colaboradores de la **Dirección Sub Regional de Salud Chanka Andahuaylas**.

Luego de hacer las observaciones pertinentes a los ítems, concluyo en las siguientes apreciaciones.

Observaciones (precisar si hay suficiencia): Demuestra calidad de redacción, amplitud del contenido a evaluar, congruencia en los indicadores y coherencia en los indicadores.

Opinión de aplicabilidad:

Aplicable

Aplicable después de corregir

No aplicable

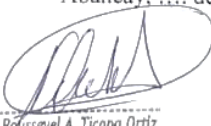
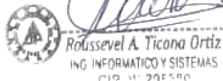
Ing. Roussevel Anderson Ticana Ortiz

(Apellidos y nombres del experto validador)

DNI: 73143778

Especialidad del validador: Ing. Informática y Sistemas

Abancay, 10 de octubre de 2022

Firma del Experto Informante

CONSTANCIA DE VALIDACIÓN DE INSTRUMENTO

Yo, Kenteliv Castillo Melendez, con Documento Nacional de Identidad N° 42159030 de profesión Ingeniero de Sistemas, grado académico Ingeniero, con código de colegiatura 16.68.42, labor que ejerzo actualmente como Responsable Estadística en la Red de Salud Abancay.

Por medio de la presente hago constar que he revisado con fines de Validación el Instrumento denominado **Encuesta de aplicación**, cuyo propósito es medir la **Variable Gestión de Riesgo**, a los efectos de su aplicación a los colaboradores de la **Dirección Sub Regional de Salud chanka Andahuaylas**.

Luego de hacer las observaciones pertinentes a los ítems, concluyo en las siguientes apreciaciones.

Observaciones (precisar si hay suficiencia): Demuestra calidad de redacción, amplitud del contenido a evaluar, congruencia en los indicadores y coherencia en los indicadores.

Opinión de aplicabilidad:

Aplicable

Aplicable después de corregir

No aplicable

Kenteliv Castillo Melendez

(Apellidos y nombres del experto validador)

DNI: 42159030

Especialidad del validador: Ing. Sistemas e Informática

Abancay, 10 de Octubre de 2022.



Firma del Experto Informante

CONSTANCIA DE VALIDACIÓN

Yo, Kenyo Solano Perales, con Documento Nacional de Identidad N° 46685886, de profesión Ingeniero de Sistemas, grado académico **Maestro en Gerencias de Tecnologías de la Información y Comunicaciones**, con código de colegiatura 151264, labor que ejerzo actualmente como **Jefe**, en la Universidad Tecnológica de los Andes Filial Andahuaylas".

Por medio de la presente hago constar que he revisado con fines de Validación el Instrumento denominado **Encuesta de aplicación**, cuyo propósito es medir la **Variable Gestión de Riesgo**, a los efectos de su aplicación a los colaboradores de la **Dirección Sub Regional de Salud Chanka Andahuaylas -2022**

Luego de hacer las observaciones pertinentes a los ítems, concluyo en las siguientes apreciaciones.

Observaciones (precisar si hay suficiencia): Demuestra calidad de redacción, amplitud del contenido a evaluar, congruencia en los indicadores y coherencia en los indicadores.

Opinión de aplicabilidad:

Aplicable [X]

Aplicable después de corregir []

No aplicable []

Mg: **SOLANO PERALES Kenyo.**
(Apellidos y nombres del experto validador)

DNI; **46685886**

Especialidad del validador: **Ingeniero de Sistemas.**

Andahuaylas, a los 10 días del mes de octubre de 2022


Firma del Experto Informante