UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
RESOLUCIÓN N°040-2022-CFI-UNAJMA
RESOLUCIÓN DE COORDINACIÓN DE FACULTAD DE INGENIERÍA

Andahuaylas, 22 de febrero de 2022

VISTO: La Carta N°006-2022-DUI-JJOC-FI-UNAJMA de fecha 21 de febrero del 2022, el Mtro. Juan José Oré Cerrón Director de la Unidad de Investigación de la Facultad de Ingeniería de la Universidad Nacional José María Arguedas, solicita la aprobación de la **designación del Jurado Evaluador** del Proyecto e Informe Final de Tesis del Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA**, y;

CONSIDERANDO:

Que, por Ley Nº 28372 del 29 de octubre del 2004, se crea la Universidad Nacional José María Arguedas, con sede en la provincia de Andahuaylas, Región Apurímac; y que por Resolución Nº 035-2017-SUNEDU/CD de 02 de octubre del 2017, el Consejo Directivo de la Superintendencia Nacional de Educación Superior Universitaria, otorga la Licencia Institucional a la Universidad Nacional José María Arguedas para ofrecer el Servicio Educativo Superior Universitario;

Que, la Ley Universitaria 30220 en su Artículo Octavo respecto a la autonomía universitaria, establece que: "El estado reconoce la autonomía universitaria". La autonomía inherente a las universidades se ejerce de conformidad a la Constitución, las leyes y demás normativa aplicable, esta Normativa se manifiesta en los siguientes regímenes: Normativo, De gobierno, Académico, Administrativo y Económico;

Que, mediante Carta Múltiple Nº 020-2014-SG-UNAJMA, de fecha 30 de julio del 2014; la Secretaría General de la UNAJMA comunica que mediante Acuerdo Nº 03 de Sesión Ordinaria de la Comisión de Gobierno se **AUTORIZA** la emisión de **RESOLUCIONES DE COORDINACIÓN DE LA FACULTAD** estrictamente para asuntos académicos y deberán remitirse un original a la Secretaría General;

Que, mediante carta Nº 236-2016-SG-UNAJMA de fecha 05 de agosto de 2016 el Secretario General de la UNAJMA, comunica que el Presidente de la Comisión Organizadora de la UNAJMA ha dispuesto que las resoluciones emitidas por la Facultad se deriven a la Vicepresidencia Académica;

Que, el **art. 39 incisos a y d del TITULO II, CAPITULO II del Reglamento General de la UNAJMA**, aprobado mediante Resolución Nº 0130-2016-CO-UNAJMA, establece que "Son *funciones de las Facultades: a) dirigir el desarrollo académico y administrativo de las Escuelas Profesionales y Departamentos Académicos adscritos a esta, dentro de la normatividad legal, d) administrar el sistema de matrícula en coordinación y apoyo con la oficina respectiva"*;

Que, el **art. 65º del CAPÍTULO IV (DEL JURADO EVALUADOR) del Reglamento General de Grados y Títulos en la UNAJMA**, aprobado con Resolución Nº0255-2021-CO-UNAJMA, de fecha 10 de setiembre de 2021, establece "*La unidad de investigación de la facultad previa revisión del cumplimiento del expediente correspondiente, convocará a sesión para la designación del jurado Evaluador del proyecto de tesis, que estará conformado por tres (03) docentes ordinarios y/o contratados, adscritos al Departamento Académico correspondiente; […] ";*

Que, mediante **Resolución Nº006-2022-CFI-UNAJMA** de fecha 06 de enero de 2022 se designa al director de la Unidad de Investigación de la Facultad de Ingeniería;

Que, con resolución N° 290-2019-CFI-UNAJMA de fecha 25 de junio del 2019, se aprueba la designación del Ing. EDWING ALCIDES MAQUERA FLORES como Asesor del Proyecto e Informe Final de Tesis con fines de titulación de **EDWIN LLASACCE BAUTISTA,**

Que, con Carta N° 02-2022-UNAJMA-ELLB de fecha 11 de enero del 2022, el bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA** presenta su proyecto de tesis virtual y solicita la designación de Jurados Evaluadores del proyecto e Informe Final de Tesis;

Que, con Acta de Designación de Jurado Evaluador N°006-2022-DUI-JJOC-FI-UNAJMA, de fecha 21 de febrero de 2022, el Director de la Unidad de Investigación de la Facultad de Ingeniería presidido por el Mtro. Juan José Oré Cerrón, designa al Jurado Evaluador del Proyecto e Informe Final de Tesis de acuerdo al siguiente detalle:

Proyecto de Tesis titulado	DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE VIDEOVIGILANCIA PARA LA DETECCIÓN DE ELEMENTOS DE PESCA ILEGAL CON VISIÓN ARTIFICIAL EN LA LAGUNA DE PACUCHA EN EL AÑO 2022	
Tesista	Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA**	
Asesor	Ing. Edwing Alcides Maquera Flores	
Jurado Evaluador	Presidente:	Mg. Enrique Edgardo Condor Tinoco
	Primer Miembro:	Ing. Ruben Apaza Apaza
	Segundo Miembro:	Ing. Richard Carrión Abollaneda

Que, con Carta N°006-2022-DUI-JJOC-FI-UNAJMA de fecha 21 de febrero de 2022, el Mtro. Juan José Oré Cerrón Director de la Unidad de Investigación de la Facultad de Ingeniería de la Universidad Nacional José María Arguedas, solicita la aprobación de la **designación del Jurado Evaluador** del Proyecto e Informe Final de Tesis del Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA;**

Que, en atención a la Carta N° 006 -2022-DUI-JJOC-FI-UNAJMA el Dr. Yalmar Temístocles Ponce Atencio, Coordinador de la Facultad de Ingeniería de la Universidad Nacional José María Arguedas, dispone a la Secretaría Académica de la Facultad de Ingeniería proyectar la Resolución correspondiente, la que se aprueba con cargo a dar cuenta a la Vicepresidencia Académica;

Por estos considerandos y en uso de las atribuciones conferidas como Coordinador de la Facultad de Ingeniería, designado mediante Resolución Nº 0298-2019-CO-UNAJMA, de fecha 15 de octubre de 2019;

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR la designación de los miembros del Jurado Evaluador del Proyecto e Informe Final de Tesis del Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA**, de acuerdo al siguiente detalle**:**

Proyecto de Tesis titulado	DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE VIDEOVIGILANCIA PARA LA DETECCIÓN DE ELEMENTOS DE PESCA ILEGAL CON VISIÓN ARTIFICIAL EN LA LAGUNA DE PACUCHA EN EL AÑO 2022	
Tesista	Bachiller en Ingeniería de Sistemas **EDWIN LLASACCE BAUTISTA**	
Asesor	Ing. Edwing Alcides Maquera Flores	
Jurado Evaluador	Presidente:	Mg. Enrique Edgardo Condor Tinoco
	Primer Miembro:	Ing. Ruben Apaza Apaza
	Segundo Miembro:	Ing. Richard Carrión Abollaneda

ARTÍCULO SEGUNDO: ENCARGAR a la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional José María Arguedas, adopte las acciones correspondientes para el cabal cumplimiento de la presente resolución.

ARTÍCULO TERCERO: REMITIR la presente Resolución a la Vicepresidencia Académica, Escuela Profesional de Ingeniería de Sistemas, Docente Asesor, Miembros de Jurado Evaluador y al interesado para su conocimiento y fines pertinentes.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
Dr. Yalmar Ponce Atencio
COORDINADOR DE LA FACULTAD DE INGENIERÍA

Ing. Richard A. Flores Condori
SECRETARIO ACADÉMICO

Unidad de Investigación de la Facultad Ingeniería

"Año del Fortalecimiento de la Soberanía Nacional"

Andahuaylas, 21 de febrero del 2022

CARTA N° 006-2022-DUI-JJOC-FI-UNAJMA

Señor:
Dr. YALMAR TEMISTOCLES PONCE ATENCIO
Coordinador de la Facultad de Ingeniería
Universidad Nacional José María Arguedas
Ciudad.-

ASUNTO: SOLICITO APROBACIÓN MEDIANTE ACTO RESOLUTIVO DE DESIGNACIÓN DEJURADO EVALUADOR DE PROYECTO DE INVESTIGACIÓN

REFERENCIA: ACTA Nº 006-2022-DUI-JJOC-FI-UNAJMA - RESOLUCIÓN Nº 006-2022- CFI- UNAJMA, y CARTA Nº 0024-2022-UNAJMA-VP/ACAD-FI

Tengo a bien dirigirme a usted para expresarle un saludo cordial, y en aplicación a los artículos 65°, 66º y 67º del CAPÍTULO IV "Del Jurado Evaluador" del TÍTULO III "De los títulos profesionales" del Reglamento de Grados y Títulos de la Universidad Nacional José María Arguedas, aprobado con Resolución Nº 0135-2021-CO-UNAJMA, de fecha 6 de mayo 2021. Solicito la aprobación mediante acto resolutivo de la designación de JURADO EVALUADOR del proyecto de investigación denominado "GESTION DE RIEGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022" de acuerdo al siguiente detalle:

JURADO EVALUADOR:

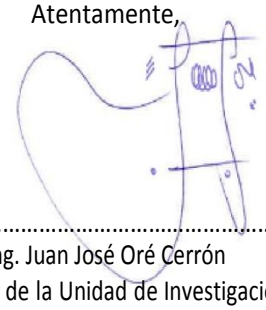
Presidente	: Mg. Condor Tinoco Enrique Edgardo
Primer Miembro	: ING. Ruben Apaza Apaza
Segundo Miembro	: ing. Richard Carrion Abollaneda
ASESOR	: ing. Edwing Alcides Maquera Flores
TESISTA	: Bachiller en Ingeniería de Sistemas, EDWIN LLASACCE BAUTISTA

TITULO DEL PROYECO DE INVESTIGACIÓN: "GESTION DE RIEGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022"

Se adjunta el ACTA Nº 006-2022-DUI-JJOC-FI-UNAJMA - RESOLUCIÓN Nº 006-2022- CFI- UNAJMA, de Fecha 06 de enero del 2022.

Sin otro particular, me suscribo de Ud.

Atentamente,



.....
Ing. Juan José Oré Cerrón
Director de la Unidad de Investigación
de la Facultad de Ingeniería

C.c
Archivo.

Unidad de Investigación de la Facultad Ingeniería

ACTA Nº 006-2022-DUI-JJOC-FI-UNAJMA - RESOLUCIÓN Nº 006-2022- CFI- UNAJMA

DESIGNACIÓN DE JURADO EVALUADOR

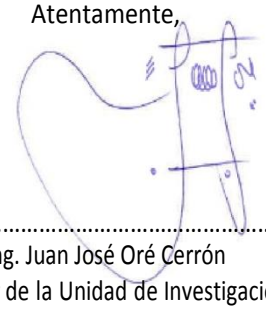
Siendo las 16:30 horas del día 21 de febrero del 2022, en amparo a la **RESOLUCIÓN Nº 006-2022- CFI-UNAJMA**, de fecha 06 de enero de 2022; que designa al ing. Juan José Oré Cerrón como Director de la Unidad de Investigación de la Facultad de Ingeniería ; con el propósito de atender la CARTA Nº 024-2022-UNAJMA-VP/ACAD-FI, de la Coordinación de la Facultad de Ingeniería, en donde el bachiller EDWIN LLASACCE BAUTISTA, solicita designación de Jurado Evaluador del proyecto de investigación denominado "GESTION DE RIEGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022" Se procedió a revisar el expediente del Bachiller EDWIN LLASACCE BAUTISTA, con el fin de verificar los requisitos (Solicitud del bachiller, resolución de designación de asesor, declaración jurada de autenticidad y proyecto de investigación), según los artículos 65°, 66º y 67º del **CAPÍTULO IV "Del Jurado Evaluador"** del **TÍTULO III "De los títulos profesionales"** del **Reglamento de Grados y Títulos de la Universidad Nacional José María Arguedas**, aprobado con Resolución Nº 0135-2021-CO-UNAJMA, de fecha 6 de mayo 2021. Después de evaluar el caso, la Unidad de Investigación de la Facultad de Ingeniería **declara procedente la solicitud,** en tal sentido queda conformada de la siguiente manera:

JURADO EVALUADOR:

Presidente	: Mg. Condor Tinoco Enrique Edgardo
Primer Miembro	: ING. Ruben Apaza Apaza
Segundo Miembro	: ing. Richard Carrion Abollaneda
ASESOR	: ing. Edwing Alcides Maquera Flores
TESISTA	: Bachiller en Ingeniería de Sistemas, EDWIN LLASACCE BAUTISTA

Siendo las 17:00 horas del mismo día y año, se da por finalizada la reunión y en señal de conformidad de los puntos acordados, se procede a firmar la presente acta.

Atentamente,



.....

Ing. Juan José Oré Cerrón
Director de la Unidad de Investigación
de la Facultad de Ingeniería

C.c.
Archivo.

Andahuaylas, 15 de febrero de 2022

CARTA N° 024-2022-UNAJMA-VP/ACAD-FI

Señor:
Msc. Juan José Ore Cerrón
DIRECTOR DE LA UNIDAD DE INVESTIGACIÓN DE LA FACULTAD DE INGENIERÍA

Presente.

ASUNTO: REMITO SOLICITUD PARA DESIGNACIÓN DE JURADO

REFERENCIA: Carta N° 02-2022-UNAJMA-ELLB

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, para expresarle un cordial saludo, y a la vez remitirle la solicitud de DESIGNACIÓN DE JURADO EVALUADOR del BACHILLER **EDWIN LLASACCE BAUTISTA,** Se adjunta la DECLARACIÓN JURADA DE AUTENTICIDAD del BACHILLER de la Escuela Profesional de Ingeniería de Sistemas, y el proyecto de tesis.

Atentamente,

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS
Dr. Yalmar Ponce Atencio
COORDINADOR DE LA FACULTA DE INGENIERÍA

Andahuaylas, 11 de enero de 2022

Carta Nº 02-2022-UNAJMA-ELLB
Señor:
Dr. Yalmar Temistocles Ponce Atencio
Coordinador de la Facultad de Ingeniería
Universidad Nacional José María Arguedas
Ciudad.-

ASUNTO: DESIGNACION DE JURADO EVALUADOR DE TESIS

……

Tengo el agrado de dirigirme a usted, para expresarle un cordial saludo, así mismo para presentar a su Despacho 03 ejemplares de mi Proyecto de Tesis intitulado: **"GESTION DE RIEGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022"** para la aprobación del jurado evaluador su evaluación y posterior aprobación mediante acto resolutivo de la Facultad de Ingeniería.

Es propicia la oportunidad para expresarle los sentimientos de mi especial consideración y estima personal.

Atentamente,

……
Bach. Edwin LLasacce Bautista
Tesista

……
ing. Edwing Alcides Maquera Flores
Asesor de Tesis

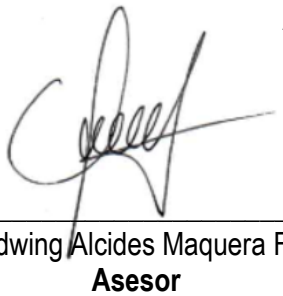
C.c.
Archivo

APROBACION DEL ASESOR

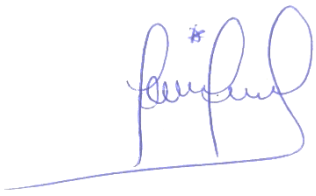
Quién suscribe:
Ing. Edwing Alcides Maquera Flores por la presente:

CERTIFICA,
Que, el Bachiller en Ingeniería de Sistemas, EDWIN LLASACCE BAUTISTA ha culminado satisfactoriamente con el levantamiento de las Observaciones realizadas por el jurado evaluador el Proyecto de Tesis intitulado: **"GESTION DE RIEGOS 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, 11 de enero de 2022



Ing. Edwing Alcides Maquera Flores
Asesor



Bach. Edwin LLasacce Bautista
Tesista

ANEXO 3

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, Edwin LLasacce Bautista, identificado (a) con DNI N° 73471099 de la Escuela Profesional de Ingeniería de Sistemas. Declaro bajo juramento que el Proyecto Titulado: (Trabajo de Investigación/ Tesis / Trabajo de Suficiencia Profesional)
"GESTION DE RIEGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022" Es auténtico y no vulnera los derechos de autor. Además, su contenido es de entera responsabilidad del autor (es) del proyecto, quedando la UNAJMA exenta de toda responsabilidad en caso de atentar contra la Ley de propiedad intelectual y derechos de autor.

Andahuaylas, 11 de enero de 2022

…….
Firma
N° DNI: 73471099

E-mail: jjedwin0410@gmail.com

N° Celular: 953756762

UNIVERSIDAD NACIONAL JOSÉ MARÍA ARGUEDAS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

P R O Y E C T O D E T E S I S

"GESTION DE RIESGOS TECNOLOGICOS EN EL DATA CENTER DE LA DIRECCION SUB REGIONAL DE SALUD CHANKA BASADO EN LA ISO 31000, ANDAHUAYLAS 2022"

LÍNEA DE INVESTIGACIÓN : SEGURIDAD DE LA INFORMACION

ÁREA PRIORIZADA PNCYT : DESARROLLO DE SISTEMAS DE GESTION

PRESENTADO POR EL BACHILLER: EDWIN LLASACCE BAUTISTA

PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

ASESOR: ING. EDWING ALCIDES MAQUERA FLORES

ANDAHUAYLAS – APURÍMAC

PERÚ

Noviembre, 2022

INDICE

TABLA DE CONTENIDO

ANEXOS

ANEXO 01: Matriz de consistencia

ANEXO 02: Plan operativo Informático

ANEXO 03: Plan estratégico de tecnología de Información

INTRODUCCION

A nivel mundial la incorporación de las tecnologías de informacion y comunicación (TIC) en la administración publica y privada se viene realizando constantemente desde que se constituyerin un elemento impresendible para el funvionamiento de las organizaciones.

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

Es entonces que al enterder la importancia de la infromacion almacenada es que se hace necesario contar con un plan estratégico de la gestión de riegos de la información, y esto se realiza a partir de la evaluación de riesgos tecnologícos del data center a fin de evitar la perdida de informacion como activo de la organización.

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

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

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

Las TIC cada vez son más demandadas por quienes forman parte de la sociedad de la Información y del conocimiento. Las organizaciones no son la excepción, dado que en ellas genera información de manera cotidiana y se requieren de las tecnologías de información para administrarlas de manera efectiva, con la idea de alinear sus objetivos hacia la mejora de sus procesos y reducción de costos de igual manera, requieren de las TIC para estar en contacto con el mundo, con sus clientes en tiempo real y lograr un nivel competitivo que les asegure una larga permanecía dentro de una sociedad globalizadora. 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 el gran facilitador, pero también presenta riesgo generalizado, potencialmente de impacto alto. El riesgo cibernético en la forma de robo de datos, cuentas comprometidas, archivos destruidos, sistemas deshabilitados o degradados en este día está en “la parte superior del pensamiento.” Las fusiones y adquisiciones pueden de manera irremediable complicar el entorno de TI 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 consideran dentro de su estructura funcional el área de tecnologías de la Información quienes son encargadas de apoyar las labores administrativas y académicas mediante un adecuado servicio informático, soporte informático y distintas funciones propias de la oficina.

La información de una empresa es uno de los activos más importantes debido a que tiene un impacto directo en las decisiones del negocio es por ello que gran parte de la información de las instituciones se encuentran almacenadas en fuentes de almacenamientos informáticos como servidores que están bajo resguardo de las Oficinas de Tecnologías de la Información siendo el caso que en la mayoría de ellas no cuentan con una adecuada gestión los riesgos existentes que pueden causar daños perjudiciales, inclusive desestabilizando la consecución de los objetivos de la institución

En la Dirección Sub Regional de Salud Chanka de Andahuaylas dentro de su estructura organizacional cuenta con el área de Tecnología de Información y como parte de sus instalaciones su propio centro de Datos, 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.

La seguridad perimetral contempla la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones de centro de datos mal denominada data center de la Dirección Sub Regional de Salud Chanka de Andahuaylas - DISA 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 - DISA 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 organizacion.

El plan estratégico de tecnología de información considera en el marco estratégico de TI en el cuadro Nº 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 Nº10 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 DISA basada en la ISO 31000, Andahuaylas-2019?

1.2.2 Problemas específicos

a) ¿Cómo es el análisis de los riesgos para el Data Center de la DISA basado en la ISO 31000?

b) ¿Cómo es la identificación de los riesgos para el Data Center de la DISA basado en la ISO 31000?

c) ¿Cómo es la evaluación de los riesgos priorizados para el Data Center de la DISA basado en la ISO 31000?

1.3 Justificación

Las tecnologías de información y comunicación han dejado de ser tan solo herramientas de apoyo para convertirse en parte del negocio, y como tal ejerce una influencia directa en la productividad y competitividad organizacional. De ahí que sean considerados recursos estratégicos vitales, para el desarrollo de cualquier organización. Sin embrago, como cualquier recurso es vulnerable a múltiples amenazas que se pueden materializar en riesgos, con diversos impactos en términos de perdida de datos, interrupción de servicios, pérdidas financieras, daños a la reputación e incluso pérdidas humanas.

Amenazas tan comunes como los virus, los fallos de software, las caídas de red, los programas espía, troyanos, los robos de equipos, el Spam, a los cuales está expuesto cualquier organización, lleva a la necesidad de valorarlos y a partir de ahí tomar acciones que permitan implementar adecuados controles para tratar

de garantizar niveles aceptables de riesgo con la finalidad de salvaguardar la información que es activo primordial de toda organización.

Uno de los aspectos de las tecnologías de la información que más importancia tiene en la actualidad es el de la seguridad.

La Oficina Nacional de Gobierno Electronico e informática – ONGEI de la Presidencia del Consejo de Minitros - PCM estable que las instituciones deben de contar con los siguientes documentos de gestión como es el Plan Operativo Infromatico – POI y el Plan Estrategico de Tecnologias de Informacion, 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 Estrategico 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 como obligatorios por la Oficina Nacional de Gobierno Electrónico e Informatico – ONGEI por cuanto es necesario realizar una evaluación de reigo del Data Center a fin de evitar perdidad de información que perjudicaría desastrosamente a la organización, para ello se realaizara la evaluación de riesgos mediante la ISO 31000 que fortalecera la gestión de las tecnologías de informacion incorporando de nuevos equipos (servidores, seguridad perimetral, sistemas de seguridad y contigencia establecidos en la TIRE) para la implementacion de nuevos servicios sobre la pataforma del Data Center.

1.4 Objetivos

1.4.1 Objetivo general

Evaluar la propuesta estratégica basada en ISO 31000 en gestión de riesgos tecnológicos para el data center de la DISA, Andahuaylas 2019”.

1.4.2 Objetivos específicos

a) Analizar los riesgos para el Data Center de la DISA basado en la ISO 31000.
b) Identificar los riesgos para el Data Center de la DISA basado en la ISO 31000.
c) Proponer los riesgos priorizados para el Data Center de la DISA basado en la ISO 31000.

CAPITULO II

MARCO TEORICO

2.1. A**ntecedentes**

2.1.1. **Antecedentes a nivel internacional**

Ramírez Castro & Ortiz Bayona (2011) en su tesis “Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios” concluye que: La gestión de los riesgos tecnológicos es importante dado que las organizaciones al usar tecnología en su actividad diaria y como parte de sus procesos de negocio se encuentran expuestas a este tipo de riesgos; por ello pueden afectar la actividad propia de las mismas y ser fuentes de pérdidas y daños considerables. De lo anterior los planes de seguridad deben enfatizar en crear conciencia en seguridad para prevenir riesgos y buscar estrategias para obtener el apoyo de la alta dirección con el fin de cumplir con los objetivos y asegurar la información crítica, adicional la gestión adecuada de los riesgos permite evitar en gran medida la ocurrencia de incidentes y con ello evitar la activación de planes de continuidad. Las organizaciones deben robustecer su protección a nivel físico (lo correspondiente a infraestructura, incluyendo la tecnológica), nivel lógico (sistemas de información y software) y factor humano (toma de medidas organizacionales); en estos tres aspectos está presente el uso de tecnología y por ello la exposición a este tipo específico de riesgo crece constantemente. Esta es la motivación de la metodología descrita, como punto de partida para dar lineamientos sobre cómo gestionar este tipo de riesgos integrando los tres aspectos mencionados y buscando un marco de

protección integral. Finalmente, es necesario resaltar que sin importar el ámbito en el que se encuentra una organización se requiere la aplicación de gestión de riesgos. Para muchas organizaciones la toma de medidas preventivas, que es el principal punto de la gestión de riesgos, y la continuidad de negocios puede pasar como irrelevante, pero en su debido cuidado radica la disminución de pérdidas y perjuicios.

Arias Reyes, Diaz Rodriguez, & Vargas Carvajal (2014) en su trabajo de investigación titulada “Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia”, concluye que: En todo proceso, área u organización siempre existirán riesgos, independientemente si estos son detectados o no, y es por este motivo que se debe implementar una gestión de riesgos eficiente para mitigarlos pues eliminarlos no es posible pero si ejercer un control adecuado sobre estos. Las empresas de tecnología que tienen procesos internos involucrados en el área de mesa de ayuda requieren un alto grado de gestión de riesgos pues no contar con mecanismos que mitiguen los estos generaran pérdidas que afectaran la funcionalidad de la organización. Actualmente existen muchas empresas de tecnologías que tienen como núcleo de negocio el área de mesa de ayuda, pero, aunque con amplia experiencia se pudo observar con la empresa trabajada que no tienen bien definido este plan de gestión de riesgos y que se guían más por las experiencias que por diseñar y seguir una guía adecuada que les permita mejorar sus procesos. Es necesario realizar campañas de concientización en todo tipo de empresa para que entiendan que la implementación de la gestión de riesgo y más cuando existen guías

puntuales generadas es necesaria y que les ayudara a dar continuidad al negocio. De manera exacta se debe seguir el procedimiento desarrollado en la guía planteada, ajustándola en caso de ser necesario a los procesos del área de mesa de ayuda, para poder obtener una correcta gestión de los riesgos y de esta manera mitigar estos llevando a cumplir los objetivos del área.

2.1.2. **Antecedentes a nivel nacional**

Ccesa Quincho (2017) en su trabajo de investogacion titulado "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: El análisis y gestión de riesgos es la columna vertebral de un sistema de gestión de seguridad de la información, porque permitió cuantificar el riesgo. Es decir, es un indicador estadístico que mide la incertidumbre. En este trabajo de investigación la evaluación de riesgos, adoptando MARGERIT V.3 como metodología de análisis y gestión de riesgos, permitió identificar y valorar los activos, identificar y valorar las amenazas, calcular el impacto e identificar los riesgos a los que se encuentra expuesta la Municipalidad Provincial de Huamanga. Asimismo, el uso de MARGERIT permitió contar con la documentación (sobre evaluación de riesgos) exigida por la NTP ISO/IEC 27001:2014. Teniendo en cuenta los riesgos identificados, se elaboró los controles de seguridad para mitigar los riesgos altos y medios (Ver Tabla 4.22). Asimismo, los controles de seguridad de la ISO 27002, permiten establecer métricas, que ayuden a medir la eficacia y eficiencia del SGSI una vez implementados.

Ríos Villafuerte (2014) en su trabajo de investogacion titulado "Diseño de un sistema de Gestión de Seguridad de Información para una central privada de información de riesgos", expresa los siguiente: Contar con un adecuado Sistema de Gestion de Seguridad de Informacion - SGSI es indispensable para la administración de la seguridad en una organización con alto nivel de complejidad como lo es una Central Privada de información de riesgo, para poder conseguir una mayor eficiencia y garantía en la protección de sus activos de información y en la calidad de la seguridad de la información. La implantación requiere conocimiento de un experto, por lo que la ayuda externa puede ser imprescindible. Asimismo, contar con un área de seguridad de información es muy importante para el seguimiento y mejoramiento del Sistema de Gestion de Seguridad de Informacion - SGSI.

2.2. Bases teórico científicas

2.2.1. Riesgo

Según Jhuéz (2015) el riesgo es Efecto de la incertidumbre sobre los objetivos, considerando que un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos; y también que los objetivos pueden tener aspectos diferentes (por ejemplo financieros, salud y seguridad, y metas ambientales) y se pueden aplicar en niveles diferentes (estratégico, en toda la organización, en proyectos, productos y procesos).

En el plano corporativo, el riesgo se define como la incertidumbre que surge durante la consecución de un objetivo. Se trata, en esencia, circunstancias, sucesos o eventos adversos que impiden el normal desarrollo de las actividades de una empresa y que, en general, tienen repercusiones económicas para sus responsables.

De acuerdo a Arenas, Lagos , & Hidalgo (2010) La amenaza o peligro se concibe como un factor externo de riesgo, representado por la potencial ocurrencia de un suceso de origen natural, que puede manifestarse en un lugar específico, con una intensidad y duración determinadas.

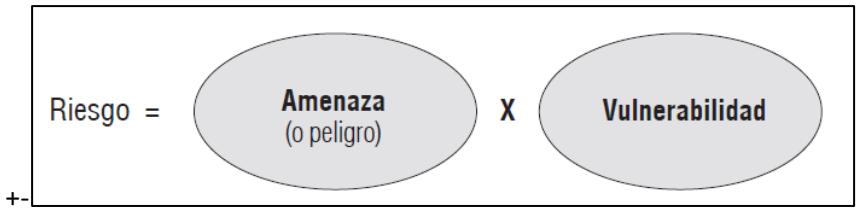


Figura 1: El Riesgo es una Función de la Amenza por Vulnerabilidad. Fuente Amenazas ambientales y vulnerabilidad, https://bit.ly/2G5tqcb

Como las amenazas son inevitables, los esfuerzos para disminuir el riesgo y desastre deben concentrarse en disminuir la vulnerabilidad de nuestros asentamientos humanos.

Según el tipo de actividad

Los riesgos están presentes en cualquier actividad. Sin embargo, algunos implican un mayor o menor nivel de incidencia sobre las actividades de las empresas. Una primera clasificación de los mismos puede hacerse en los siguientes términos:

- **Ç+5432 R0iesgo sistemático:** Se refiere a aquellos riesgos que estén presentes en un sistema económico o en un mercado en su conjunto. Sus consecuencias pueden aquejar a la totalidad del entramado comercial, como sucede, por ejemplo, con las crisis

económicas de gran envergadura y de las cuales ninguna compañía puede sustraerse. También pueden ser originados por accidentes, guerras o desastres naturales.

- **Riesgo no sistemático:** Son los riesgos que se derivan de la gestión financiera y administrativa de cada empresa. Es decir, en este caso la que falla es una compañía en concreto y no el conjunto del mercado o escenario comercial. Varían en función de cada tipo de actividad y cada caso, al igual que la manera en que son gestionados. Las situaciones de crisis internas o un plan de crecimiento mal implementado son algunos ejemplos.
- **Según su naturaleza:** Pero los riesgos también pueden definirse en función de su naturaleza. De hecho, es la manera más extendida a la hora de clasificarlos. Está claro que un riesgo de tipo legal o jurídico no debe tener la misma gestión que otro de tipo económico.

En ese sentido, la clasificación de los riesgos quedaría de la siguiente manera:

- **Riesgos financieros:** Son todos aquellos relacionados con la gestión financiera de las empresas. Es decir, aquellos movimientos, transacciones y demás elementos que tienen influencia en las finanzas empresariales: inversión, diversificación, expansión, financiación, entre otros. 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:** En este caso, se refiere a los riesgos asociados a la actividad económica, ya sean de tipo interno o externo. En el primer caso, hablamos de las pérdidas que puede sufrir una organización debido a decisiones tomadas en su interior. En el segundo, son eventos cuyo origen es externo. Para diferenciarlo del ítem anterior, es preciso señalar que el riesgo económico afecta el valor de la gestión de riesgos en las organizaciones básicamente a los beneficios monetarios de las empresas, mientras que los financieros tienen que ver con todos los bienes que tengan las organizaciones a su disposición.
- **Riesgos ambientales:** Son aquellos a los que están expuestas las empresas cuando el entorno en el que operan es especialmente hostil o puede llegar a serlo. Tienen dos causas básicas: naturales o sociales. En el primer grupo podemos mencionar elementos como la temperatura, la altitud, la presión atmosférica, las fallas geológicas, entre otros. En el segundo, cuestiones como los niveles de violencia y la desigualdad. Sea como sea, lo cierto es que son riesgos que no dependen de las empresas y que, por tanto, su gestión requiere de planes preventivos más eficaces.
- **Riesgos políticos:** Este riesgo puede derivarse de cualquier circunstancia política del entorno en el que operen las empresas. Los hay de dos tipos: gubernamentales, legales y extralegales. En el primer caso se engloban todos aquellos que son el resultado de acciones que han sido llevadas a cabo por las instituciones del lugar, por ejemplo, un cambio de gobierno o una modificación en las políticas comerciales. En el segundo caso, se sitúan actos al margen de la ley como acciones terroristas, revoluciones o sabotajes.

- **Riesgos legales:** Se refiere a los obstáculos legales o normativos que pueden obstaculizar el rol de una empresa en un sitio determinado. Por ejemplo, en algunos países operan leyes restrictivas en el mercado que limitan la acción de ciertas compañías. Estos riesgos van generalmente ligados a los de carácter político.

2.2.2. **La gestión del riesgo**

Gómez Rivadeneira (2014) La gestión del riesgo puede entenderse como el proceso de identificar la vulnerabilidad de las poblaciones ante una amenaza, luego analizar las posibles consecuencias derivadas del impacto de la amenaza obre esa población, delimitar la incertidumbre relativa a la ocurrencia del evento crítico que se desea evitar y mecanismos para reducir la amenaza, la vulnerabilidad y para afrontar el evento crítico si llegara a ocurrir.

2.2.3. **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.

2.2.4. **Consecuencia**

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

2.2.5. **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 perdida.

2.2.6. **ISO 31000**

Según Casares, Martí, & Lizarzaburu Bolaños (2016) Es una guía de implementación que pretende ayudar a las organizaciones en el desarrollo de su propio enfoque de gestión del riesgo. Pero no es un estándar del que se pueda solicitar certificación. Mediante la implementación de la norma ISO 31000, las organizaciones pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente para conseguir una gestión eficaz de los riesgos y un buen gobierno corporativo. Es muy utilizada para programas de auditoría interna o externa de riesgos.

2.2.7. **Principios de la gestión de riesgos**

2.2.7.1. **Principio 1: La gestión del riesgo crea y protege el valor**

(Bolaños, 2016) afirma que “La gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño, por ejemplo, en lo referente a la salud y seguridad de las personas, a la conformidad con los requisitos legales y reglamentos, a la aceptación por el público, a la protección

ambiental, a la calidad del producto, a la gestión del proyecto, a la eficacia en las operaciones, y a su gobierno y reputación".

2.2.7.2. **Principio 2:**

(Bolaños, 2016) afirma que "La gestión del riesgo es una parte integral de todos los procesos de la organización. La gestión del riesgo no es una actividad independiente, separada de las actividades y procesos principales de la organización, sino que es parte de las responsabilidades de gestión y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica y todos los procesos de la gestión de proyectos y de cambios".

.

2.2.7.3. **Aplicación del principio 3:**

(Bolaños, 2016) afirma que "Este principio establece que la gestión del riesgo proporciona la base para la toma de decisiones. La gestión del riesgo debe integrarse en las actividades para la consecución de los objetivos y el proceso de toma de decisiones, así como recoger las políticas de la organización sobre la gestión del riesgo y la forma en que se debe comunicar. El proceso de toma de decisiones debe evaluarse constantemente y, en caso necesario, proceder al tratamiento del riesgo. La toma de decisiones implica riesgos y es importante comprender los riesgos asociados en ambas situaciones".

2.2.7.4. **Aplicación del principio 4:**

(Bolaños, 2016) afirma que “Lo que hace a la gestión del riesgo única entre otros tipos de gestión es que aborda específicamente el efecto de la incertidumbre sobre los objetivos. El riesgo solo se puede evaluar o tratar eficazmente si se conoce la naturaleza y el origen de esa incertidumbre, muy importante cuando se seleccionan tratamientos para el riesgo, y se consideran el efecto y la fiabilidad de los controles. Asimismo, habrá incertidumbre asociada con las medidas de apoyo del proceso de la gestión del riesgo, por ejemplo, si la información ha sido eficaz cuando hay comunicación o consultas con las partes involucradas, o si los intervalos seleccionados por los procesos de seguimiento son suficientes para detectar cambio”.

2.2.7.5. **Principio 5:**

(Bolaños, 2016) afirma que “La gestión del riesgo es sistemática, estructurada y oportuna.Un enfoque sistemático, oportuno y estructurado de la gestión del riesgo contribuye a la eficacia y a resultados coherentes, comparables y fiables”.

2.2.7.6. **Aplicación del principio 6:**

(Bolaños, 2016) afirma que “Solo se puede comprender correctamente un riesgo si está basado en la mejor información disponible, por lo que las decisiones de la gestión del riesgo deberían incluir métodos para recoger o genera información, aunque esta puede estar limitada. Por ejemplo, prever lo que

ocurrirá en el futuro puede estar limitado al uso de proyecciones estadísticas".

2.2.7.7. **Principio 7:** La gestión del riesgo está adaptada

(Bolaños, 2016) afirma que "La gestión del riesgo se alinea con el contexto externo e interno de la organización y con el perfil del riesgo".

2.2.7.8. **Principio 8:** La gestión del riesgo integra los factores humanos y culturales

(Bolaños, 2016) afirma que "La gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización".

2.2.7.9. **Principio 9:** (Bolaños, 2016) afirma que "La gestión del riesgo es transparente y participativa. La implicación apropiada y oportuna de las partes interesadas y, en particular, de las personas que toman decisiones a todos los niveles de la organización, asegura que la gestión del riesgo se mantenga pertinente y actualizada. La implicación también permite a las partes interesadas estar correctamente representadas y que sus opiniones se tengan en cuenta en la determinación de los criterios de riesgo".

2.2.7.10. **Aplicación del principio 10:** (Bolaños, 2016) afirma que "Cualquier cambio en los objetivos de la organización o cualquier aspecto de las circunstancias internas o Cualquier cambio en los objetivos de la organización o cualquier aspecto de las circunstancias internas o externas, inevitablemente cambiará el riesgo (por ejemplo, una reestructuración interna, un importante proveedor nuevo o un cambio en la normativa legal). Asimismo, los cambios en el contexto organizacional (por ejemplo, la adquisición de otra compañía o conseguir un nuevo contrato importante) pueden requerir cambios en el marco de referencia (por ejemplo, en formación, en especialistas de riesgos). Los procesos de gestión del riesgo deben diseñarse para reflejar la dinámica de la organización (por ejemplo, rapidez del cambio)".

2.2.7.11. **Principio 11:** La gestión del riesgo facilita la mejora continua de la organización

(Bolaños, 2016) afirma que "Las organizaciones deberían desarrollar e implementar estrategias para mejorar su madurez en la gestión del riesgo y en todos los demás aspectos de la organización".

2.2.8. **Data center:** Según Bautista Díaz (2017) Un data center o también llamado CPD (Centro de Procesamiento de Datos) en un espacio con determinadas características físicas especiales de refrigeración, protección y redundancia, cuyo objetivo es alojar todo el equipamiento tecnológico de la compañía brindando seguridad y

confiabilidad. Todas estas condiciones aseguran la disponibilidad de los servicios de red.

Es un lugar crítico para las empresas, ya que en él se alojan los activos más importantes de las empresas, y además es una unidad de negocio muy importante con valor propio.

De acuerdo a Tongo Evangelista (2017) clasifica en:

2.2.8.1. **Clasificación**

a) Por el tipo de servicio

Data center de internet: Construido por empresas para proveer a sus clientes tanto servicios de internet como servicios de datos (housing y hosting) quien abarca gran parte del mercado de las telecomunicaciones.

Data center corporativo: Son construidos para proveer servicio de datos a una sola empresa, quien permite la interconexión entre los diferentes servidores internos de una organización hacia la WLAN e internet.

b) Por los niveles de redundancia

Está determinada por el Uptime Institute (18) y depende de la disponibilidad y redundancia que posee una data center, se definen por 4 niveles de TIER:

TIER I: Infraestructura básica

Usados en empresas pequeñas, no posee redundancia en ningún de sus componentes por lo que es susceptible a interrupciones de los servicios en el caso de existir alguna falla en sus elementos.

TIER II: Infraestructura con dispositivos redundantes

Posee elementos redundantes, usualmente en aspectos eléctricos y de refrigeración, que lo hace menos susceptible a interrupciones en comparación al nivel I, tiene una sola ruta de distribución eléctrica, el piso y el uso de UPS es un requerimiento para su alimentación.

TIER III: Infraestructura concurrente mantenible

Además de contar con redundancia en sus componentes, posee dos rutas de alimentación eléctrica y de enfriamiento de las cuales una está activa, todos los equipos de telecomunicaciones deben tener fuentes de alimentación redundantes esto permite realizar mantenimiento sin interrupciones de los servicios. Se establece el control de acceso mediante uso de lector de tarjeta o la identificación biométrica con el tiempo estimado de fallas de 105 minutos al año.

TIER IV: Infraestructura tolerante a fallos

Data center con sistemas independientes con múltiples componentes redundantes y rutas de

distribución que están activas siempre. Tiene resguardo contra desastres naturales como sismos, huracanes o inundaciones.

CAPITULO III

DISEÑO METODOLOGICO

3.3 Hipótesis de investigación

3.3.1 Hipótesis general

Hernández Sampieri (2014) no todas las investigaciones cuantitativas plantean hipótesis. La formulación de hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas cuyo alcance de estudio es exploratorio, no se formula hipótesis; si es descriptivo, sólo se formulan hipótesis cuando se pronostica un hecho o dato; si es correlacional, formulan hipótesis correlacionales; y si es explicativo, formulan hipótesis causales.

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

Monje (2011) La investigación descriptiva se basa en la información conseguida, a ordenar los rasgos, atributos o características de la realidad observada con respecto al problema indagado, la descripción permite reunir los resultados de la observación en una exposición relacionada de los rasgos del fenómeno que se estudia de acuerdo con criterios que le den coherencia y orden a la exposición de los datos. En el nivel descriptivo de la investigación no se plantean claramente la hipótesis; por consiguiente, no es una condición necesaria para la investigación cualitativa la formulación de hipótesis.

Considerando las citas mencionadas, la presente investigación tiene un nivel de investigación descriptivo y no pronostica ningún hecho o dato es por ello que no se considerará la hipótesis, debido a que se realizará una propuesta de mejora para la gestión de riesgos para el Data Center con el ISO 31000.

3.4 Operacionalización de variables

La variable para el estudio de la investigación es única:

Variable Independiente: gestión de riesgos

Operacionalizacion De Variables

Tabla 1: *Operacionalización de variables*

DIMENSIONES	INDICADORES
D1: Establecer contexto	I1: Objetivos definidos
	I2: Estrategias definidas
	I3: Responsables asignados
	I4: Procesos identificados
	I5: Recursos identificados
D2: Identificar riesgos	I1: Riesgos internos
	I2: Causas de los riesgos internos
	I3: Fuentes Riesgos
	I4: Zonas de Impacto
D3: Analizar Riesgos en el Data Center	I1: Controles de Gestion de Riesgo
	I2: Probabilidad de Ocurrencia
	I3: Causas
	I4: Consecuencias
D4: Evaluacion de Riesgos del Data Center	I1: Datos Priorizados
	I2: Actividades de Reduccion
	I3: Toma de Decisiones

Fuente: Elaboracion Propia

3.5 Diseño de investigación

3.5.1 Diseño no experimental

La investigación no experimental es aquella que se realiza sin manipular deliberadamente variables. Es decir, es investigación donde no hacemos variar intencionalmente las variables independientes. Lo que hacemos en la Investigación no experimental es observar fenómenos tal y como se dan en su

contexto natural, para después analizarlos. Como señala Kerlinger (1979, p.116). “La investigación no experimental o expostfacto es cualquier investigación en la que resulta imposible manipular variables o asignar aleatoriamente a los sujetos o a las condiciones". De hecho, no hay condiciones o estímulos a los cuales se expongan los sujetos del estudio. Los sujetos son observados en su ambiente natural, en su realidad. Una investigación experimental es en la cual el investigador manipula y controla una o más variables independientes y observa la o las variables dependientes para medir las variaciones concomitantes.

3.5.2 Diseño descriptivo simple

El diseño de la presente investigación es descriptiva simple, en este diseño el investigador busca y recoge información actual con respecto a una situación previamente determinada, no presentándose la administración o control de un tratamiento, es decir que se busca conseguir información para poder tomar una decisión. Hernandez, Fernández, & Baptista (2010)

Se esquematiza de la siguiente forma:

Figura 2 Investigación no experimental descriptiva simple, Fuente Diseño de Investigación Educacional - Atilio G. Olano Martínez, 2010

M: Representa la muestra del personal de la sede administrativa de la DISA

O: Representa la información recogida de la muestra

De acuerdo a las teorías expuestas se debe tener en cuenta en la investigación, que solo se basará en la recolección de información actual con respecto a una situación objeto de estudio.

3.6 Población y muestra

3.6.1 Población

Se considerará como población a todos los administrativos de la oficina de la DISA.

Descripción

- Dirección General.
- Oficina de Administración.
- Oficina de Gestión y Desarrollo de RR.HH.
- Oficina de Comunicaciones.
- Oficina de Seguros.
- Oficina de Asesoría Jurídica.
- Oficina de Planeamiento Estratégico.
- Dirección Ejecutiva de Promoción de la Salud.
- Dirección Ejecutiva de Salud de las Personas.
- Dirección Ejecutiva de Productos Farmacéuticos, dispositivos Médicos y Productos Sanitarios.
- Órganos Desconcentrados.

3.6.2 Muestra

La muestra será censal pues se seleccionará al 100% de la población

3.6.3 Técnicas de instrumentos de acopio de datos

En el presente proyecto se aplicará la técnica de la Encuesta para la variable (gestión de riesgo).

Para Trespalacios Gutiérrez, Vázquez Casielles, & Bello Acebrón (2005) las encuestas son instrumentos de investigación descriptiva que precisan identificar a priori las preguntas a realizar, las personas seleccionadas en una muestra representativa de la población, especificar las respuestas y determinar el método empleado para recoger la información que se vaya obteniendo.

3.7 Método de investigación

Para la presente investigación se usará el método descriptivo, puesto que se basa en observaciones sistemática del objeto de estudio cuyo objetivo es evaluar algunas características de una población o situación en particular.

3.8 Técnicas de análisis de datos

Se Utilizará hojas de cálculo (MS Excel 2016) para dichos análisis de datos, se calculará el porcentaje total del cumplimiento de la Norma ISO 31000.2009 para la gestión de riesgos en el Data Center de la DISA elaborando tablas, gráficos de barra.

CAPITULO IV

ASPECTOS ADMINISTRATIVOS

4.1. Periodo de desarrollo

El periodo de ejecución para el presente proyecto de Investigación tendrá una duración de 04 meses calendarios.

4.2. Presupuesto

Tabla 2: Presupuesto

ITEM	DESCRIPCIÓN	CANTIDAD	UND. MEDIDA	PRECIO UNIT	PRECIO PARCIAL
100.000	ELABORACIÓN Y APROBACIÓN DE TESIS				1,480.00
101.000	Elaboración				1,480.00
101.001	Asesoría	2	Unid	600.00	1,200.00
101.002	Servicio de Internet	4	Mensual	50.00	200.00
101.003	Fotocopias y útiles de escritorio	100	Unid	0.20	20.00
101.004	impresión	600	Unid	0.10	60.00
101.005	anillado	6	Unid	5.00	30.00
200.000	EQUIPAMIENTO				3,350.00
201.000	Equipos				3,350.00
201.001	Laptop	1	Unid	3,000.00	3,000.00
201.002	Comunicaciones	500	Minutos	0.50	250.00
201.003	router	1	Unid	100.00	100.00
300.000	MATERIAL BIBLIOGRÁFICO				490.00
301.000	Libros de Especialidad				210.00
301.001	Libros de Gestión de Riesgo	2	Unid	70.00	140.00
301.002	Introducción a la Gestión de Riesgo Integral ISO 31000	1	Unid	70.00	70.00
302.000	Libros Metodológicos				280.00
302.001	Libros de Metodología de Investigación	4	Unid	70.00	280.00
400.000	DISEÑO Y DESARROLLO				1,000.00
401.000	Elaboración				1,000.00
401.001	Diseñador	1	Persona	500.00	500.00
401.002	Analista	1	Persona	500.00	500.00
500.000	REVISIÓN DE INFORME Y LEVANTAMIENTO DE OBSERVACIONES				200.00
501.000	Levantamiento de observaciones				200.00
501.001	Asesor	1	Sesion	200.00	200.00
501.002	impresión	1	millar	100.00	100.00
600.000	ELABORACIÓN DE INFORME DE TESIS				710.00
601.000	Redacción				100.00
601.001	Digitador	1	Persona	100.00	100.00
602.000	impresión				610.00
602.001	impresión	1	millar	100.00	100.00
602.002	Empastado y Acabado	3	Unid	170.00	510.00
700.000	SUSTENTACION Y DEFENSA DE TESIS				700.00
701.000	Sustentación				700.00
701.001	Gasto Por Sustentación	1	Pago	700.00	700.00
800.000	RECURSOS HUMANOS				450.00
801.000	Asesores				400.00
801.001	Asesor Metodológico	4	sesion	50.00	200.00
801.002	Asesor Técnico Especialista	2	Sesion	50.00	100.00
801.003	Asesor Estadístico	2	Sesion	50.00	100.00
802.000	Procesamiento de Datos				50.00
802.001	Digitador	1	Sesion	50.00	50.00
900.000	GASTOS GENERALES				5,700.00
901.000	Tesista				3,500.00
901.001	Tesista	5	mes	700.00	3,500.00
902.000	Servicios				2,200.00
902.001	Viáticos	4	mes	300.00	1,200.00
902.002	imprevistos	1	Unid	1,000.00	1,000.00
COSTO TOTAL DE LA TESIS					14,080.00

Fuente: Elaboración propia

Financiamiento

Estructura de financiamiento.

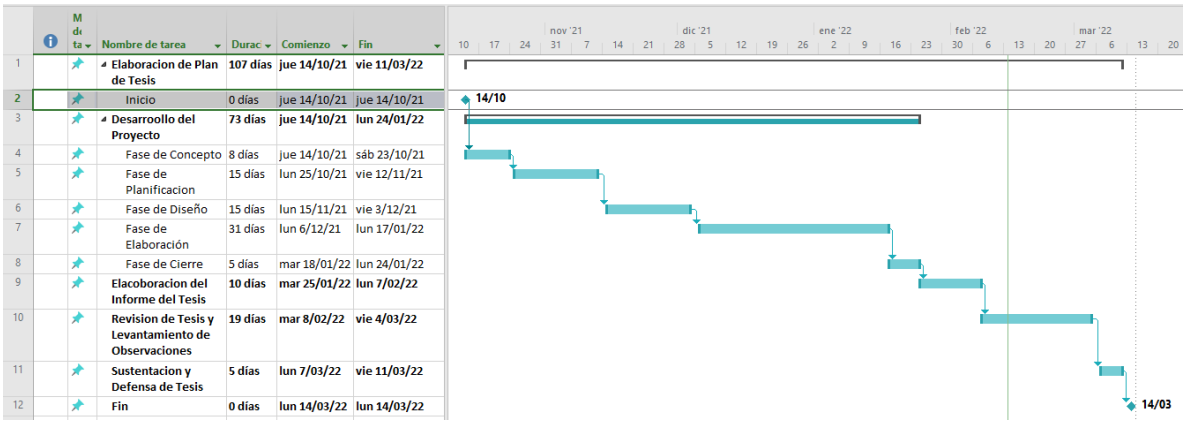
Autofinanciado ..... S/. 14.080

Financiado por ..... S/. 0.00

TOTAL..... S/. 14.080

4.3. Cronograma de actividades

Se expresa mediante la diagramación Gantt en software especializado en el que se especifica las actividades en función del tiempo de ejecución.



	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		**Elaboracion de Plan de Tesis**	**107 días**	**jue 14/10/21**	**vie 11/03/22**
2		Inicio	0 días	jue 14/10/21	jue 14/10/21
3		**Desarroollo del Proyecto**	**73 días**	**jue 14/10/21**	**lun 24/01/22**
4		Fase de Concepto	8 días	jue 14/10/21	sáb 23/10/21
5		Fase de Planificacion	15 días	lun 25/10/21	vie 12/11/21
6		Fase de Diseño	15 días	lun 15/11/21	vie 3/12/21
7		Fase de Elaboración	31 días	lun 6/12/21	lun 17/01/22
8		Fase de Cierre	5 días	mar 18/01/22	lun 24/01/22
9		**Elacoboracion del Informe del Tesis**	**10 días**	**mar 25/01/22**	**lun 7/02/22**
10		**Revision de Tesis y Levantamiento de Observaciones**	**19 días**	**mar 8/02/22**	**vie 4/03/22**
11		**Sustentacion y Defensa de Tesis**	**5 días**	**lun 7/03/22**	**vie 11/03/22**
12		**Fin**	**0 días**	**lun 14/03/22**	**lun 14/03/22**

Imagen 2: Diagrama de Gantt

Fuente: Elaboración propia

Bibliografía

Arenas, F., Lagos , M., & Hidalgo, R. (Octubre de 2010). *Los riesgos naturales en la planificación territorial.* Chile: Pontifica Universidad Católica de Chile.

Arias Reyes, Y. L., Diaz Rodriguez, 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.

Casares, I., Martí, S. J., & Lizarzaburu Bolaños, E. (2016). *Introducción a la gestión Integral de riesgos empresariales Enfoque: ISO 31000.* Lima: Platinum Editorial S.A.C.

Ccesa 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.

Gómez Rivadeneira, A. (2014). Marco conceptual y legal sobre la gestión. *Monitor Estrategico*, 1-8.

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.

ISO73. (2009). GUIDE 73 Risk management - Vocabulary.

Jhuéz , J. (2015). Metodologías para la gestión de riesgo. *J.JHuéz Internacional*, 46.

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

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

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: Universidada Nacional Autonoma de Mexico .

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 estandar 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 conocimineto sobre caracterización y monitoreo de amenazas del volcán Tungurahua en el Cantón Baños.* Ecuador: Escuela Politecnica Nacional.

Kerlinger, F. N., Lee, H. B., Pineda, L. E., & Mora Magaña, I. (2002). Investigación del comportamiento.

ANEXO 01

Matriz de consistencia

Título: Evaluación de la gestión de riesgos para el Data Center de la DISA basada en la ISO 31000, Andahuaylas 2019

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 DISA basada en la ISO 31000?	Evaluar la gestión de riesgos para el Data Center de la DISA basado en la ISO 31000.	D1: Establecer contexto del Data Center	I1: Objetivos definidos
			I2: Estrategias definidas
			I3: Responsables asignados
			I4 : Procesos identificados
			I5: Recursos identificados
		D2: Identificar riesgos del Data Center	I1: Riesgos internos
			I2: Riesgos externos
			I3: Fuentes de riesgo
			I4: Zonas de impacto
Problemas específicos:	**Objetivos específicos:**	D3: Analizar riesgos en el Data Center	I1: Controles de gestión de riesgo
a) ¿Cómo es el contexto del Data Center de la DISA basado en la ISO 31000?	a) Evaluar el contexto del Data Center de la DISA basado en la ISO 31000		I2: Probabilidad de ocurrencia
b) ¿Cómo es la identificación de los riesgos para el Data Center de la DISA basado en la ISO 31000?	b) Evaluar la identificación de los riesgos para el Data Center de la DISA basado en la ISO 31000		I3 : Causas
c) ¿Cómo es el análisis de los riesgos para el Data Center de la DISA basado en la ISO 31000?	c) Evaluar el análisis de los riesgos para el Data Center de la DISA basado en la ISO 31000		I4: Consecuencias
d) ¿Cómo es la evaluación de los riesgos priorizados para el Data Center de la DISA basado en la ISO 31000?	d) Evaluar los riesgos priorizados para el Data Center de la DISA basado en la ISO 31000	D4: Evaluar riesgos del Data Center	I1: Riesgos priorizados
			I2 : Actividades de reducción
			I3: Toma de decisiones
Población		**Técnica - Instrumento**	
El tamaño de la población es el total de personas en la DISA		Encuesta – cuestionario	
Muestra		**Diseño de la investigación**	
Se trabajó con toda la población		Diseño no experimental – nivel descriptivo	

ANEXO 02

MARCO ESTRATÉGICO DE TI

Como resultado del diagnóstico realizado, se definen los componentes estratégicos en el marco de las TI.

Misión

"Proveer servicios de TI a la DISA, de alta calidad y confiabilidad, que incrementen la eficiencia y seguridad de la información y contribuyan al logro de los objetivos institucionales; utilizando el concepto de innovación como principal política de gestión".

Objetivos y Estrategias TI

En el siguiente cuadro se muestra un (01) objetivo general y cuatro (04) objetivos específicos, definidos sobre la base de las estrategias que buscan aprovechar las fortalezas y oportunidades para mejorar el estado de debilidad y mitigar el posible impacto de las amenazas detectadas.

Cuadro N° 9: Objetivos y Estrategias TI

Objetivo General TI	Objetivo Especifico TI	Estrategias TI
Fortalecer la gestión de servicios de TI para mejorar la calidad y eficiencia de Tecnologías de Información en la DISA.	OE1. Contribuir a posicionar como una institución superior universitaria basada en las TI.	• Contar con una plataforma institucional de interacción virtual (software y hardware). • Aumentar la oferta académica virtual de la DISA en un 80% de cursos con interacción virtual. • Integrar las plataformas de cursos en línea existentes en la DISA.
	OE2. Gestionar la calidad y seguridad de la información.	• Extender el alcance al Sistema de Gestión de la Seguridad de la información (SGSI) para los procesos que soportan la misión de la DISA. • Fortalecer el control interno y la seguridad de la información, mediante el establecimiento de políticas en materia de TI.
	OE3. Modernizar la infraestructura y soluciones TI que garanticen la continuidad, seguridad y eficiencia de las operaciones de la DISA.	• Perfeccionar la arquitectura tecnológica de la DISA haciendo uso eficiente de tecnologías modernas que procuren la disponibilidad y continuidad de los servicios. • Apoyar el emprendimiento y la innovación mediante la Implementación de una plataforma para búsqueda de proyectos informáticos.
	OE4. Gestionar de manera eficaz y eficiente los servicios que brinda la Oficina de Sistemas de Información.	• Implementar herramientas de Software que brinden soporte integrado a los procesos de atención a usuarios procurando reducir los niveles de complejidad y que estén alineados a las mejores prácticas de ITIL.

ANEXO 03

Alineamiento Estratégico entre los objetivos TI y el PEI

Los objetivos TI están alineados a las acciones estratégicas AEI 04.03 "Equipos informáticos y de comunicación implementados de manera permanente en la DISA" y AEI 04.05 “Sistemas de gestión automatizados con enfoque de procesos en la DISA”, del objetivo estratégico institucional OEI4 del PEI "Fortalecer la gestión institucional", tal como se aprecia en la siguiente tabla:

Cuadro N° 10: Alineamiento PETI - PEI

PETI 2019-2021			PEI 2019-2021	
COD.	**OBJETIVOS ESPECIFICOS TI**	**OBJETIVO GENERAL TI**	**COD.**	**OBJETIVO DEL PEI**
OE1.	Contribuir a desarrollar una institución competitiva basada en las TICs	Fortalecer la gestión de servicios de TI para mejorar la calidad y eficiencia de tecnologías de información en la DISA.	OE1.	Fortalecer la formación académica integral, con enfoque intercultural de los estudiantes.
OE2.	Gestionar la calidad de la información Incrementar la seguridad de la información.		OE2.	Fortalecer la gestión de la investigación científica, tecnológica e innovación en la comunidad universitaria.
OE3.	Modernizar la infraestructura y soluciones TI que garanticen la continuidad, seguridad y eficiencia de las operaciones de la DISA.		OE3.	Fortalecer las actividades de proyección social y extensión universitaria y los servicios culturales en beneficio de la comunidad.
OE4.	Gestionar de manera eficaz y eficiente los servicios que brinda y requiere la Oficina de Sistemas de Información.		OE4. AEI.04.03 AEI.04.05	Fortalecer la gestión institucional. Equipos informáticos y de comunicación implementados de manera permanente en la DISA. Sistemas de gestión automatizados con enfoque de procesos en la DISA.
			OE5.	Implementar la gestión integral de riesgo de desastres.