



UNIVERSIDAD ANDINA
NÉSTOR CÁCERES VELÁSQUEZ
ESCUELA DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN: DERECHO CIVIL Y EMPRESARIAL



**APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA
DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN
EN CAJAS DE AHORRO Y CRÉDITO
JULIACA - 2024**

TESIS PRESENTADA POR:
MIRIAM YANETH LUPACA VALERIANO

PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN DERECHO
MENCIÓN: DERECHO CIVIL Y EMPRESARIAL

JULIACA - PERÚ

2025



UNIVERSIDAD ANDINA
NÉSTOR CÁCERES VELÁSQUEZ
ESCUELA DE POSGRADO
MAESTRÍA EN DERECHO
MENCIÓN: DERECHO CIVIL Y EMPRESARIAL
APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA
DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN
EN CAJAS DE AHORRO Y CRÉDITO
JULIACA - 2024

TESIS PRESENTADA POR:
MIRIAM YANETH LUPACA VALERIANO

PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN DERECHO
MENCIÓN: DERECHO CIVIL Y EMPRESARIAL
APROBADA POR:

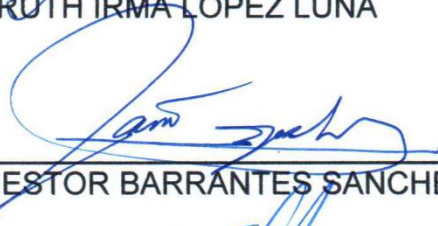
PRESIDENTE

:


Dra. RUTH IRMA LOPEZ LUNA

PRIMER MIEMBRO

:


Dr. NESTOR BARRANTES SANCHEZ

SEGUNDO MIEMBRO

:


Dr. RAMIRO ALMILCAR BOLAÑOS CALDERON

ASESOR DE TESIS

:


Dra. YENNY ROSARIO ACERO APAZA

LÍNEA DE INVESTIGACIÓN

: DERECHO PRIVADO – P38



TESIS UANCV

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ" ESCUELA DE POSGRADO



VICERRECTORADO DE
INVESTIGACIÓN

"OFICINA DE INVESTIGACIÓN"



RESOLUCIÓN DIRECTORAL N°0229-2025-D-EPG-UANCV/J

Juliaca, 07 de julio del 2025

VISTOS:

El expediente N° 2025-05690 presentado por el (la) Bachiller: **MIRIAM YANETH LUPACA VALERIANO** quien solicita nominación de jurados, fecha y hora de sustentación de tesis, en la Escuela de Posgrado de la Universidad Andina "Néstor Cáceres Velásquez".

CONSIDERANDO:

Que, el (a) Bachiller: **MIRIAM YANETH LUPACA VALERIANO** con número de DNI 73586893 con número de matrícula 1810200352 ha solicitado asignación de jurados, Fecha y hora de sustentación de la Tesis Titulada: **APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024**, para optar el GRADO de: **MAESTRO EN DERECHO** Mención: **DERECHO CIVIL Y EMPRESARIAL** de la Escuela de Posgrado de la Universidad Andina Néstor Cáceres Velásquez;

Que, de conformidad con lo previsto en el artículo 18° del Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos, **COMITÉ DE INVESTIGACIÓN**;

Que, mediante Resolución N°644-2024 -USA-EPG/UANCV SE APRUEBA Y AUTORIZA LA EJECUCION DE LA PROPUESTA DE INVESTIGACION y con Resolución N°1136-2024-USA-EPG/UANCV, se APRUEBA y AUTORIZA EL INFORME FINAL DE LA INVESTIGACIÓN (BORRADOR DE TESIS) Titulada: **APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024**. La misma que pertenece a la Línea de Investigación: **DERECHO PRIVADO – P38**;

Que, al habérselo cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos en su artículo 28° **DE LA SUSTENTACIÓN**.

Y estando, la opinión favorable del Director de la Unidad de Investigación y el Director de la Escuela de Posgrado mediante acta de sorteo de jurado, con registro N° 000204 de fecha: 04 de julio de 2025 se nombra jurados.

Que, conforme al artículo 66° del Reglamento General de la Escuela de Posgrado de la UANCV, establece que la Tesis de Posgrado es un trabajo de investigación científica original de actualidad y de alto valor científico;

En uso de las atribuciones conferidas a la Dirección en el inciso "J" del artículo 17° del Reglamento General de la Escuela de Posgrado, y el artículo 76° del Estatuto Universitario;

SE RESUELVE:

ARTÍCULO PRIMERO. - DECLARAR APTO para la sustentación presencial del **INFORME FINAL DE LA INVESTIGACIÓN** (borrador de tesis), **TITULADO: APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024**, del (la) Bach: **MIRIAM YANETH LUPACA VALERIANO**, para optar el GRADO de: **MAESTRO EN DERECHO** Mención: **DERECHO CIVIL Y EMPRESARIAL**, en virtud de los considerandos expuestos.

ARTÍCULO SEGUNDO. - NOMINAR JURADOS para la sustentación presencial y defensa de la tesis a los siguientes docentes ordinarios:

Presidente	: Dra. RUTH IRMA LOPEZ LUNA
Primer miembro	: Dr. NESTOR BARRANTES SANCHEZ
Segundo miembro	: Dr. RAMIRO AMILCAR BOLAÑOS CALDERON
Asesor	: Dra. YENNY ROSARIO ACERO APAZA

ARTÍCULO TERCERO. - PROGRAMAR FECHA Y HORA de sustentación como se detalla:

Fecha	: Miércoles, 16 de julio del 2025
Hora	: 2:30 p.m..
Lugar	: Aula N°309 EPG-UANCV-JULIACA

ARTÍCULO CUARTO. - El Director de la Escuela de Posgrado queda encargado del cumplimiento de la presente Resolución.

Regístrese, comuníquese y archívese.



UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
ESCUELA DE POSGRADO

Dr. Javier Romulo Quispe Zapana
DIRECTOR (a)



UNIVERSIDAD ANDINA

"NÉSTOR CÁCERES VELÁSQUEZ"

ESCUELA DE POSGRADO

RESOLUCIÓN DIRECTORAL N° 007-2025-CP-EPG-UANCV/J

Juliaca, 08 mayo del 2025

VISTOS:

El acuerdo del Consejo de la Escuela de Posgrado de la Universidad Andina "Néstor Cáceres Velásquez" en su sesión ordinaria presencial de fecha 07 de mayo del 2025.

CONSIDERANDO:

Que, de conformidad con lo previsto por el artículo 18° de la Constitución Política del Perú, concordante con el artículo 8° y 43° de la Ley Universitaria N° 303220, artículo 11° del Estatuto Universitario de la Autonomía de la Universidad Andina "Néstor Cáceres Velásquez" de Juliaca, artículo 5° del Reglamento General de la Escuela de Posgrado;

Que, el Estatuto de Universitario de la UANCV aprobado mediante Resolución N° 0018-2020-UANCV-AU-R en su artículo 73° establece: La Escuela de Posgrado tiene como órgano de dirección al Consejo de Posgrado integrados por los Directores de las unidades de posgrado de cada Facultad;

Que, el artículo 12° del Reglamento General de la Escuela de Posgrado, de las funciones y atribuciones del Consejo de Posgrado literal m) pronunciarse sobre otros asuntos académicos y administrativos de la Escuela de Posgrado no previstos;

Que, es función del Director cumplir y hacer cumplir los acuerdos de la Asamblea Universitaria, Consejo Universitario y Consejo de Posgrado, mediante la emisión de resoluciones de Consejo de Posgrado y de la Dirección.

Que, conforme a los artículos 19° 20° y 21° del reglamento general de la Escuelas de posgrado, establece que, son funciones del coordinado *"desempeñar otras funciones inherentes para la buena marcha del programa a su cargo"*

Que, la Superintendencia Nacional de Educación Superior Universitaria (SUNEDU) mediante Resolución del Consejo Directivo N° 034-2020-SUNEDU/CD, deniega la licencia institucional a la Universidad Andina Néstor Cáceres Velásquez, garantizando en todo momento la continuidad de la prestación de servicio educativo y la consecuente emisión de grados y títulos (...);

Estando, al acuerdo del Consejo de Posgrado y en uso de las facultades que le confiere la Ley Universitaria 30220, Ley de creación de la UANCV N° 23738 y modificatoria, atribuciones conferidas al Consejo de Posgrado en su artículo 12° del Reglamento General de la Escuela de Posgrado, y el Art. 73° del Estatuto Universitario;

SE RESUELVE:

ARTÍCULO PRIMERO. - AUTORIZAR, al Director de la Escuela de Posgrado Dr. JAVIER ROMULO QUISPE ZAPANA, COORDINADORES Y DIRECTOR DE INVESTIGACIÓN de la Escuela de Posgrado, para que puedan asumir con las firmas en el libro de actas de sustentaciones de tesis, empastes y otros documentos pendientes en los Programas de Doctorados, Maestría y Segundas Especialidades Profesionales, que dejaron los docentes que han cesado en sus funciones y aquellos que hayan fallecido y/o no tengan vínculo laboral con la Universidad Andina "Néstor Cáceres Velásquez".

ARTÍCULO SEGUNDO. - ELEVAR, la presente resolución a Consejo Universitario de la Universidad Andina "Néstor Cáceres Velásquez" de Juliaca para su ratificación.

ARTÍCULO TERCERO. - ENCARGAR, el cumplimiento de la presente resolución a Rectorado, Vicerectorado Administrativo, Vicerectorado Académico, Oficina de Informática, Registro Central y Oficinas Administrativas de la EPG, para su cumplimiento.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
ESCUELA DE POSGRADO
Dr. Javier Romulo Quispe Zapana
DIRECTOR (e)



TESIS UANCV



UNIVERSIDAD ANDINA
"NÉSTOR CÁCERES VELÁSQUEZ"
ESCUELA DE POSGRADO



VICERRECTORADO DE
INVESTIGACIÓN

"OFICINA DE INVESTIGACIÓN"



RESOLUCIÓN DIRECTORAL N° 01136-2024-USA-EPG/UANCV

Juliaca, 14 de Agosto de 2024

VISTOS:

El Expediente N° 2024-08649 de fecha 17 de Julio de 2024, el (la) Bach. MIRIAM YANETH LUPACA VALERIANO, con DNI N° 73586893, código de matrícula N° 1810200352, quien solicita Revisión de Informe Final de la Investigación (borrador de Tesis); **INFORME N° 00261-2024-UI-EPG-UANCV** y el Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)" del 05 de Agosto de 2024, que fue revisada por el Comité de Investigación de la Escuela de Posgrado.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, con Expediente N° 2024-08649 el (la) Bach. MIRIAM YANETH LUPACA VALERIANO, solicita la revisión y aprobación del Informe Final de la Investigación (borrador de Tesis) titulado: **APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024**. Línea de investigación **DERECHO PRIVADO - P38**, para optar el **GRADO de MAESTRO EN DERECHO** con mención en: **DERECHO CIVIL Y EMPRESARIAL**.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución N° 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión **FAVORABLE** al Informe Final de la Investigación (borrador de Tesis).

Que, el Director de la Unidad de Investigación de la Escuela de Posgrado, corroboró el asesoramiento en el Informe Final de la Investigación (borrador de Tesis) del **ASESOR Dra. YENNY ROSARIO ACERO APAZA**; y,

Estando, la opinión favorable del Comité de Investigación, según **INFORME N° 00261-2024-UI-EPG-UANCV** y el Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)" en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución N° 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria N° 30220, Ley de Creación de la UANCV N° 23738 y Modificatoria N° 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Escuela de Posgrado.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR EL INFORME FINAL DE LA INVESTIGACIÓN (BORRADOR DE TESIS) para la **REVISIÓN DE SIMILITUD TURNITIN**, titulado: **APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024**, presentado por el (la) Bach. MIRIAM YANETH LUPACA VALERIANO, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RATIFICAR, como **ASESOR** al (a) **Dra. YENNY ROSARIO ACERO APAZA**.

ARTICULO TERCERO. - DISPONER que la Escuela de Posgrado, la Secretaría Académica y administrativa, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.



UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
ESCUELA DE POSGRADO

Dr. Leopoldo Wenceslao Córdova Carr
DIRECCIÓN (e)



TESIS UANCV



VICERRECTORADO DE INVESTIGACIÓN

"OFICINA DE INVESTIGACIÓN"



UNIVERSIDAD ANDINA

"NÉSTOR CÁCERES VELÁSQUEZ"

ESCUELA DE POSGRADO



RESOLUCIÓN DIRECTORAL N° 644-2024-USA-EPG/UANCV

Juliaca, 14 de junio de 2024

VISTOS:

El Expediente N° 2024-061 de fecha 30 de mayo de 2024 el (la) Bach. MIRIAM YANETH LUPACA VALERIANO, con DNI N° 73588893, código de matrícula N° 1810200352, quien solicita Revisión de propuesta de Investigación; **INFORME N° 0056-2024-UI-EPG-UANCV** y el Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación" del 06 de junio de 2024, que fue revisada por el Comité de Investigación de la Escuela de Posgrado.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, con Expediente N° 2024-06763 el (la) Bach. MIRIAM YANETH LUPACA VALERIANO, solicita la revisión y aprobación de la propuesta de investigación titulado: **APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024**, Línea de investigación **DERECHO PRIVADO - P38**, para optar el GRADO de **MAESTRO EN DERECHO** con mención en: **DERECHO CIVIL Y EMPRESARIAL**.

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos dictado en la Resolución N° 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión **FAVORABLE** a la propuesta de investigación.

Que, el Director de la Unidad de Investigación de la Escuela de Posgrado, corroboró la propuesta del **ASESOR Dra. YENNY ROSARIO ACERO APAZA**, quien debe estar acreditado y facultado para orientar y ayudar al asesorado en el proceso de elaboración del trabajo de investigación (Tesis) de acuerdo a la **DIRECTIVA N° 004-2019-UANCV-VRAD-OI**; y.

Estando, la opinión favorable del Comité de Investigación, según **INFORME N° 0058-2024-UI-EPG-UANCV** y el **Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación"** en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución N° 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria N° 30220, Ley de Creación de la UANCV N° 23738 y Modificatoria N° 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Escuela de Posgrado.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR LA EJECUCIÓN DE LA PROPUESTA DE INVESTIGACIÓN, titulado: APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024, presentado por el (la) Bach. MIRIAM YANETH LUPACA VALERIANO, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RECONOCER, como ASESOR al Dra. YENNY ROSARIO ACERO APAZA.

ARTICULO TERCERO.- DISPONER que la Escuela de Posgrado, la Secretaría Académica y administrativa, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.



UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
ESCUELA DE POSGRADO

Dr. Leopoldo Wenceslao Condori Cari
DIRECTOR (a)



APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024

INFORME DE ORIGINALIDAD

25%

INDICE DE SIMILITUD

22%

FUENTES DE INTERNET

12%

PUBLICACIONES

16%

TRABAJOS DEL
ESTUDIANTE

FUENTES PRIMARIAS

1

Submitted to Universidad Andina Nestor
Caceres Velasquez

Trabajo del estudiante

4%

2

Submitted to utn

Trabajo del estudiante

1%

3

repositorio.udl.edu.pe

Fuente de Internet

1%

4

alicia.concytec.gob.pe

Fuente de Internet

1%

5

repositorio.autonoma.edu.pe

Fuente de Internet

1%

6

repositorio.puce.edu.ec

Fuente de Internet

1%

7

repositorio.utn.edu.ec

Fuente de Internet

1%

8

repositorio.uisek.edu.ec

Fuente de Internet

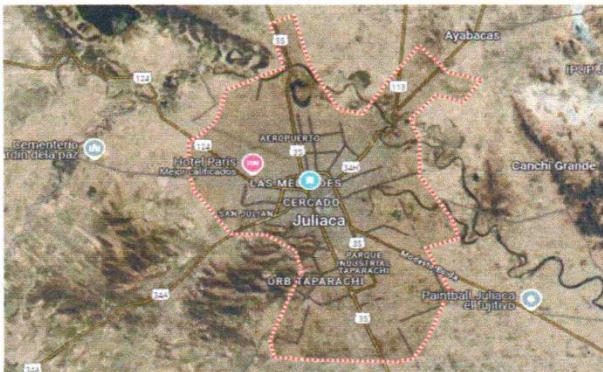
1%



Metadatos complementarios - UANCV

Título de la Tesis	
APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024	
Datos de autor	
Nombres y Apellidos	MIRIAM YANETH LUPACA VALERIANO
Tipo de documento de identidad	DNI
Número de documento de identidad	73586893
URL de ORCID	https://orcid.org/0009-0000-6781-3899
Datos de asesor	
Nombres y apellidos	YENNY ROSARIO ACERO APAZA
Tipo de documento de identidad	DNI
Número de documento de identidad	01324434
URL de ORCID	https://orcid.org/0000-0002-9783-7733
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	RUTH IRMA LOPEZ LUNA
Tipo de documento	DNI
Número de documento de identidad	29524013
URL de ORCID	https://orcid.org/0000-0003-0721-4362
Miembro del jurado 1	
Nombres Y Apellidos	NESTOR BARRANTES SANCHEZ
Tipo de documento	DNI
Número de documento de identidad	02389922
URL de ORCID	https://orcid.org/0000-0001-6965-6831



Miembro del jurado 2	
Nombres Y Apellidos	RAMIRO ALMILCAR BOLAÑOS CALDERON
Tipo de documento	DNI
Número de documento de identidad	29565004
URL de ORCID	https://orcid.org/0000-0003-4274-3040
Datos de investigación	
Línea de investigación	Derecho Privado – P38
Grupo de investigación	No aplica.
Agencia de financiamiento	Sin financiamiento.
Ubicación geográfica de la investigación	CAJAS DE AHORRO Y CRÉDITO JULIACA País: Perú Departamento: Puno Provincia: San Román Distrito: Juliaca Coordenadas Longitud: -15.499078211070485 Latitud: -70.13088653792708 https://maps.app.goo.gl/kWNep2yEpkwpx3L67 
Año o rango de años en que se realizó la investigación	Enero del 2024 – Julio del 2025
URL de disciplinas OCDE https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html - Librería	Derecho https://purl.org/pe-repo/ocde/ford#5.05.00 Derecho penal https://purl.org/pe-repo/ocde/ford#5.05.02



UNIVERSIDAD ANDINA VICEPRESIDENCIA VICEPRESIDENCIA
ESCUELA DE POSTGRADO
Dr. Jesús Mamani Mamani
DIRECTOR
DE INVESTIGACIÓN - EPG



DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo Miriam Vaneth Lupaca Valeriano identificado con DNI
Nro. 73 586893 en mi condición de egresado de:

- ☐ Escuela Profesional
☐ Programa de Segunda Especialidad,
☒ Programa de Maestría o Doctorado

Maestría en Derecho

informo que he elaborado el/la ☒ Tesis o ☐ Trabajo de Investigación, ☐ Trabajo Académico
denominada:

"Aplicación de la norma ISO 27001 en el sistema de
gestión de seguridad de información en cajas de
ahorro y crédito Juliaca - 2024"

Asesorado por: Dra. Yenny Rosario Acero Apaza

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como tuyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia, a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca 05 de Diciembre del 2025

FIRMA (ASESOR)

FIRMA (obligatoria)



Huella



TESIS UANCV



VICERRECTORADO DE
INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"



DEDICATORIA

A mis padres, quienes me enseñaron el valor del esfuerzo y la perseverancia. Su amor incondicional y su apoyo constante han sido mi mayor motivación.

A mi familia, por su comprensión y paciencia durante este viaje académico.

A mis amigos, por estar siempre a mi lado y brindarme su apoyo en los momentos más difíciles.

A mis profesores y mentores, cuya guía y conocimiento han sido fundamentales para la culminación de esta tesis.



AGRADECIMIENTO

Agradezco profundamente a Dios por darme la fuerza y la sabiduría necesarias para alcanzar esta meta.

A mis padres, por su inquebrantable amor, apoyo y sacrificio. Gracias por creer en mí y por darme las herramientas necesarias para avanzar.

A mis hermanos, por su constante ánimo y por ser una fuente de inspiración en mi vida.

A mis amigos, por su compañía y por los momentos compartidos que hicieron este camino más llevadero.

A mis profesores y tutores, especialmente al, por su orientación, paciencia y valiosos consejos a lo largo de este proceso. Su dedicación y experiencia han sido cruciales para el desarrollo de esta investigación.



ÍNDICE GENERAL

DEDICATORIA.....	iii
AGRADECIMIENTO.....	iv
ÍNDICE GENERAL	v
ÍNDICE DE TABLAS	vii
INDICE DE FIGURAS	viii
RESUMEN.....	ix
ABSTRACT	x
INTRODUCCIÓN	xi

CAPITULO I

PROBLEMA

1.1. EXPOSICIÓN DE LA PROBLEMÁTICA	1
1.2. FORMULACIÓN DEL PROBLEMA.....	4
1.2.1. Problema General	4
1.2.2. Problemas Específicos	4
1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN	4
1.4. OBJETIVOS DE LA INVESTIGACIÓN	6
1.4.1. Objetivo general	6
1.4.2. Objetivos Específicos	7

CAPITULO II

MARCO TEORICO REFERENCIAL

2.1. ANTECEDENTES DE LA INVESTIGACIÓN	8
2.1.1. A nivel Internacional	8
2.1.2. A Nivel Nacional	11
2.1.3. A nivel Local	14
2.2. BASES TEÓRICAS	14
2.2.1. Definición de las normas ISO 27001.....	14
2.2.2. Importancia de la Norma ISO 27001	15
2.2.3. Gestión de riegos	17
2.2.4. Estándar Internacional	18
2.2.5. Definición de Control de Seguridad de Información	19
2.2.6. Clases de control de seguridad de información.....	20



2.2.7. Dimensiones del Control de Seguridad de Información	22
2.3. VARIABLES.....	23
2.3.1. Variable 01	23

CAPITULO III

PROCEDIMIENTOS METODLOGICOS DE LA INVESTIGACION

3.1. ENFOQUE DE LA INVESTIGACIÓN.....	24
3.2. MÉTODO DE INVESTIGACIÓN	24
3.3. TIPO DE INVESTIGACIÓN	25
3.4. NIVEL DE INVESTIGACIÓN.....	25
3.5. DISEÑO DE INVESTIGACIÓN	25
3.6. POBLACIÓN Y MUESTRA	25
3.6.1. Población.....	25
3.6.2. Muestra.....	25
3.7. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.....	26
3.7.1. Técnicas	26
3.7.2. Instrumentos.....	27
3.8. CONFIABILIDAD Y VALIDEZ DEL INSTRUMENTO.....	27
3.9. PROCEDIMIENTO DE TRATAMIENTOS DE DATOS	28

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS INFERENCIALES	29
4.1.1. Objetivo Especifico 01.....	29
4.1.2. Objetivo Especifico 02.....	35
4.1.3. Objetivo Especifico 03.....	41
4.1.4. Objetivo General	46
4.2. DISCUSIÓN DE RESULTADOS.....	48

CONCLUSIONES

RECOMENDACIONES

REFERENCIAS BIBLIOGRÁFICAS

ANEXOS



ÍNDICE DE TABLAS

Tabla 2 Dimensión Confidencialidad	29
Tabla 3 Total Dimensión Confidencialidad	33
Tabla 4 Dimensión Integridad	35
Tabla 5 Total Dimensión Integridad	39
Tabla 6 Dimensión Disponibilidad	41
Tabla 7 Total Dimensión Disponibilidad	44
Tabla 8 Total, Conocimiento de la ISO 27001	46



INDICE DE FIGURAS

Figura 1 Dimensión de confidencialidad	31
Figura 2 Total Dimensión Confidencialidad	33
Figura 3 Dimensión Integridad	37
Figura 4 Total Dimensión Integridad	39
Figura 5 Dimensión Disponibilidad.....	42
Figura 6 Total Dimensión Disponibilidad.....	44
Figura 7 Total, Conocimiento de la ISO 27001.....	46



RESUMEN

El objetivo general fue Determinar la aplicación de la Norma ISO 27001 en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024. La metodología se utilizó fue de enfoque cualitativo como método fue el deductivo de tipo básica, nivel descriptivo de diseño no experimental – transversal, se utilizó como muestra a 10 cajas de ahorro y crédito Juliaca 2024, para la recolección de datos se utilizó como técnica la encuesta e instrumento el cuestionario para la variable ISO 27001 el instrumento debidamente validado, en el análisis e interpretación de resultados se usó el Software IBM SPSS v.23, y los programas Microsoft Word y Excel. Los resultados en la dimensión confidencialidad muestra un resultado regular con el (70%), con una minoría indicando malo con (30%). En la dimensión integridad muestra una escala de regular con (50%), con un 30% consideran buena y un 20% mala, en la dimensión disponibilidad muestra una escala de Regular con el (60%), con un 20% que la considera buena y un 10% considera excelente y un 10% la califica como mala. Por lo que se concluye que la percepción predominante en las dimensiones de confidencialidad, disponibilidad e integridad se ubican en la categoría regular en cuanto a la aplicación de la Norma ISO 27001 en el sistema de gestión de seguridad de información en cajas de ahorro y crédito Juliaca - 2024.

Palabras Clave: Aplicación, Norma, ISO 27001, microfinanzas, Juliaca 2024.



ABSTRACT

The general objective was to determine the application of the ISO 27001 Standard in the continuous improvement of the information security management system in the Juliaca 2024 savings and credit banks. The methodology used was a qualitative approach as the method was the basic deductive type. , descriptive level of non-experimental - transversal design, 10 Juliaca 2024 savings and credit banks were used as a sample, for data collection the survey was used as a technique and the questionnaire for the variable ISO 27001 was used as a duly validated instrument, in For the analysis and interpretation of results, IBM SPSS v.23 software and Microsoft Word and Excel programs were used. The results in the confidentiality dimension show a regular result with (70%), with a minority indicating bad with (30%). In the integrity dimension it shows a scale of regular with (50%), with 30% considering it good and 20% considering it bad, in the availability dimension it shows a scale of Regular with (60%), with 20% considering it. good and 10% consider it excellent and 10% rate it as bad. Therefore, it is concluded that the predominant perception in the dimensions of confidentiality, availability and integrity are located in the regular category in terms of the application of the ISO 27001 Standard in the information security management system in Juliaca savings and credit banks. - 2024.

Keywords: Application, Standard, ISO 27001, microfinance, Juliaca 2024.



INTRODUCCIÓN

El presente informe de investigación titulado **APLICACIÓN DE LA NORMA ISO 27001 EN LA MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN LAS CAJAS DE AHORRO Y CRÉDITO JULIACA 2024**. La seguridad de la información se ha convertido en un eje fundamental para el funcionamiento de las organizaciones modernas, especialmente en un entorno donde la digitalización avanza con rapidez y las amenazas cibernéticas se vuelven cada vez más sofisticadas. En este contexto, la Norma ISO 27001 representa uno de los estándares internacionales más reconocidos y utilizados para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su finalidad es asegurar que la información, considerada hoy uno de los activos más valiosos, se proteja adecuadamente en términos de confidencialidad, integridad y disponibilidad.

Las cajas de ahorro y crédito, por manejar datos financieros altamente sensibles, se encuentran entre las instituciones más expuestas a incidentes de seguridad. Por ello, la aplicación eficaz de la ISO 27001 constituye un elemento clave para el fortalecimiento de sus procesos internos, la prevención de riesgos y la consolidación de la confianza de sus usuarios. La ciudad de Juliaca, cuyo dinamismo económico ha impulsado el crecimiento de estas entidades, constituye un escenario propicio para evaluar el grado de implementación de este estándar y su contribución a la mejora del SGSI durante el año 2024.

En el ámbito internacional, diversos estudios han demostrado que la adopción de la ISO 27001 contribuye significativamente a elevar los niveles de protección de datos, optimizar los procedimientos y establecer una cultura organizacional



orientada a la seguridad digital. En el contexto nacional, investigaciones recientes resaltan que las entidades financieras peruanas han incrementado su interés por adoptar este estándar; sin embargo, aún se enfrentan a limitaciones asociadas a la capacitación del personal, la gestión del riesgo y la actualización tecnológica. A nivel local, investigaciones preliminares evidencian que, si bien existe intención de implementar buenas prácticas de seguridad, el proceso se encuentra en etapas iniciales, lo que evidencia la necesidad de contar con un diagnóstico más preciso y actualizado.

El presente estudio se estructura en seis capítulos que abordan los elementos esenciales del proceso investigativo.

- El **Capítulo I** desarrolla el planteamiento de la problemática, la formulación del problema general y específico, así como la justificación teórica, práctica y metodológica.
- En el **Capítulo II** se detallan el objetivo general y los objetivos específicos que orientan la investigación.
- El **Capítulo III** presenta el marco teórico, donde se revisan antecedentes nacionales e internacionales, y se profundiza en los conceptos que sustentan la aplicación de la norma ISO 27001.
- El **Capítulo IV** expone las variables y sus dimensiones.
- El **Capítulo V** describe la metodología utilizada, precisando el enfoque, tipo, nivel y diseño de investigación, además de la población, muestra y técnicas de recolección de datos.



- Finalmente, el **Capítulo VI** contiene los resultados obtenidos, su análisis, la discusión correspondiente, así como las conclusiones y recomendaciones derivadas del trabajo.

Este estudio busca, en suma, aportar una visión clara sobre la situación actual de la gestión de la seguridad de la información en las cajas de ahorro y crédito de Juliaca y valorar en qué medida la aplicación de la Norma ISO 27001 contribuye a fortalecer sus procesos y garantizar una protección eficaz de los datos que administran.

.



TESIS UANCV



VICERRECTORADO DE
INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"



CAPITULO I

PROBLEMA

1.1. EXPOSICIÓN DE LA PROBLEMÁTICA

En los últimos años, la seguridad de la información se ha convertido en un desafío urgente para organizaciones de todo el mundo. Diversos estudios internacionales evidencian un incremento preocupante de incidentes cibernéticos que afectan tanto a instituciones financieras como a empresas de distintos sectores. Por ejemplo, investigaciones como las desarrolladas por el Repositorio Institucional de la Universidad Piloto de Colombia (2022) revelan que los ataques informáticos ocurren, en promedio, cada 39 segundos, utilizando técnicas como *phishing*, *malware*, *spam* y *ransomware*. Este escenario se agudiza debido a la insuficiencia de políticas efectivas de seguridad digital, lo que deja a los usuarios y a las entidades vulnerables ante amenazas constantes.

Asimismo, en América Latina, una encuesta elaborada por Microsoft (Morales, 2022) durante la pandemia evidenció que el 31% de las grandes empresas reportaron un incremento significativo de ciberataques, sobre todo en el sector bancario y en empresas dedicadas a la consultoría. A pesar de ello, solo un 27% de estas organizaciones proporciona a sus



trabajadores equipos configurados con medidas de seguridad adecuadas; en la mayoría de los casos, las labores se realizan con dispositivos personales, lo que eleva notablemente el riesgo de exposición y vulneración de datos.

En el caso peruano, antes de la pandemia, muchas pequeñas y medianas empresas (PYMES) no consideraban necesaria la inversión en seguridad de la información, ya que no se percibían como objetivos frecuentes de ataques. No obstante, la digitalización acelerada de procesos internos durante la emergencia sanitaria reveló múltiples vulnerabilidades aprovechadas por ciberdelincuentes (Rossi, 2021). En este contexto, ataques como el *phishing* aumentaron un 49% entre 2020 y 2021, afectando principalmente a entidades del rubro financiero y consultorías, de las cuales solo un 20% tomó acciones para fortalecer su seguridad (Seguridad América, 2022).

La norma ISO 27001 establece lineamientos para la gestión de los activos de información, abarcando desde documentos físicos y digitales hasta infraestructura tecnológica como servidores, equipos móviles, estaciones de trabajo y aplicaciones. Su correcta identificación y gestión permiten implementar medidas de protección adecuadas (Guerrero, 2022).

Sin embargo, en el contexto local de Juliaca se evidencia una problemática particular. Las cajas de ahorro y crédito almacenan información histórica en dispositivos externos como discos duros portátiles o unidades USB, sin contar con un sistema centralizado de respaldo. Esto dificulta el acceso oportuno a datos críticos y expone la información a daños físicos, deterioro, pérdida o accesos no autorizados. Además, el inadecuado resguardo de



estos dispositivos, muchas veces almacenados en lugares vulnerables o climáticamente inestables, aumenta el riesgo de incidentes.

La ausencia de controles de seguridad alineados con la norma ISO 27001 genera riesgos significativos, entre los que destacan:

- **Vulneración de datos sensibles de los clientes**, como información financiera, datos personales y transacciones, cuya exposición tendría repercusiones legales y reputacionales.
- **Pérdida de integridad de la información**, lo cual podría traducirse en manipulación de registros, errores operativos o inconsistencias en las transacciones financieras.
- **Incumplimiento de normativas vigentes**, incluyendo requisitos de protección de datos personales y regulaciones financieras que exigen mecanismos robustos de seguridad.
- **Desconfianza de los usuarios**, quienes podrían optar por entidades más seguras ante incidentes o fallas en la protección de su información.

Esta situación justifica la necesidad de evaluar cómo se está aplicando la Norma ISO 27001 en las cajas de ahorro y crédito de Juliaca, con el fin de identificar brechas, riesgos y oportunidades de mejora que permitan fortalecer su sistema de gestión de seguridad de la información y garantizar procesos confiables, seguros y eficientes.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema General

PG: ¿Como se aplica la Norma ISO 27001 en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024?

1.2.2. Problemas Específicos

PE1: ¿Como se describe la aplicación de la Norma ISO 27001 en la dimensión confidencialidad e la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024?

PE2: ¿Como caracterizar la aplicación de la Norma ISO 27001 en la dimensión integridad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024?

PE3: ¿Como se describe la aplicación de la Norma ISO 27001 en la dimensión disponibilidad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

La presente investigación se justifica porque aborda una necesidad real y urgente dentro del ámbito financiero: la protección de los datos sensibles que administran las cajas de ahorro y crédito. Estas instituciones manejan información altamente confidencial —como datos personales, registros financieros y movimientos económicos— que, de ser vulnerados, podrían generar pérdidas económicas, sanciones legales y un deterioro significativo de la confianza de los clientes. La Norma ISO 27001 ofrece un



marco internacionalmente validado que permite identificar, gestionar y reducir los riesgos asociados a la seguridad de la información, por lo que su aplicación resulta esencial para garantizar un entorno operativo confiable.

Desde una **perspectiva teórica**, la investigación cobra relevancia porque contribuye al estudio y aplicación de modelos de gestión de seguridad de la información basados en estándares internacionales. La ISO 27001 no solo establece lineamientos claros para la protección de datos, sino que también fortalece el diseño de políticas internas, la gestión del riesgo y la toma de decisiones estratégicas. Además, su implementación se relaciona con principios fundamentales de la Ley de Protección de Datos Personales del Perú (Ley N.º 29733), lo que permite analizar la coherencia entre las normativas nacionales e internacionales.

En cuanto a la **justificación práctica**, el estudio permitirá identificar el estado actual del sistema de gestión de seguridad de la información en las cajas de ahorro y crédito de Juliaca y reconocer las principales vulnerabilidades que enfrentan. Con ello, las instituciones podrán fortalecer sus controles de acceso, mejorar sus mecanismos de protección contra amenazas cibernéticas y optimizar la administración de sus activos de información. Implementar la ISO 27001 también favorece el cumplimiento regulatorio y refuerza la confianza del usuario, aspecto fundamental para la continuidad y competitividad del sector financiero.

Asimismo, la certificación en esta norma puede representar una **ventaja** competitiva, ya que evidencia un compromiso institucional con la seguridad y la calidad del servicio. En un contexto donde los clientes buscan



entidades confiables, la adopción de ISO 27001 se convierte en un valor agregado que permite diferenciarse de otras organizaciones que aún no cuentan con un sistema de seguridad formalizado.

Desde el punto de vista **metodológico**, la investigación es pertinente porque emplea un proceso de diagnóstico, análisis y evaluación que permitirá comprender a profundidad la situación actual de las cajas de ahorro y crédito respecto a la seguridad de la información. Esta evaluación inicial facilita la identificación de riesgos, la priorización de vulnerabilidades, el diseño de controles adecuados y la formulación de recomendaciones que servirán como base para futuras investigaciones y para la posible implementación de un Sistema de Gestión de Seguridad de la Información conforme a la Norma ISO 27001.

Finalmente, el estudio genera un aporte significativo para la comunidad académica y profesional, ya que proporciona evidencia empírica sobre la aplicación de un estándar internacional en un contexto local, ofreciendo información útil para la toma de decisiones, el fortalecimiento institucional y el desarrollo de nuevas líneas de investigación en materia de seguridad de la información.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general

OG: Determinar la aplicación de la Norma ISO 27001 en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.



1.4.2. Objetivos Específicos

OE1: Describir la aplicación de la Norma ISO 27001 de la dimensión confidencialidad e la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.

OE2: Caracterizar la aplicación de la Norma ISO 27001 de la dimensión integridad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.

OE3: Describir la aplicación de la Norma ISO 27001 de la dimensión disponibilidad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.



CAPITULO II

MARCO TEORICO REFERENCIAL

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. A nivel Internacional

Chicaiza (2020), en su estudio titulado *Implementación del SGSI basado en la Norma ISO/IEC 27001*, tuvo como objetivo analizar el estado de seguridad del área de tecnologías de una entidad financiera para proponer mejoras en la gestión de la información. La investigación se desarrolló mediante entrevistas, encuestas y observación in situ, lo que permitió identificar amenazas y vulnerabilidades relacionadas con la integridad y disponibilidad de los datos. Como resultado, se determinó que existían deficiencias en el control de accesos y en la gestión de activos informáticos, lo que motivó el diseño de políticas de seguridad ajustadas a la normativa. El autor concluyó que la aplicación de la ISO 27001 contribuye a establecer lineamientos claros para proteger la información, siempre que exista coherencia con los límites institucionales y un compromiso organizacional para implementar las mejoras propuestas.

Por su parte, Sánchez (2021) desarrolló la investigación *Modelo de gestión de seguridad de la información para cooperativas de ahorro y crédito de*



Guayaquil, cuyo propósito fue optimizar las prácticas de seguridad en pequeñas entidades financieras. A través de una metodología mixta que incluyó revisión documental, entrevistas y análisis situacional mediante matriz FODA, se identificaron debilidades en los procesos de gestión de riesgos y en la inexistencia de controles estandarizados. Los resultados mostraron que estas cooperativas carecían de políticas claras alineadas con la norma ISO 27001. En sus conclusiones, el autor señala que la implementación del modelo basado en esta norma permite reducir la exposición al riesgo, mejorar la protección de la información y fortalecer la toma de decisiones estratégicas.

Asimismo, Núñez (2022), en su trabajo *Auditoría informática a la Cooperativa de Ahorro y Crédito Riobamba Ltda.*, se propuso evaluar el nivel de seguridad de los sistemas de información mediante auditorías basadas en el marco COSO II e instrumentos como entrevistas, cuestionarios y encuestas dirigidas al personal. Los resultados evidenciaron niveles de confianza del 86.90% y 96.96% en ciertos componentes del sistema, pero también revelaron la ausencia de socialización de políticas de uso, así como la falta de evaluación del SGSI bajo ISO 27001. El autor concluyó que es imprescindible implementar medidas correctivas y fortalecer el marco de control para salvaguardar los recursos tecnológicos, involucrando activamente a todo el personal en la mejora continua.

En otra contribución relevante, Pazmiño (2019), en su investigación *Política de seguridad de la información para la Cooperativa Chibuleo basada en ISO/IEC 27002:2013*, buscó establecer lineamientos de seguridad para la división de TI de la cooperativa. Mediante un diagnóstico situacional,



identificación de riesgos y análisis de la norma ISO 27002, se determinaron las vulnerabilidades más críticas. El estudio concluyó con la elaboración de una política integral de seguridad, recomendando su aprobación institucional para asegurar su aplicación y difusión entre los empleados. El autor concluyó que la estandarización de controles mitigaría eventos de alto riesgo y fortalecería la cultura organizacional de seguridad.

Finalmente, Granada (2019), en *Diseño del Sistema de Gestión de Seguridad de la Información conforme a la INEN-ISO/27001*, tuvo como objetivo desarrollar un SGSI para una organización tecnológica, siguiendo una metodología basada en NIST 800-30 y herramientas como Nessus, Nmap y listas de verificación. La investigación permitió identificar múltiples vulnerabilidades y formular estrategias de tratamiento del riesgo. Granada concluyó que un SGSI alineado con ISO 27001 proporciona un marco sólido para garantizar la continuidad de las operaciones y elevar la madurez en seguridad de la información, siempre que se continúe con la implementación progresiva de los controles.

Rodriguez (2020) El propósito del estudio fue evaluar cómo la implementación de la norma ISO 27001 afectó la seguridad de los datos en poder de una empresa privada de Lima, Perú. Se utilizó como metodología un estudio pre-experimental para determinar el efecto de la aplicación de la norma ISO 27001. Esto se logró mediante el uso de una metodología cuantitativa. Los hallazgos demuestran, entre otras cosas, la necesidad de administrar información vital que puede ser esencial para los intereses estratégicos de las empresas. La conclusión cuantitativa indica que el uso

de ISO tiene un efecto en la seguridad de la información, incluyendo la confidencialidad y disponibilidad.

Pinto (2021) El objetivo del proyecto, es crear un sistema de gestión de seguridad de la información que cumpla con los estándares ISO/IEC 27001:2013. El diseño del sistema ha establecido la metodología de gestión de riesgos, inventario de actividades, identificación de vulnerabilidades, evaluación de riesgos y establecimiento de controles. Los resultados demuestran cómo garantizar la confidencialidad, la integridad y la accesibilidad de la información y las organizaciones de apoyo, asegurando la continuación de los negocios como de costumbre, ya que las buenas prácticas descritas en la norma ISO 27002 complementan la gestión de la seguridad de la información. Se concluye que el sistema de gestión diseñado se transforma en una herramienta para aumentar la madurez, ayudando a la organización a reducir riesgos y sirviendo como pilar para el establecimiento de una cultura de seguridad de la información.

2.1.2. A Nivel Nacional

Calderón (2021), en su tesis titulada *Auditoría interna y el Sistema de Gestión de Seguridad de la Información en la Caja Municipal de Tacna*, tuvo como propósito determinar la relación entre ambas variables durante el año 2020. Mediante un diseño no experimental y correlacional, aplicó dos cuestionarios validados por expertos a una muestra de 100 colaboradores. Los resultados mostraron una correlación moderada ($r = 0.4966$) entre la auditoría interna y el SGSI, destacándose la disponibilidad como la dimensión más relevante dentro de la seguridad de la información. El autor concluyó que fortalecer los procesos de auditoría interna contribuye a

mejorar el desempeño del SGSI, principalmente en lo referente al acceso, disponibilidad y protección de los activos de información

Por su parte, Yaguar (2021), en su investigación *Plan de ciberseguridad basado en ISO 27001 para el centro de datos de la Cooperativa de Ahorro y Crédito 1 de Julio*, tuvo como objetivo diseñar una propuesta de seguridad alineada a la norma internacional para fortalecer la protección de la infraestructura tecnológica. Utilizó una metodología mixta compuesta por entrevistas y encuestas al personal responsable de TI. Los resultados permitieron identificar que la institución no aplicaba adecuadamente las políticas de seguridad en sus operaciones, evidenciando vulnerabilidades en la gestión de recursos, procedimientos de acceso y control de incidentes. El autor concluyó que el plan basado en ISO 27001 representa una guía efectiva para reducir riesgos, mejorar la continuidad operativa y fortalecer la seguridad del centro de datos.

Asimismo, Navarro (2021), en su estudio *Sistema de Gestión de Seguridad de la Información para el área de operaciones del Banco Sullana*, se propuso desarrollar un SGSI tomando como referencia los lineamientos de la norma ISO 27001 y las buenas prácticas del PMBOK. Su metodología incluyó entrevistas y encuestas dirigidas al personal del área de operaciones, lo que permitió identificar brechas en el control de accesos, gestión de incidentes y manejo de información crítica. Los resultados evidenciaron la necesidad de implementar controles estandarizados para evitar vulneraciones y mejorar la capacidad de respuesta institucional. Navarro concluyó que la ISO 27001 proporciona una base sólida para regular los flujos de información y garantizar la protección de los activos más sensibles del banco.

En otra contribución, Moscaiza (2020), en su estudio *Modelo de gestión de seguridad de la información para la Cooperativa ABC*, tuvo como finalidad diseñar un sistema de seguridad conforme a la norma ISO 27001:2013. La investigación utilizó una metodología descriptiva basada en el análisis de documentos, revisión de normativas, diagnóstico institucional y evaluación de riesgos. Los resultados identificaron falencias significativas en la gestión de incidentes, monitoreo de accesos y políticas internas. El autor concluyó que la aplicación de un modelo SGSI fortalece la capacidad de la organización para mitigar riesgos y cumplir con los requisitos regulatorios vigentes.

Finalmente, Cumpa (2020), en su tesis *Sistema de Gestión de Seguridad de la Información para pymes de Chiclayo basado en ISO 27001*, planteó como objetivo elaborar un modelo aplicable a pequeñas y medianas empresas con recursos limitados. A través de encuestas y análisis situacional, identificó debilidades en la protección de activos tecnológicos, falta de capacitación del personal y ausencia de procedimientos formales para la gestión de la información. Los resultados demostraron que la adecuación de la norma ISO 27001 a las características de las pymes permite elevar sus niveles de seguridad, reducir vulnerabilidades y mejorar la confiabilidad de sus sistemas. El autor concluyó que, aun con limitaciones presupuestales, es posible aplicar controles efectivos que contribuyan a la seguridad integral de la información.

Aleman (2024) el objetivo del presente estudio, que buscó determinar cuánto afectó la implementación de la norma ISO 27001:2013 al control de la

seguridad de la información en una determinada organización. La metodología fue enfoque cuantitativo diseño experimental luego, utilizando como guía mediciones con las dimensiones definidas de la variable dependiente, se realizó un análisis de resultados. Esto fue aprobado por el juicio de tres expertos. Teniendo en cuenta una prueba de distribución no normal no paramétrica, los resultados de la prueba posterior fueron menos significativos que los resultados de la prueba previa en un nivel de significación de 0,5, se concluye la norma ISO 27001:2013 mejorará la seguridad de la información en las empresas de consultoría privadas.

2.1.3. A nivel Local

No se encontraron antecedentes relacionados al estudio en el ámbito local

2.2. BASES TEÓRICAS

2.2.1. Definición de las normas ISO 27001

La Norma ISO 27001 es un estándar internacional que establece los requisitos necesarios para implementar y gestionar un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización. Según Steve (2019), esta norma constituye un marco de referencia que orienta a las instituciones en la protección de sus activos de información, considerando procesos, recursos tecnológicos y documentos físicos o digitales que puedan verse expuestos a riesgos. Su propósito central es garantizar que la información permanezca confidencial, íntegra y disponible, mediante un conjunto de políticas, procedimientos y controles que permiten gestionar las amenazas de manera sistemática.

De acuerdo con Kalambkar (2021), la ISO 27001 se centra en promover un enfoque estructurado y basado en procesos, lo que implica planificar, implementar, monitorear y mejorar continuamente las prácticas de seguridad. Este enfoque facilita la identificación de riesgos, la evaluación de vulnerabilidades y la adopción de medidas preventivas o correctivas, asegurando que las organizaciones puedan anticiparse a incidentes que comprometan la información. Además, establece lineamientos que favorecen una cultura institucional orientada a la protección de datos, en la que la gestión de riesgos se convierte en un elemento esencial para la toma de decisiones.

La norma puede aplicarse en cualquier tipo de organización, independientemente de su tamaño o sector, lo que la convierte en un instrumento versátil y ampliamente adoptado a nivel global. Su implementación no solo contribuye al fortalecimiento de la seguridad interna, sino que también permite demostrar a clientes, entidades reguladoras y socios comerciales el compromiso de la organización con estándares reconocidos internacionalmente. Asimismo, la ISO 27001 puede ser certificada por organismos acreditados, quienes verifican que la institución cumple con los requisitos establecidos, reforzando así la confianza y credibilidad en sus procesos de gestión de la información.

2.2.2. Importancia de la Norma ISO 27001

La Norma ISO 27001 es de especial relevancia porque proporciona un conjunto integral de lineamientos que permiten a las organizaciones proteger información sensible frente a amenazas internas y externas. Adidas (2019) señala que este estándar ofrece una estructura sólida para salvaguardar

datos críticos, entre ellos información financiera, registros de clientes y activos estratégicos que forman parte del funcionamiento institucional. En un entorno donde los ciberataques se incrementan de manera constante, contar con un marco formal de seguridad se convierte en un elemento esencial para minimizar riesgos y evitar pérdidas derivadas de accesos no autorizados, filtraciones o manipulación indebida de datos.

Asimismo, la norma contribuye al cumplimiento de leyes y regulaciones relacionadas con la protección y tratamiento adecuado de la información. En ese sentido, Aleman (2024) enfatiza que adoptar la ISO 27001 permite a las organizaciones alinearse con exigencias nacionales e internacionales, tales como disposiciones de protección de datos personales, normativas bancarias, estándares de privacidad y regulaciones específicas según cada sector. El cumplimiento normativo no solo evita sanciones, sino que fortalece la transparencia y la confianza entre la institución y sus usuarios.

Además, la ISO 27001 fomenta la implementación de controles preventivos y correctivos que mejoran la capacidad de respuesta frente a incidentes de seguridad. A través de la identificación, evaluación y tratamiento de riesgos, las organizaciones pueden anticiparse a vulnerabilidades, gestionar adecuadamente sus activos de información y asegurar la continuidad operativa. Esto se traduce en procesos más eficientes, reducción de errores, disminución de interrupciones y una administración más responsable de los recursos tecnológicos.

Finalmente, la certificación basada en la ISO 27001 se convierte en un distintivo competitivo, pues demuestra el compromiso institucional con altos

estándares de seguridad. Esto no solo eleva la reputación de la organización, sino que también fortalece la confianza de clientes, socios comerciales y entidades reguladoras, generando ventajas estratégicas frente a otras instituciones que aún no adoptan sistemas de gestión de seguridad formales.

2.2.3. Gestión de riesgos

La gestión de riesgos constituye uno de los pilares fundamentales de la Norma ISO 27001, ya que permite identificar, analizar y controlar las amenazas que pueden afectar la seguridad de la información dentro de una organización. Según Aleman (2024), este proceso implica reconocer de manera sistemática los factores que pueden comprometer los activos informáticos, evaluar su probabilidad de ocurrencia y estimar el impacto que tendrían en caso de materializarse. Al tratarse de un enfoque preventivo, la gestión de riesgos facilita adoptar medidas oportunas para mitigar vulnerabilidades, reducir la exposición a incidentes y fortalecer las defensas institucionales frente a ciberataques o fallas internas.

La norma propone un modelo estructurado que guía a las organizaciones a lo largo de varias etapas: identificación de activos, evaluación de amenazas potenciales, análisis de vulnerabilidades, valoración de riesgos y selección de controles adecuados para minimizar su efecto. Este proceso no se limita a aspectos tecnológicos, sino que abarca elementos humanos, físicos, administrativos y operativos, lo que permite una visión integral del entorno de seguridad. Además, la gestión de riesgos fomenta una cultura organizacional orientada a la prevención, donde las decisiones se basan en evidencia y se prioriza la continuidad de las operaciones.

Implementar este enfoque contribuye a fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI), ya que permite a la organización anticiparse a posibles incidentes, asignar mejor sus recursos, tomar decisiones estratégicas informadas y cumplir con normativas legales y estándares internacionales. En síntesis, la gestión de riesgos no solo protege los activos de información, sino que también optimiza la eficiencia institucional y garantiza un funcionamiento más seguro y confiable.

2.2.4. Estándar Internacional

La Norma ISO 27001 es reconocida a nivel mundial como el principal estándar para gestionar la seguridad de la información dentro de las organizaciones. Su carácter internacional permite que sus lineamientos sean aplicados en diversos sectores y países, lo que facilita la interoperabilidad, la mejora continua y la adopción de buenas prácticas globalmente aceptadas. Al ser un estándar ampliamente reconocido, ofrece una estructura uniforme que ayuda a las instituciones a implementar controles consistentes, comparables y alineados con los requisitos de seguridad que exigen los mercados internacionales.

Su aceptación global también fortalece la confianza entre las organizaciones y sus distintas partes interesadas, ya que demuestra el compromiso institucional con la protección de los datos y la gestión adecuada de los riesgos asociados. Asimismo, la adopción de un estándar internacional permite que las empresas se mantengan competitivas, ya que la certificación ISO 27001 funciona como un aval que garantiza la credibilidad y la solidez de los procesos de seguridad implementados.

En síntesis, la ISO 27001 trasciende fronteras al proporcionar una referencia universal para la gestión de la seguridad de la información, asegurando que las organizaciones cuenten con sistemas robustos, actualizados y alineados con las necesidades tecnológicas y regulatorias que demanda un entorno globalizado.

2.2.5. Definición de Control de Seguridad de Información

Villalón (2020) señala que los controles de seguridad de la información comprenden un conjunto estructurado de políticas, prácticas, procedimientos y medidas orientadas a proteger los datos de una organización, asegurando su confidencialidad, integridad y disponibilidad. Su finalidad esencial es mantener a salvo la información sensible frente a riesgos o amenazas internas y externas que puedan afectarla. Para ello, se emplean mecanismos técnicos, administrativos y físicos que contribuyen a reducir vulnerabilidades y garantizar que la información sea tratada conforme a las normativas y estándares vigentes. Entre los principales elementos que abarca este tipo de control se encuentran:

- **Confidencialidad:** asegurar que los datos solo sean accesibles para usuarios autorizados, evitando su exposición o divulgación indebida.
- **Integridad:** garantizar que la información se mantenga correcta, completa y sin alteraciones no autorizadas.
- **Disponibilidad:** procurar que los datos estén accesibles cuando los usuarios los requieran, evitando interrupciones o fallos que obstaculicen su uso.

- **Autenticación:** verificar adecuadamente la identidad de las personas o dispositivos que intentan acceder a la información, permitiendo el ingreso únicamente a quienes cuenten con autorización.
- **Autorización:** establecer y gestionar los niveles de acceso de cada usuario, asegurando que solo puedan visualizar o manipular la información necesaria para sus funciones.
- **Auditoría y monitoreo:** implementar sistemas que permitan registrar y supervisar las actividades relacionadas con los datos, con el fin de identificar comportamientos inusuales y actuar frente a posibles incidentes.
- **Gestión de riesgos:** analizar permanentemente las amenazas que puedan afectar la seguridad de la información y aplicar medidas preventivas o correctivas para reducir su impacto.

2.2.6. Clases de control de seguridad de información

Según Villalón (2020), la protección adecuada de la información requiere la aplicación de diferentes tipos de controles que se clasifican, de manera general, en tres grandes grupos: controles técnicos, controles administrativos y controles físicos. Cada categoría cumple funciones específicas dentro del sistema de seguridad y se complementan entre sí para garantizar una protección integral.

Los **controles técnicos** comprenden los mecanismos basados en tecnología que resguardan los sistemas y los datos. Entre ellos se encuentra el **control de acceso**, que regula quién puede ingresar a los recursos informáticos mediante procesos de autenticación, autorización, uso de contraseñas seguras y registros de actividad. También se incluye el **cifrado**,



que transforma la información sensible para que resulte ilegible a usuarios no autorizados, tanto cuando los datos están almacenados como cuando se transfieren. Otros controles técnicos abarcan los **firewalls y sistemas de seguridad de red**, encargados de bloquear amenazas externas mediante filtros, detección de intrusiones y protección contra malware. Asimismo, la **seguridad de aplicaciones** incorpora acciones como pruebas de penetración, actualización de parches y desarrollo seguro. Finalmente, la **detección y respuesta a incidentes** implica el uso de herramientas y protocolos destinados a identificar y atender eventos que puedan comprometer la seguridad.

Por otro lado, los **controles administrativos** corresponden a las políticas, normas y procesos que orientan el comportamiento del personal y la gestión interna de la información. Incluyen la elaboración de **políticas y procedimientos de seguridad**, la **gestión de riesgos** mediante la identificación de amenazas y la implementación de medidas de mitigación, y la **administración de identidades y accesos**, que regula los privilegios de cada usuario. De igual modo, abarca acciones de **capacitación y sensibilización** para que los empleados reconozcan posibles riesgos y sepan cómo actuar, así como la **gestión de incidentes**, que establece pasos claros para responder ante eventos que afecten la seguridad de la información.

Finalmente, los **controles físicos** se enfocan en proteger los espacios y equipos donde se almacena o procesa la información. Entre estos se encuentran las medidas de **seguridad física**, como cámaras de vigilancia, sistemas de control de ingreso a áreas restringidas y protección de la

infraestructura de TI. También se contempla la **custodia de los soportes de información**, asegurando el almacenamiento adecuado de copias de respaldo y dispositivos como discos duros o cintas. Además, la **gestión del hardware y software** implica controlar el acceso a los equipos y garantizar su correcto mantenimiento para evitar daños o manipulaciones no autorizadas.

2.2.7. Dimensiones del Control de Seguridad de Información

De acuerdo con Ladrón (2020), las dimensiones de la seguridad de la información representan los aspectos esenciales que deben considerarse para garantizar la adecuada protección de los datos dentro de una organización. Estas dimensiones permiten evaluar el grado de seguridad aplicado y orientar la implementación de controles que aseguren el funcionamiento confiable de los sistemas informáticos. Entre las principales dimensiones se encuentran la disponibilidad, la adaptabilidad o resiliencia, la accesibilidad y el resguardo de la información.:

2.2.7.1. Disponibilidad:

hace referencia a la capacidad de que los sistemas, servicios y datos estén operativos y accesibles cuando los usuarios autorizados los necesiten. Esta dimensión implica prevenir interrupciones no planificadas, como fallas técnicas, ataques cibernéticos o desastres naturales, asegurando la continuidad de los servicios esenciales.

2.2.7.2. Adaptabilidad (o Resiliencia):

se relaciona con la habilidad de los sistemas de información para reaccionar, ajustarse y recuperarse rápidamente frente a eventos que alteren su

funcionamiento normal. Esto incluye la preparación ante incidentes, la capacidad de respuesta y la implementación de estrategias que garanticen la continuidad del negocio ante situaciones adversas.

2.2.7.3. Accesibilidad:

por su parte, se centra en asegurar que solo las personas autorizadas puedan acceder a la información, mediante controles adecuados de autenticación, verificación de identidad y políticas de acceso. Esta dimensión evita que terceros no autorizados logren ingresar o manipular los datos.

Resguardo (o Salvaguardia).- comprende las medidas destinadas a proteger la información ante amenazas como el robo, la exposición no autorizada o la destrucción accidental o deliberada. Incluye acciones de protección tecnológica, física y administrativa que buscan mantener la seguridad y confiabilidad de los datos..

2.3. VARIABLES

2.3.1. Variable 01

Norma ISO 27001

- Dimensión Confidencialidad
- Dimensión Integridad
- Dimensión Disponibilidad



CAPITULO III

PROCEDIMIENTOS METODLOGICOS DE LA INVESTIGACION

3.1. ENFOQUE DE LA INVESTIGACIÓN

Esta investigación fue de enfoque cualitativo según Quispe et al. (2023) El enfoque cualitativo es un método de investigación utilizado en diversas disciplinas, especialmente en las ciencias sociales y humanidades, que se centra en entender los fenómenos desde una perspectiva holística y contextual. En lugar de cuantificar variables y analizar datos numéricos, el enfoque cualitativo se enfoca en las características y cualidades de los fenómenos estudiados, buscando comprender el "cómo" y el "por qué" de los comportamientos, experiencias y estructuras sociales.

3.2. MÉTODO DE INVESTIGACIÓN

El método aplicado fue el deductivo. Bernal (2010) lo describe como un sistema que clasifica las afirmaciones basándose en la calidad de las hipótesis y busca replicar o falsificar esas hipótesis al encontrar conexiones coherentes cuando se comparan con los resultados, yendo de lo específico a lo general (p.60).

3.3. TIPO DE INVESTIGACIÓN

Según Arias (2020), la investigación fue de carácter básico ya que no tiene aplicaciones prácticas inmediatas, y se enfoca en ampliar y profundizar el conocimiento científico existente relacionado con la realidad. Esto incluye examinar y perfeccionar las teorías científicas que fundamentan el estudio (p.43).

3.4. NIVEL DE INVESTIGACIÓN

Fue descriptivo porque se centra en la descripción de fenómenos, situaciones o eventos tal como se presentan naturalmente, sin manipular o controlar variables. El objetivo principal de la investigación descriptiva es obtener una imagen clara y precisa de un fenómeno o una población específica (Hernández et al., 2014, p.92).

3.5. DISEÑO DE INVESTIGACIÓN

Según Hernández (2014) la investigación no experimental como aquellos estudios que se realizan sin manipulación deliberada de variables, observando los fenómenos en sus entornos naturales para su análisis.

3.6. POBLACIÓN Y MUESTRA

3.6.1. Población

Para Arias (2020) la población es el conjunto de todos los factores de los que se ocupa el estudio. También se puede definir como el conjunto de todas las unidades de muestreo" la población estará conformado por todas las cajas municipales de ahorro y crédito de la ciudad de Juliaca – 2024.

3.6.2. Muestra

Para Barriento (2021) una muestra se refiere a un subconjunto seleccionado de una población más amplia. La población es el grupo total de elementos o

individuos que se estudian o se quieren analizar, mientras que la muestra es una porción representativa de esa población utilizada para realizar inferencias o generalizaciones sobre la misma. La muestra de estudio estará conformada por el total 10 cajas municipales de ahorro y crédito de la ciudad de Juliaca del presente año 2024.

Muestreo no probabilístico

Es una técnica de muestreo en la que los elementos de la población se eligen según su disponibilidad y conveniencia para el investigador. En este método, la selección de la muestra no se basa en ningún criterio estadístico, sino en la facilidad de acceso o en la conveniencia del investigador Quispe et al, (2024)

3.7. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.7.1. Técnicas

Encuesta.

a técnica principal utilizada para la recolección de información en esta investigación fue la **encuesta**, debido a su utilidad para obtener datos de manera directa, sistemática y eficiente a partir de un conjunto de participantes. Según Carrasco (2013), las técnicas constituyen el conjunto de procedimientos y lineamientos que orientan el trabajo del investigador durante el proceso de obtención de datos. En este sentido, la encuesta se reconoce como uno de los métodos más empleados en estudios sociales y organizacionales, ya que permite recopilar opiniones, percepciones y valoraciones de los sujetos involucrados de forma estructurada.

3.7.2. Instrumentos

Cuestionario

Para la recolección de datos se empleó como instrumento el **cuestionario**, el cual permitió registrar de manera estructurada las percepciones y valoraciones de los participantes respecto a la aplicación de la Norma ISO 27001. Hernández, Fernández y Baptista (2014) señalan que un instrumento de medición es la herramienta utilizada por el investigador para captar información sobre las variables que desea analizar, por lo que su diseño debe responder a criterios de claridad, coherencia y validez.

3.8. CONFIABILIDAD Y VALIDEZ DEL INSTRUMENTO

Para, Arias (2021). Para garantizar la calidad del instrumento aplicado en esta investigación, se evaluaron dos aspectos fundamentales: **la validez** y **la confiabilidad**. La **validez** hace referencia al grado en que el instrumento realmente mide la variable que se propone estudiar. En este caso, el cuestionario fue sometido a un proceso de **validación por juicio de expertos**, quienes revisaron la pertinencia, claridad y coherencia de cada ítem en relación con las dimensiones de la Norma ISO 27001. Los especialistas realizaron observaciones y sugerencias que permitieron ajustar el contenido, mejorando su precisión y adecuación al objetivo de la investigación.

Por otro lado, la **confiabilidad** se evaluó para asegurar que el instrumento produzca resultados estables y consistentes en condiciones similares. Para ello, se aplicó el coeficiente **alfa de Cronbach**, técnica ampliamente utilizada en estudios cuantitativos para medir la consistencia interna de los

ítems. El coeficiente obtenido se ubicó dentro de los valores aceptables, lo que indica que las preguntas presentan una adecuada correlación entre sí y que el instrumento es fiable para recopilar información sobre la aplicación de la Norma ISO 27001 en las cajas de ahorro y crédito.

Escala de confiabilidad

Escalabilidad	Nivel de confiabilidad
< a 0.9	Muy aceptable
Entre 0.8 a 0.89	Aceptable
Entre 0.7 a 0.79	Baja
> a 0.69	Inaceptable

Fuente: Arias (2021)

3.9. PROCEDIMIENTO DE TRATAMIENTOS DE DATOS

Para realizar el estudio, los datos teóricos se recopilaron utilizando técnicas y herramientas y la estadística descriptiva, luego se ingresaron en tablas y gráficos estadísticos. Estos datos luego serán tabulados para ser procesados estadísticamente de manera cualitativa, y en el curso se utilizó los programas Microsoft Word y Excel y otro software estadístico SSPS v 25 para determinar para ver insitu el comportamiento de la variable en el mismo lugar e los hechos



CAPITULO VI

ANALISIS DE RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS INFERENCIALES

4.1.1. Objetivo Especifico 01

Describir la aplicación de la Norma ISO 27001 de la dimensión confidencialidad e la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.

Tabla 1
Dimensión Confidencialidad

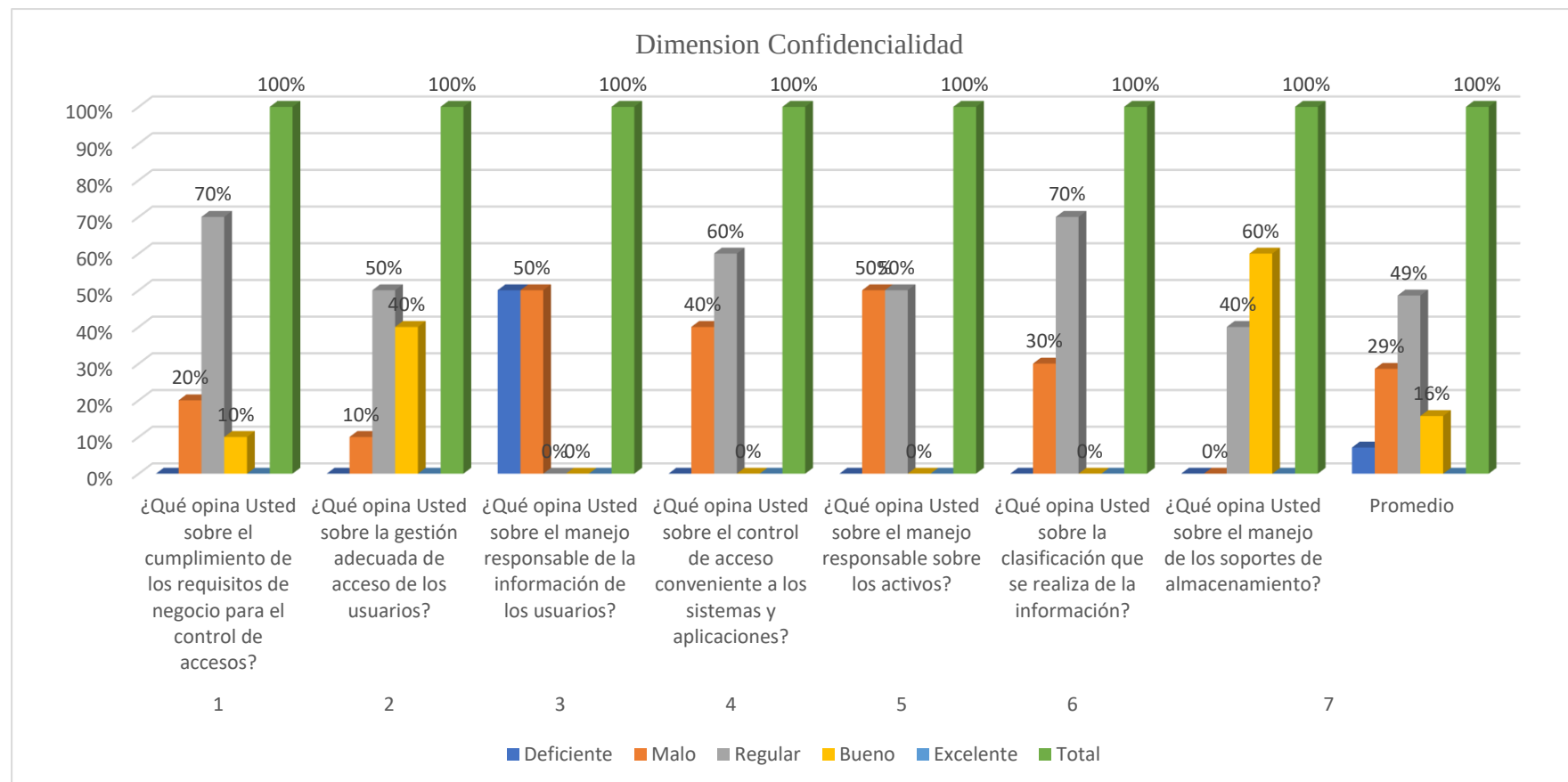
N a	Ítem Dimensión Confidencialida d	Deficient e				Malo				Regular				Bueno				Excelent e				Total	
		fi	%	fi	%	fi	%	fi	%	fi	%	fi	%	fi	%	fi	%	fi	%	fi	%	fi	%
	¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de	0	0%	2	20%	7	70%	1	10%	0	0%	10	100%										
1	accesos?																						
	¿Qué opina Usted sobre la gestión adecuada de acceso de los	0	0%	1	10%	5	50%	4	40%	0	0%	10	100%										
2	usuarios?																						
	¿Qué opina Usted sobre el manejo	5	50%	5	50%	0	0%	0	0%	0	0%	10	100%										
3	responsable de																						



la información de los usuarios?												
¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	0	0%	4	40%	6	60%	0	0%	0	0%	10	100%
4 ¿Qué opina Usted sobre el manejo responsable sobre los activos?	0	0%	5	50%	5	50%	0	0%	0	0%	10	100%
5 ¿Qué opina Usted sobre la clasificación que se realiza de la información?	0	0%	3	30%	7	70%	0	0%	0	0%	10	100%
6 ¿Qué opina Usted sobre el manejo de los soportes de almacenamient	0	0%	0	0%	4	40%	6	60%	0	0%	10	100%
7 o?												
Promedio				29	49	16					100	
		7%		%	%	%		0%			%	

Nota: se realizó según los datos recolectados

Figura 1
Dimensión de confidencialidad



Nota: Realizado según la tabla



Interpretación

Muestra la tabla según la tabla del ítem 01 Cumplimiento de los requisitos de negocio para el control de accesos: La mayoría considera que el cumplimiento de los requisitos de negocio para el control de accesos es "Regular" (70%), seguido por "Malo" (20%) y "Bueno" (10%). en el ítem Gestión adecuada de acceso de los usuarios: ítem 3 La opinión predominante es que la gestión adecuada de acceso de los usuarios es "Regular" (50%), con una apreciable cantidad de respuestas indicando "Bueno" (40%), y una minoría considerándolo "Malo" (10%). Ítem 4 Manejo responsable de la información de los usuarios: Las respuestas están divididas equitativamente entre "Deficiente" (50%) y "Malo" (50%), lo que indica una percepción general negativa sobre el manejo responsable de la información de los usuarios. Ítem 5 Control de acceso conveniente a los sistemas y aplicaciones: La mayoría considera que el control de acceso a los sistemas y aplicaciones es "Regular" (60%) y "Malo" (40%), sin calificaciones positivas. ítem 6 Manejo responsable sobre los activos: Las opiniones están divididas entre "Malo" (50%) y "Regular" (50%), lo que sugiere que hay una percepción de deficiencia en el manejo responsable de los activos. Ítem 7 Clasificación de la información: La mayoría considera la clasificación de la información como "Regular" (70%), con una minoría indicando "Malo" (30%). Manejo de los soportes de almacenamiento: Las opiniones son predominantemente positivas, con "Bueno" (60%) y "Regular" (40%).

Tabla 2

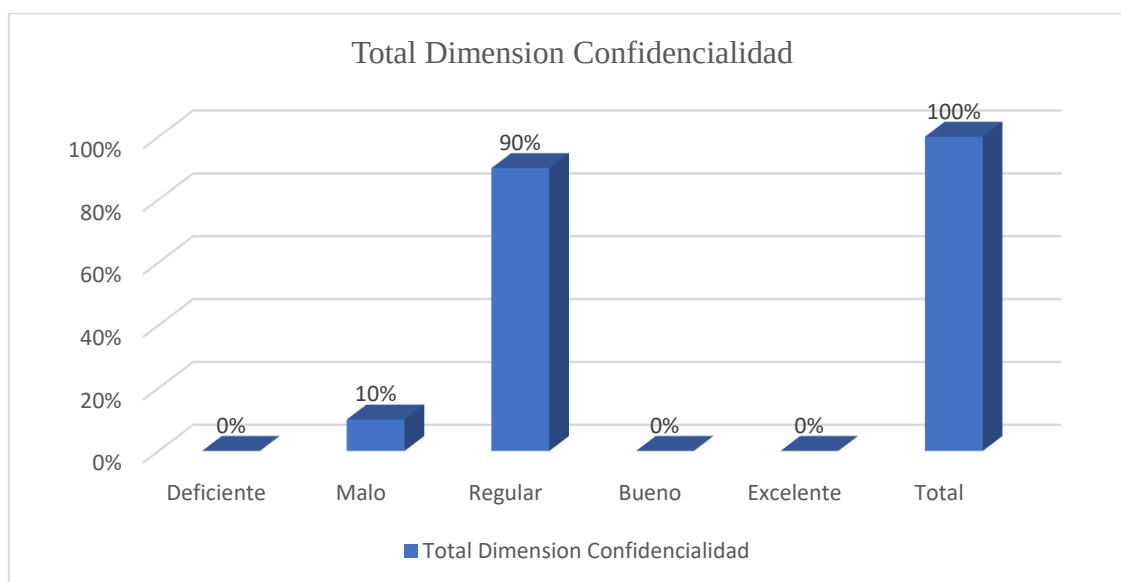
Total Dimensión Confidencialidad

		Fi	%
Total Dimensión Confidencialidad	Deficiente	0	0%
	Malo	1	10%
	Regular	9	90%
	Bueno	0	0%
	Excelente	0	0%
	Total	10	100%

Nota: se realizó según los datos recolectados

Figura 2

Total Dimensión Confidencialidad



Nota: Realizado según la tabla

Interpretación

Distribución General: La mayoría de las respuestas (90%) consideran que la confidencialidad es "Regular". Una minoría (10%) considera que es "Malo". No hay respuestas indicando "Deficiente", "Bueno" o "Excelente". La percepción general es que la confidencialidad en la organización es "Regular", lo que sugiere que, aunque no se considera inadecuada, hay margen para mejoras. La presencia de un 10% de respuestas calificando la confidencialidad como "Malo" indica que hay aspectos



específicos que necesitan ser atendidos para evitar que esta percepción negativa crezca.

La ausencia de respuestas en las categorías "Deficiente" y "Excelente" sugiere que no hay percepciones extremadamente negativas ni extremadamente positivas, reforzando la idea de que la confidencialidad se maneja de manera aceptable pero no sobresaliente. En resumen, aunque la confidencialidad es mayormente vista como adecuada (Regular), se requiere esfuerzo para elevar su calidad a niveles más altos y eliminar las percepciones negativas.

4.1.2. Objetivo Especifico 02

Caracterizar la aplicación de la Norma ISO 27001 de la dimensión integridad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.

Tabla 3

Dimensión Integridad

Nº	Ítem Dimensión Integridad	Deficiente		Malo		Regular		Bueno		Excelente		Total	
		fi	%	fi	%	fi	%	fi	%	fi	%	fi	%
8	¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	2	20%	3	30%	5	50%	0	0%	0	0%	10	100%
9	¿Qué opina Usted sobre la protección conveniente contra código malicioso?	4	40%	6	60%	0	0%	0	0%	0	0%	10	100%
10	¿Qué opina Usted sobre el manejo de copias de seguridad?	0	0%	7	70%	3	30%	0	0%	0	0%	10	100%
11	¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	0	0%	3	30%	7	70%	0	0%	0	0%	10	100%
12	¿Qué opina Usted sobre el control de software de explotación?	0	0%	4	40%	5	50%	1	10%	0	0%	10	100%
13	¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	0	0%	2	20%	5	50%	3	30%	0	0%	10	100%
14	¿Qué opina Usted sobre las consideraciones de la auditorías de	0	0%	3	30%	6	60%	1	10%	0	0%	10	100%

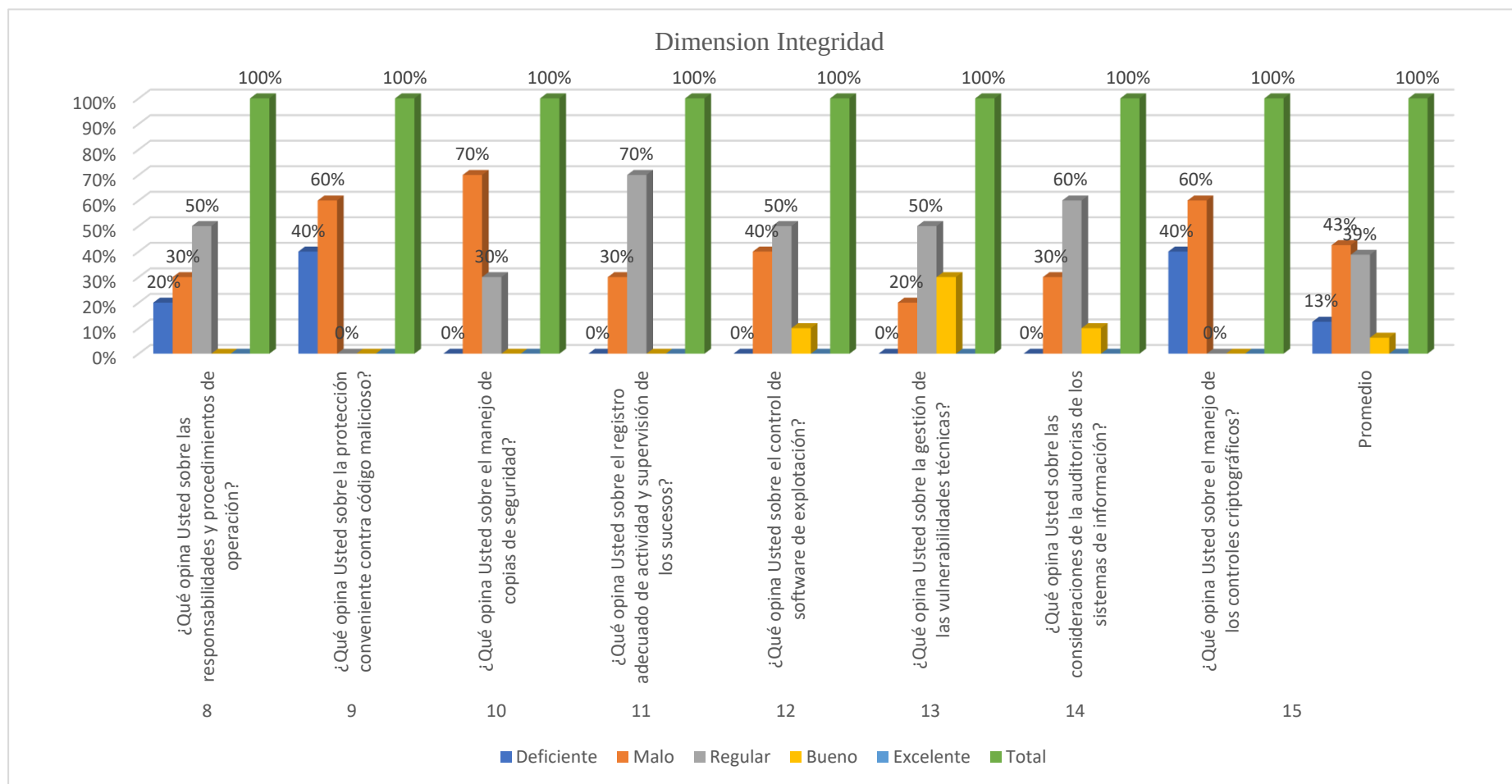


los sistemas de
información?

¿Qué opina Usted sobre el manejo de los controles 15 criptográficos?	4	40%	6	60%	0	0%	0	0%	0	0%	10	100%
Promedio		13%		43%		39%		6%		0%		100%

Nota: se realizó según los datos recolectados

Figura 3
Dimensión Integridad



Nota: Realizado según la tabla

Interpretación

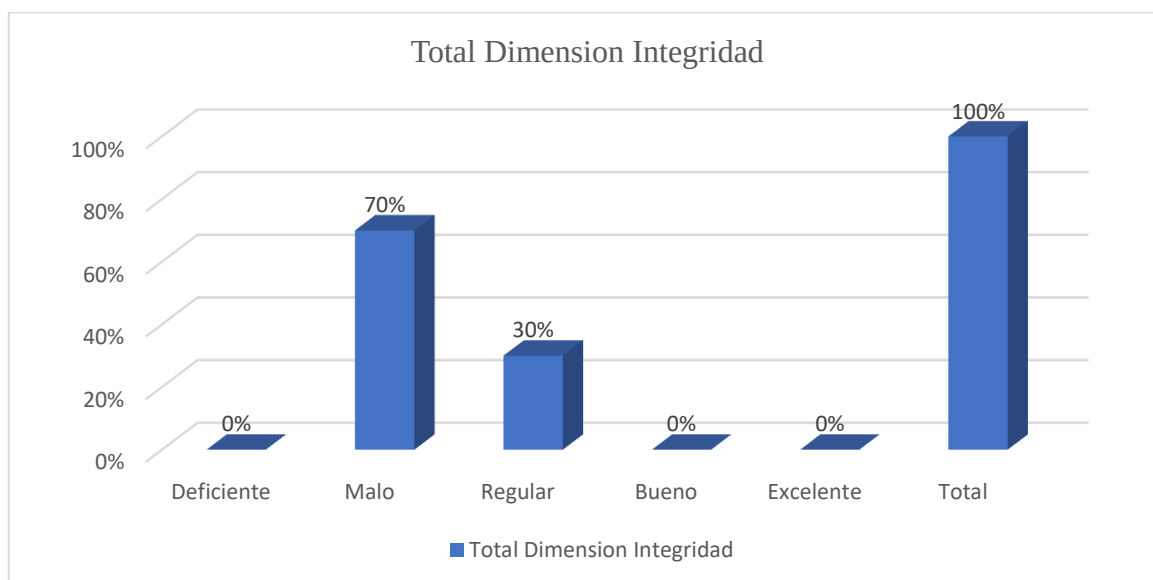
Muestra el resultado según el ítem: Responsabilidades y procedimientos de operación: La mitad de los encuestados consideran que las responsabilidades y procedimientos de operación son "Regulares" (50%). Un 30% los considera "Malos" y un 20% "Deficientes", lo que indica áreas significativas de mejora. Protección contra código malicioso: La percepción general es negativa, con el 100% de las respuestas indicando que la protección contra código malicioso es "Deficiente" (40%) o "Mala" (60%). Manejo de copias de seguridad: La mayoría de los encuestados consideran que el manejo de copias de seguridad es "Malo" (70%), con el resto opinando que es "Regular" (30%). Registro y supervisión de actividad: La mayoría considera que el registro y la supervisión de actividad son "Regulares" (70%), con un 30% que lo consideran "Malo". Control de software de explotación: La opinión predominante es que el control de software de explotación es "Regular" (50%), con un 40% que lo consideran "Malo" y un 10% "Bueno". Gestión de vulnerabilidades técnicas: La mayoría considera que la gestión de vulnerabilidades técnicas es "Regular" (50%), con un 30% que la consideran "Buena" y un 20% "Mala". Consideraciones de auditorías de sistemas de información: La mayoría considera las auditorías como "Regulares" (60%), con un 30% que las consideran "Malas. la mayoría de las áreas evaluadas en la dimensión de integridad necesitan mejoras significativas, especialmente en protección contra código malicioso y manejo de controles criptográficos. Las opiniones "Regulares" predominan, lo que sugiere que los sistemas y procedimientos actuales no son completamente inadecuados pero requieren optimización para alcanzar un nivel más alto de desempeño.

Tabla 4
Total Dimensión Integridad

		Fi	%
Total	Deficiente	0	0%
Dimensión	Malo	7	70%
Integridad	Regular	3	30%
	Bueno	0	0%
	Excelente	0	0%
	Total	10	100%

Nota: Realizado según la tabla

Figura 4
Total Dimensión Integridad



Nota: Realizado según la tabla

Interpretación

Muestra los resultados según la tabla la mayoría de las respuestas (70%) califican la integridad como "Malo". Un 30% de las respuestas califican la integridad como "Regular". No hay respuestas que indiquen que la integridad sea "Deficiente", "Buena" o "Excelente". Percepción Predominante: La percepción predominante es negativa, con una gran mayoría (70%) considerando que la integridad es "Mala". Una minoría (30%) percibe la integridad como "Regular", lo que indica que hay



algunos aspectos que funcionan adecuadamente, pero no de manera óptima.

Ausencia de Opiniones Extremas Positivas y Negativas:

La falta de respuestas en las categorías "Deficiente", "Bueno" y "Excelente" sugiere que los encuestados no consideran que la integridad esté en el extremo negativo (muy mala) ni en el positivo (muy buena). Esto refuerza la idea de que, aunque hay problemas significativos, no son percibidos como extremadamente graves ni existen áreas destacadas por su alta calidad.

4.1.3. Objetivo Especifico 03

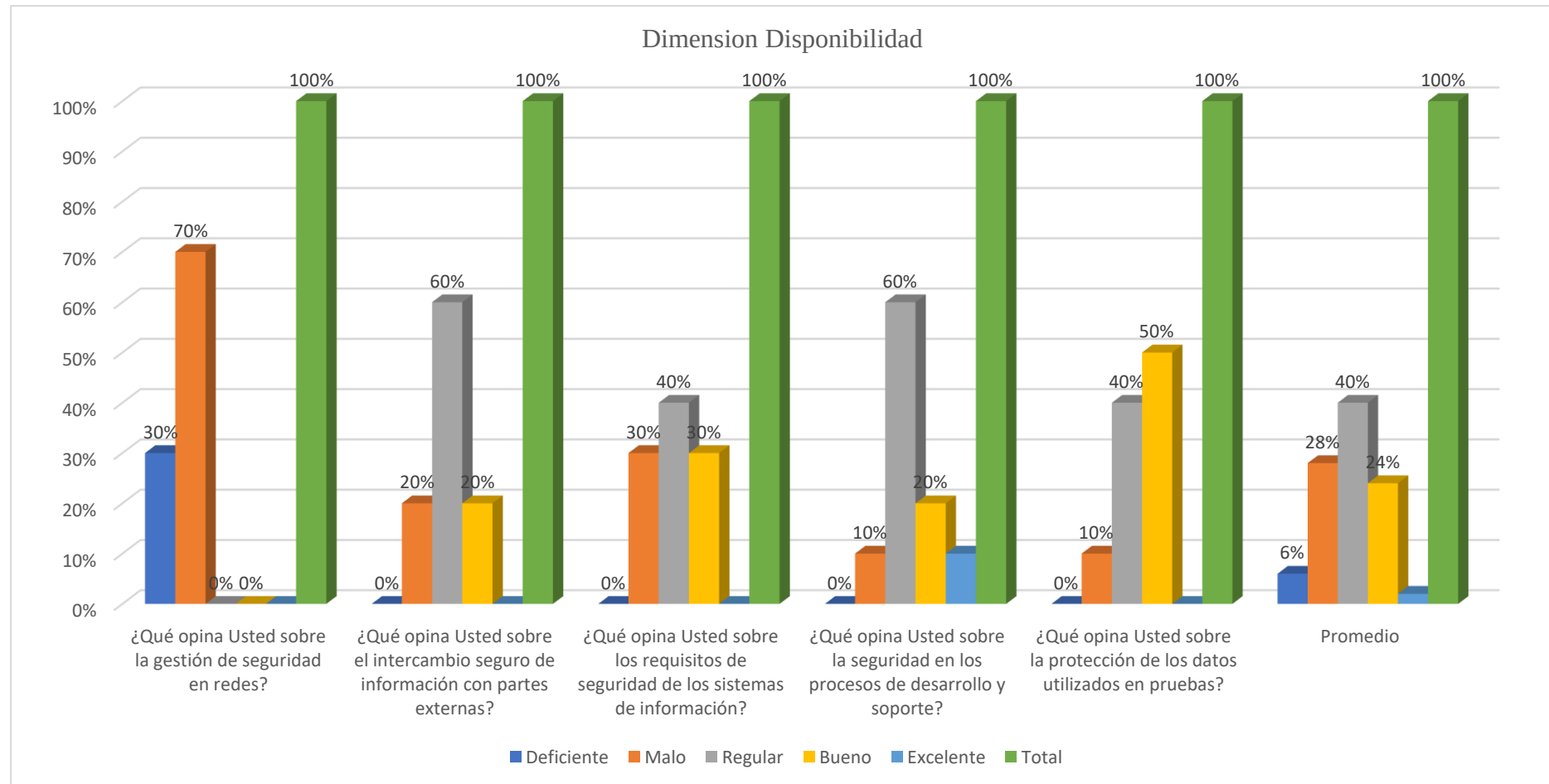
Describir la aplicación de la Norma ISO 27001 de la dimensión disponibilidad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.

Tabla 5
Dimensión Disponibilidad

ítem		Deficiente		Malo		Regular		Bueno		Excelente		Total	
Nº	Dimensión Disponibilidad	fi	%	fi	%	fi	%	fi	%	fi	%	fi	%
16	¿Qué opina Usted sobre la gestión de seguridad en redes?	3	30%	7	70%	0	0%	0	0%	0	0%	10	100%
17	¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	0	0%	2	20%	6	60%	2	20%	0	0%	10	100%
18	¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	0	0%	3	30%	4	40%	3	30%	0	0%	10	100%
19	¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	0	0%	1	10%	6	60%	2	20%	1	10%	10	100%
20	¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	0	0%	1	10%	4	40%	5	50%	0	0%	10	100%
Promedio			6%		28%		40%		24%		2%		100%

Nota: se realizó según los datos recolectados

Figura 5
Dimensión Disponibilidad



Nota: Realizado según la tabla

Interpretación

Muestra los resultados tabla Gestión de seguridad en redes: La percepción general es negativa, con el 100% de las respuestas indicando que la gestión de seguridad en redes es "Deficiente" (30%) o "Mala" (70%). Ítem dos el intercambio seguro de información con partes externas: Las opiniones están distribuidas mayormente entre "Regular" (60%) y "Bueno" (20%), con un 20% que considera que es "Malo". ítem tres los requisitos de seguridad de los sistemas de información: las opiniones se dividen casi equitativamente entre "Regular" (40%) y "Bueno" (30%), con un 30% que considera que es "Malo". ítem cuatro Seguridad en los procesos de desarrollo y soporte: La mayoría considera que la seguridad en los procesos de desarrollo y soporte es "Regular" (60%), con un 20% que la considera "Buena" y un 10% que la considera "Excelente". Un 10% la califica como "Mala". ítem cinco la protección de los datos utilizados en pruebas: La mayoría de los encuestados considera que la protección de los datos utilizados en pruebas es "Buena" (50%), con un 40% que la considera "Regular" y un 10% que la considera "Mala". Se concluye que los resultados indican una percepción mayormente negativa en cuanto a la gestión de seguridad en redes, que necesita atención urgente. Otros aspectos como el intercambio de información y los requisitos de seguridad requieren mejoras, mientras que la seguridad en los procesos de desarrollo y soporte y la protección de los datos utilizados en pruebas son vistos de manera más positiva pero aún pueden beneficiarse de mejoras adicionales.

Tabla 6

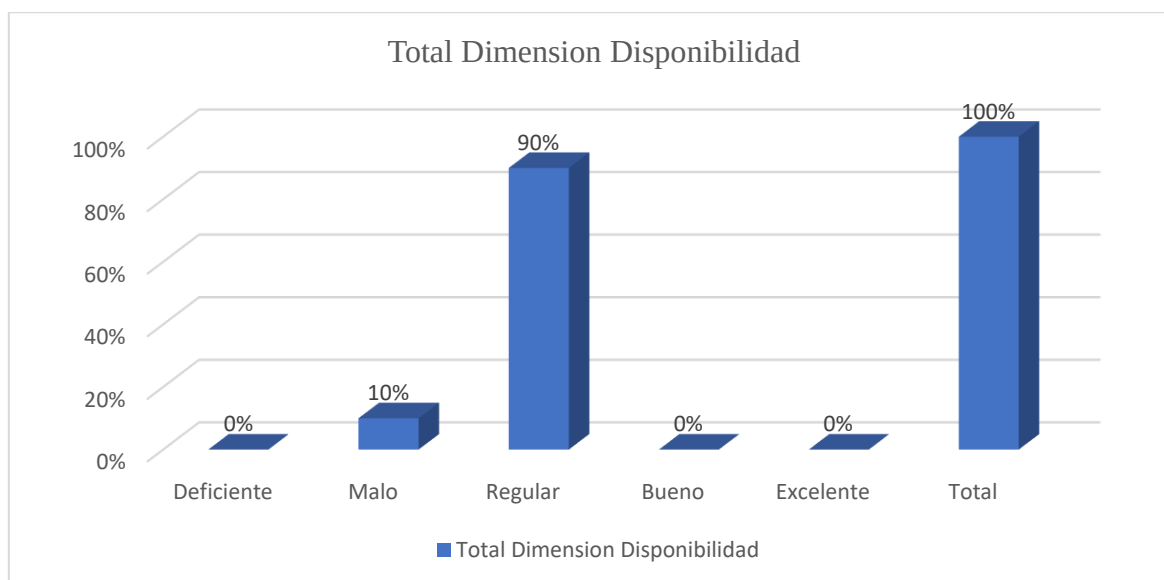
Total Dimensión Disponibilidad

		fi	%
Total	Deficiente	0	0%
Dimensión	Malo	1	10%
Disponibilidad	Regular	9	90%
	Bueno	0	0%
	Excelente	0	0%
	Total	10	100%

Nota: Realizado según la tabla

Figura 6

Total Dimensión Disponibilidad



Nota: Realizado según la tabla

Interpretación

Muestra los resultados que según la distribución General: La mayoría de las respuestas (90%) califican la disponibilidad como "Regular". Una minoría (10%) considera que la disponibilidad es "Mala". No hay respuestas que indiquen que la disponibilidad sea "Deficiente", "Buena" o "Excelente". Percepción Predominante: La percepción predominante es que la disponibilidad es "Regular". Esto sugiere que, aunque la disponibilidad no es considerada deficiente, tampoco es vista como



particularmente buena o excelente. Áreas de Mejora: La presencia de un 10% de respuestas que califican la disponibilidad como "Mala" indica que existen áreas que necesitan ser atendidas para mejorar la percepción general. Ausencia de Opiniones Extremas Positivas y Negativas: La ausencia de respuestas en las categorías "Deficiente", "Bueno" y "Excelente" sugiere que los encuestados no consideran que la disponibilidad esté en el extremo negativo (muy mala) ni en el positivo (muy buena). Esto refuerza la idea de que la disponibilidad está en un nivel intermedio. Se concluye que, aunque la disponibilidad es mayormente vista como adecuada (Regular), se requiere esfuerzo para elevar su calidad a niveles más altos y eliminar las percepciones negativas.

4.1.4. Objetivo General

Determinar la aplicación de la Norma ISO 27001 en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2024.

Tabla 7

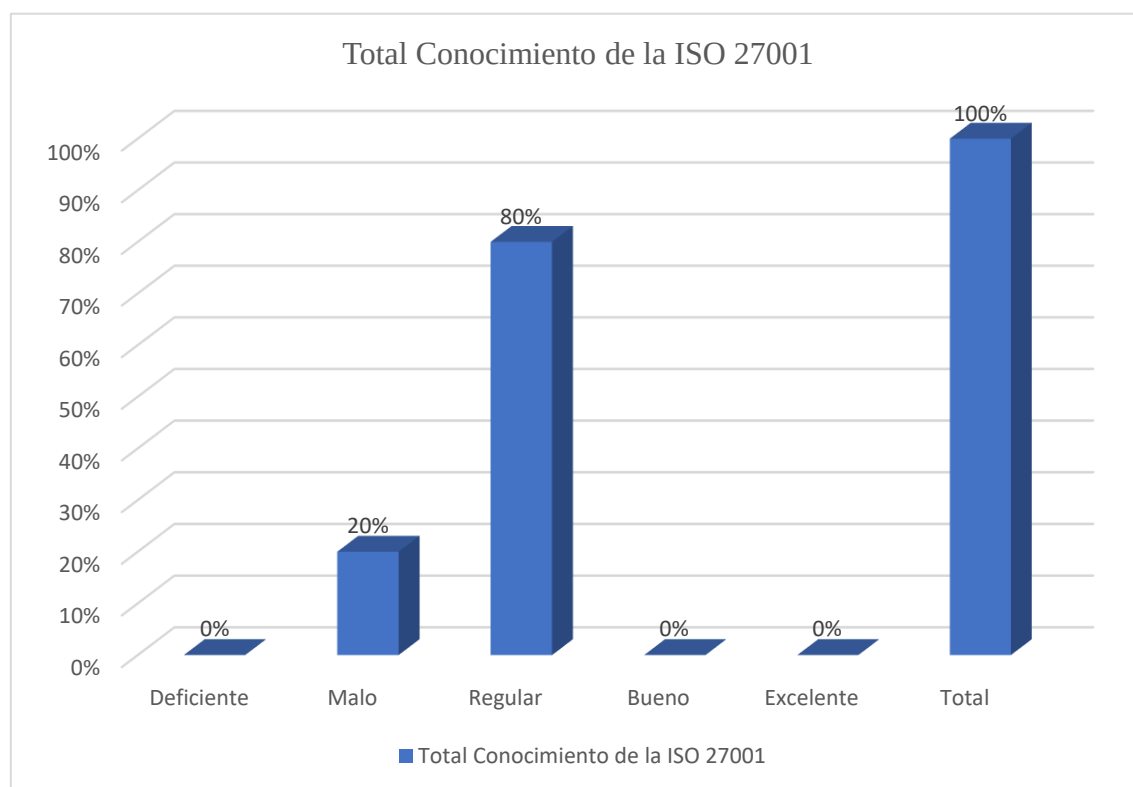
Total, Conocimiento de la ISO 27001

		fi	%
Total, Conocimiento de la ISO 27001	Deficiente	0	0%
	Malo	2	20%
	Regular	8	80%
	Bueno	0	0%
	Excelente	0	0%
	Total	10	100%

Nota: se realizó según los datos recolectados

Figura 7

Total Conocimiento de la ISO 27001



Nota: Realizado según la tabla



Interpretación

Muestra la tabla en los resultados se obtuvo en cuanto a una distribución General:

La mayoría de las respuestas (80%) califican el conocimiento de la ISO 27001 como "Regular". Una minoría (20%) considera que el conocimiento de la ISO 27001 es "Malo". No hay respuestas que indiquen que el conocimiento sea "Deficiente", "Bueno" o "Excelente". Percepción Predominante: La percepción predominante es que el conocimiento de la ISO 27001 es "Regular". Esto sugiere que, aunque el conocimiento no es considerado deficiente, tampoco es visto como particularmente bueno o excelente. Áreas de Mejora: La presencia de un 20% de respuestas que califican el conocimiento de la ISO 27001 como "Malo" indica que existen áreas que necesitan ser atendidas para mejorar la comprensión y aplicación de esta norma. Ausencia de Opiniones Extremas Positivas y Negativas: La ausencia de respuestas en las categorías "Deficiente", "Bueno" y "Excelente" sugiere que los encuestados no consideran que el conocimiento esté en el extremo negativo (muy malo) ni en el positivo (muy bueno). Esto refuerza la idea de que el conocimiento está en un nivel intermedio.

4.2. DISCUSIÓN DE RESULTADOS

Según Chicaiza (2020) evaluación del estado actual de seguridad en el departamento de tecnologías de la información de la entidad financiera se realizó de entrevistas, encuestas y recopilación de información con visitas in situ como resultados se realizó el análisis de posibles amenazas a la integridad y disponibilidad de la seguridad de la información con el fin de determinar el nivel de seguridad deseado. Se concluye que se establecieron políticas de seguridad con la gestión necesaria para garantizar la seguridad de la información, y estas se establecieron respetando los límites institucionales. Menciona también Sánchez (2021) Guayaquil este sistema se basó principalmente en la norma ISO 27001. Como resultado, se espera que el modelo de gestión de la seguridad de la información ayude a establecer políticas y procedimientos relacionados con los objetivos comerciales de las cooperativas de ahorro y crédito. Se concluye que esto ayudará a mantener los niveles de exposición por debajo del nivel de riesgo que la organización puede manejar y, como resultado, garantizar que la seguridad de la información se maneje correctamente. Para Núñez (2022) en Riobamba reveló un nivel de confianza de 86.90% y 96.96% , respectivamente. Adicionalmente, se desarrollaron indicadores de eficiencia de recursos, eficiencia de procesos, capacidad de pronóstico e indicadores lógicos de seguridad; como resultado, falencias como la falta de socialización de las políticas de uso del sistema de TI por parte de los empleados, la falta de evaluación del Sistema de Gestión de Seguridad de la Información utilizando la norma ISO 27001, pero no menos importante, al culminar las fases de la AU, con el fin de implementar medidas correctivas para



salvaguardar la integridad de los recursos tecnológicos, se concluye que la máxima autoridad del COAC Riobamba, el titular de la UTIC y todo el personal que labora dentro de la organización tomar en consideración las conclusiones y recomendaciones contenidas en este informe. tecnológicas y científicas. Por otro lado Pazmiño (2019) en Chibuleo detalla las actividades de recopilación de información y los riesgos potenciales. Luego de realizar este diagnóstico, se realizó un análisis de la norma internacional ISO 27002:2013 con el fin de identificar los controles aplicables y posteriormente mitigar los eventos de alto riesgo. Se concluye que el paso final, se desarrolló la política de seguridad de la información para el campo de la tecnología de la información. Finalmente, se recomienda que esta política sea aprobada por el Consejo de Administración, allanando el camino para su posterior implementación y difusión a todos los empleados de la Cooperativa. Menciona Granada (2019) un sistema de gestión de la seguridad de la información de acuerdo con la NTE INEN-ISO/27001, sus alcances y plazos. También se muestran los pasos que se deben seguir para desarrollar el plan de gestión de la seguridad de la información, se concluye que así como los entregables que se generaron a medida que fueron desarrollados y de acuerdo con la norma la cuarta sección del documento propone una guía de implementación. También Rodríguez (2020) demuestran, entre otras cosas, la necesidad de administrar información vital que puede ser esencial para los intereses estratégicos de las empresas. La conclusión cuantitativa indica que el uso de ISO tiene un efecto en la seguridad de la información, incluyendo la confidencialidad y disponibilidad. Según Pinto (2021) demuestran cómo garantizar la confidencialidad, la integridad y la accesibilidad de la



información y las organizaciones de apoyo, asegurando la continuación de los negocios como de costumbre, ya que las buenas prácticas descritas en la norma ISO 27002 complementan la gestión de la seguridad de la información. Se concluye que el sistema de gestión diseñado se transforma en una herramienta para aumentar la madurez, ayudando a la organización a reducir riesgos y sirviendo como pilar para el establecimiento de una cultura de seguridad de la información. En el ámbito nacional Calderon (2021) en Tacna. muestran que estadísticamente existe una correlación significativa entre el departamento de auditoría interna y el sistema de gestión de seguridad de la información en la cooperativa de ahorro y crédito municipal Tacna S.A., con un coeficiente de correlación de 0,4966 y un nivel de correlación moderado. Adicionalmente, el factor Satisfacción del Cliente es el más importante según Auditoría Interna, puntuando "De acuerdo" con una frecuencia de 70, o 61%, se concluye que para la variable Sistema de Gestión de Seguridad de la Información el factor más importante es "disponibilidad, anotando "Casi siempre" con una frecuencia de 62, o 54%. Para Yaguar (2021) la estrategia de seguridad de TI propuesta cumple con los estándares ISO 27001 e incluye políticas y procedimientos de seguridad de TI que administrarán de manera efectiva los procesos comerciales internos y, como resultado, mejorarán la seguridad del centro de datos. Se concluye que la evaluación de riesgos, identificación de riesgos, establecimiento de prioridades de ciber protección e implementación de las medidas de precaución (políticas) adecuadas. Según Navarro (2021) las experiencias que tuvieron los exempleados y compañeros de trabajo del área cuando estaban atentos a los controles del sistema de seguridad de la



información en el área de operaciones de la empresa donde laboramos para garantizar que los riesgos asociados con las actividades relacionadas con la información se reconozcan, gestionen, minimicen y documenten, la conclusión de la tesis incluye recomendaciones basadas en los objetivos de los dominios de control de la norma ISO 27001: 2013 que deben ponerse en práctica. Según Moscaiza (2020) estas instituciones financieras presentan aspectos que muestran la necesidad de encaminar sus procesos hacia una gestión de riesgos efectiva y acorde con los requerimientos regulatorios vigentes, que permitan. Por otro lado Cumpa (2020) su uso en un modelo de sistemas de gestión de seguridad de la información en la empresa Berendson Natación S.R.L.se concluye que propone una metodología de implementación de la norma ISO 27001. Menciona Aleman (2023) teniendo en cuenta una prueba de distribución no normal no paramétrica, los resultados de la prueba posterior fueron menos significativos que los resultados de la prueba previa en un nivel de significación de 0,5, se concluye la norma ISO 27001:2013 mejorará la seguridad de la información en las empresas de consultoría privadas.

CONCLUSIONES

Primera: De acuerdo al objetivo específico número uno, con respecto a la dimensión de confidencialidad, se concluye que la mayoría considera la clasificación de la información como "Regular" (70%), con una minoría indicando "Malo" (30%). Manejo de los soportes de almacenamiento: Las opiniones son predominantemente positivas, con "Bueno" (60%) y "Regular" (40%). Por lo que aunque la confidencialidad es mayormente vista como adecuada "regular", se requiere esfuerzo para elevar su calidad a niveles mas altos y eliminar las percepciones negativas.

Segunda: De acuerdo al objetivo específico numero dos, con respecto a la dimensión de Integridad, se concluye que la mayoría considera que la gestión de vulnerabilidades técnicas es "Regular" (50%), con un 30% que la consideran "Buena" y un 20% "Mala". Consideraciones de auditorías de sistemas de información: La mayoría considera las auditorías como "Regulares" (60%), con un 30% que las consideran "Malas. La mayoría de las áreas evaluadas en la dimensión de integridad necesitan mejoras significativas, especialmente en protección contra código malicioso y manejo de controles criptográficos.

Tercera: De acuerdo al objetivo específico tres, con respecto de la Dimensión de Disponibilidad la mayoría considera que la seguridad en los procesos de desarrollo y soporte es "Regular" (60%), con un 20% que la considera "Buena" y un 10% que la considera "Excelente". Un 10% la califica como "Mala". Ítem cinco la protección de los datos utilizados en pruebas: La mayoría de los encuestados considera que la protección de los datos



utilizados en pruebas es "Buena" (50%), con un 40% que la considera "Regular" y un 10% que la considera "Mala". Aunque la disponibilidad es mayormente vista como adecuada, otros aspectos como intercambio de información y los requisitos de seguridad requieren mejoras, los mismo que aun pueden mejorarse de manera significativa.

Cuarto: De acuerdo al objetivo general se concluye que la percepción predominante es que el conocimiento de la ISO 27001 es "Regular". Aunque el conocimiento no es considerado deficiente, tampoco es visto como particularmente bueno o excelente. Por lo que la ausencia de Opiniones Extremas Positivas y Negativas: La ausencia de respuestas en las categorías "Deficiente", "Bueno" y "Excelente" sugiere que los encuestados no consideran que el conocimiento esté en el extremo negativo (muy malo) ni en el positivo (muy bueno). Esto refuerza la idea de que el conocimiento está en un nivel intermedio y sugiere una posibilidad de mejora continua.



RECOMENDACIONES

Primera: Se recomienda mejorar la Clasificación de la Información capacitación y Implementar programas de capacitación regulares para el personal sobre la importancia de la clasificación adecuada de la información. Desarrollar y comunicar políticas claras sobre la clasificación de la información para asegurar que todos los empleados comprendan y sigan los procedimientos adecuados. Auditorías y Revisiones Periódicas: Realizar auditorías periódicas para asegurar que los soportes de almacenamiento sean manejados de manera segura y eficiente. Invertir en tecnologías de almacenamiento más seguras y eficientes para mejorar la gestión y la seguridad de los datos.

Segunda: Se sugiere utilizar herramientas de monitoreo y análisis continuo para identificar y gestionar vulnerabilidades técnicas en tiempo real. Formación en Seguridad Informática: Proveer formación continua en seguridad informática para el personal técnico, enfocándose en la identificación y mitigación de vulnerabilidades. Considerar la contratación de auditores externos para obtener una perspectiva imparcial y experta sobre la seguridad de los sistemas de información. Revisar y mejorar los procesos de auditoría actuales para asegurar que sean exhaustivos y efectivos en la identificación de fallos y áreas de mejora. Asegurar que los controles criptográficos estén bien implementados y actualizados para proteger la integridad de la información.

Tercera: Se recomienda promover y adoptar prácticas de desarrollo seguro (como el ciclo de vida de desarrollo de software seguro, o SDLC seguro).



Implementar revisiones de código y pruebas de seguridad regulares para identificar y corregir vulnerabilidades en las etapas tempranas del desarrollo. Utilizar técnicas de enmascaramiento y anonimización de datos para proteger la información sensible durante las pruebas. Asegurar que los entornos de pruebas cuenten con medidas de seguridad adecuadas para proteger los datos contra accesos no autorizados.

Cuarta: Se recomienda implementar una planificación y gestión de capacidad efectiva para asegurar que los sistemas puedan manejar la carga de trabajo y mantener la disponibilidad. Establecer medidas de redundancia y planes de recuperación ante desastres para minimizar el tiempo de inactividad y asegurar la continuidad del negocio. Realizar evaluaciones periódicas para identificar áreas con baja disponibilidad y tomar acciones correctivas. Recoger y analizar feedback de los usuarios y el personal para identificar problemas de disponibilidad, confidencialidad e integridad y trabajar en soluciones efectivas. Asegurar que la alta dirección esté comprometida con la mejora continua de la disponibilidad y seguridad de los sistemas. Establecer indicadores de rendimiento clave (KPIs) y realizar seguimientos regulares para evaluar el progreso y hacer ajustes necesarios.



REFERENCIAS BIBLIOGRÁFICAS

- Aleman, B. F. (2024). *Norma ISO 27001 para el control de la seguridad de información en una consultoría privada, Lima 2024*. Recuperado el 7 de Mayo de 2022, de <https://hdl.handle.net/20.500.12692/106824>
- Arias, G. J. (2020). *Técnicas e instrumentos de investigación científica*. doi:file:///C:/Users/USUARIO/Downloads/AriasGonzales_TecnicasInstrumentosDeInvestigacion
- Barriento, N. (2021). *Metologia de la Investigacion*. doi:https://es.scribd.com/document/504549046/Metodologia-de-la-Investigacion-Nelly-Barrientos-C-l29933584
- Benites, D. C. (2019). *Implementación de un sistema de gestión de seguridad de la información - Norma ISO 27001 para la fábrica Radiadores Fortaleza*. Recuperado el 07 de Mayo de 2024, de <https://hdl.handle.net/20.500.12867/1933>
- Bernal. (2010). *Metodología de la investigación administración, economía, humanidades y ciencias sociales (3ra. Ed.)*. Pearson Educacion Colombia. [https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigación -F.G.-Arias-2012-pdf.pdf](https://abacoenred.com/wp-content/uploads/2019/02/El-proyecto-de-investigación-F.G.-Arias-2012-pdf.pdf)
- Calderon, G. L. (2021). *Auditoría interna y el sistema de gestión de seguridad de la información de la Caja Municipal de Ahorro y Crédito de Tacna S.A., 2020*. Recuperado el 12 de Julio de 2024, de <http://repositorio.unjbg.edu.pe/handle/UNJBG/4349>
- Camposano, M. G. (2020). *Propuesta para el control y seguridad de la información de la empresa de ventas en Línea Buy Now aplicando Norma ISO 27001*. Recuperado el 12 de Mayo de 2024, de <http://dspace.utb.edu.ec/handle/49000/8614>
- Carrasco, D. S. (2005). *Metodologia de la Investigacion Cientifica*. Lima: San Marcos . doi:file:///C:/Users/Usuario/Downloads/Metodologia_de_La_Investigacion_Cientifi.pdf



Chávarry, B. S. (2021). *Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en Secretaría Ejecutiva de Policía Nacional del Perú*. Recuperado el 06 de Mayo de 2024, de <https://hdl.handle.net/20.500.12692/79133>

Chavez, C. L. (2021). *proceso de auditoria iso 27001 para la mejora de los controles de seguridad de la información en la municipalidad distrit al de san juan bautista 2018*. Recuperado el 12 de Mayo de 2024, de <http://repositorio.ucp.edu.pe/handle/UCP/1292>

Chicaiza, C. D. (2020). *Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indígena SAC*. Recuperado el 13 de Mayo de 2024, de <https://repositorio.uta.edu.ec/jspui/handle/123456789/31305>

Cumpa, V. J. (2020). *modelo de seguridad informática aplicando la norma iso/iec 27001 para proteger los activos de información en la empresa berendson natación S.R.L.* Recuperado el 12 de Mayo de 2024, de <https://repositorio.udl.edu.pe/handle/UDL/338>

Definiciones. (9 de Setiembre de 2021). Obtenido de <https://www.google.com/search?q=la+obesidad+y+el+sobrepeso+se+definen+como+una+acumulaci%C3%B3n+anormal+o+excesiva+de+grasa+que+puede+ser+perjudicial+para+la+salud%E2%80%9D&oq=la+obesidad+y+el+sobrepeso+se+definen+como+una+acumulaci%C3%B3n+anormal+o+exces>

Diccionario. (8 de Setiembre de 2021). Obtenido de <https://www.google.com/search?q=ejercicios+f%C3%ADsicos+recreativos&oq=ejercicios+f%C3%ADsicos+recreativos&aqs=chrome..69i57j0i19i22i30l2j0i10i19i22i30.3567j0j7&sourceid=chrome&ie=UTF-8>

Gonzales Aybar, R. G. (2019). *Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el Departamento Telemática de la Oficina de Economía del Ejército del Perú*. Recuperado el 14 de Mayo de 2024, de <https://hdl.handle.net/20.500.13067/1039>



- González, L. (2020). Retos y oportunidades en la adopción de la norma ISO 27001 en el Perú. *Journal of Peruvian Security Studies*, 4(1), 45-59.
- Granada, G. E. (2019). *El presente informe de tesis desarrolló un modelo de sistema de gestión de seguridad de la información aplicada a las pymes en la ciudad de Chiclayo, basado en la norma ISO 27001. Las Normas ISO no sólo son herramientas al alcance de las grandes empresas.* Recuperado el 12 de Junio de 2024, de <http://bibdigital.epn.edu.ec/handle/15000/19938>
- Hernández, R., & Mendoza, C. (2014). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. México: McGraw-Hill Interamericana.
- Hernández, S. R. (2014). *Metodologia de la Investigacion* (Sexta edición ed.). (S. D. McGRAW-HILL / INTERAMERICANA EDITORES, Ed.) México, Mexico . Recuperado el 15 de Diciembre de 2022, de <https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf>
- Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13(4), 247-255.
- Kalambkar, D. D. (2021). *Implementing ISO 27001 Simplified Full Fledged Information on Implementing End-to-End Information Security with Real Time Statistical Data and Analysis*. (N. Press, Ed.) Recuperado el 13 de Agosto de 2024, de https://www.google.com.pe/books/edition/Implementing_ISO_27001_Simplified/QrEcEAAQBAJ?hl=es-419&gbpv=0
- Ladrón, d. G. (2020). *Transmisión de información por medios convencionales e informáticos*. UF0512. (E. T. Formación, Ed.) Recuperado el 13 de Agosto de 2024, de https://www.google.com.pe/books/edition/Transmisi%C3%B3n_de_informaci%C3%B3n_por_medios/cAIAEAAQBAJ?hl=es-419&gbpv=0



- Mamani, J., & Quispe, R. (2022). Seguridad de la información en cajas de ahorro y crédito en Juliaca. *Revista de Ciencias Empresariales de Juliaca*, 3(1), 87-101.
- Mera, A. I. (2022). *Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: empresa ALTAC*. Recuperado el 12 de Mayo de 2024, de <http://repositorio.puce.edu.ec:80/handle/22000/21108>
- Moscaiza, M. O. (2020). *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013*. Recuperado el 12 de Mayo de 2024, de <https://repositorioacademico.upc.edu.pe/handle/10757/623063>
- Navarro, C. M. (2021). *Sistema de gestión de seguridad de la información basada en la Norma ISO 27001 para la Caja Sullana*. Recuperado el 12 de Julio de 2024, de <http://repositorio.usanpedro.edu.pe/handle/20.500.129076/20288>
- Núñez, B. A. (2022). *Auditoría informática a la "Cooperativa de Ahorro y Crédito Riobamba Ltda.", agencia matriz, cantón Riobamba, provincia de Chimborazo, periodo 2020*. Recuperado el 13 de Mayo de 2024, de <http://dspace.esPOCH.edu.ec/handle/123456789/16760>
- Pazmiño, F. C. (2019). *Diseño de una política de seguridad de la información para el área de tecnología de la información de la Cooperativa de Ahorro y Credito Chibuleo LTDA., basado en la norma ISO/IEC 27002:2013*. Recuperado el 13 de Mayo de 2024, de <http://repositorio.uisek.edu.ec/handle/123456789/3601>
- Pinto, A. D. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí*. Recuperado el 07 de Mayo de 2024, de <http://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf>



- Quispe, Q. Y., Machicao, L. V., Cora, F. N. P., & Velásquez, A. (2024). Diseños y secuencia didáctica para la investigación en un nuevo paradigma. *Centro de Investigación y Desarrollo*. doi: https://doi.org/10.37811/cli_w957
- Ramírez, J., & Vargas, M. (2019). Implementación de la norma ISO 27001 en instituciones financieras peruanas. *Revista Peruana de Ingeniería y Tecnología*, 5(2), 123-136.
- Rodriguez, B. L. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana*. Recuperado el 13 de Mayo de 2024, de <http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf>
- Steve, W. A. (2019). *Information Security Risk Management for ISO 27001/ISO 27002, third edition*. (I. G. Ltd, Ed.) Recuperado el 13 de Agosto de 2024, de https://www.google.com.pe/books/edition/Information_Security_Risk_Management_for/GEGuDwAAQBAJ?hl=es-419&gbpv=0
- Sánchez, P. C. (2021). *Modelo de Gestión de la Seguridad de la Información adaptado a las Cooperativas de Ahorro y Crédito de la ciudad de Guayaquil*. Recuperado el 12 de Julio de 2024, de <http://biblioteca.uteg.edu.ec/xmlui/handle/123456789/1533>
- Tamayo, T. M. (2004). *Diccionario de la investigación científica*. Mexico: Limusa, México y cop. 2004.
- Ticona, L. H. (2021). *Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa Ico el año 2021*. Recuperado el 13 de Mayo de 2024, de <https://hdl.handle.net/11537/28162>
- Vasquez, V. R. (2020). *Aplicación para la gestión de incidencias de TI bajo la perspectiva ITIL y el enfoque Open Source para Departamento de TI de la Caja Rural de Ahorro y Crédito Cajamarca S.A.* Recuperado el 12 de Mayo de 2024, de <https://hdl.handle.net/20.500.12893/8697>
- Vásquez, W. (2007). *Diccionario de Pedagogía*. Lima: San Marcos.



- Vilca, C. V. (2022). *Una estrategia didáctica en educación ambiental con base en el manejo de residuos sólidos*. Recuperado el 12 de Junio de 2024, de <https://www.revistas-historico.upel.edu.ve/index.php/revinpost/article/view/10099>
- Villalón, H. A. (2020). *Seguridad en Unix y redes. Versión 2.1'*. (N. Llibres, Ed.) Recuperado el 13 de Agosto de 2024, de [https://www.google.com.pe/books/edition/Seguridad en Unix y redes Versi%C3%B3n 2 1-i-LTDwAAQBAJ?hl=es-419&gbpv=0](https://www.google.com.pe/books/edition/Seguridad%20en%20Unix%20y%20redes/Versi%C3%B3n%202.1-i-LTDwAAQBAJ?hl=es-419&gbpv=0)
- Villamar, S. C. (2021). *Análisis de seguridad de la información basado en la norma ISO 27001 en el Área Técnica de Reparación e Instalación de la Corporación Nacional de Telecomunicaciones "CNT EP" de la ciudad de Babahoyo*. Recuperado el 07 de Mayo de 2024, de <http://dspace.utb.edu.ec/handle/49000/10549>
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
- Wikipedia. (22 de Agosto de 2021). Obtenido de La enciclopedia libre: <https://www.google.com/search?q=wikipedia+espa%C3%B1ol&og=wikipedia&aqs=chrome.1.69i57j0i512l9.9367j0j7&sourceid=chrome&ie=UTF-8>
- Yaguar, M. J. (2021). *Plan de seguridad informática alineado a la Norma ISO 27001 para fortalecer las seguridades del data center en la cooperativa de ahorro y crédito 1 de julio de la ciudad del Tena*. Recuperado el 12 de Julio de 2024, de <https://dspace.uniandes.edu.ec/handle/123456789/12752>



Apéndice 01 Matriz de Consistencia

APLICACIÓN DE LA NORMA ISO 27001 EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN EN CAJAS DE AHORRO Y CRÉDITO JULIACA - 2024

Problema	Objetivos	Hipótesis	Metodología	Técnicas e Instrumentos	Variable	Dimensiones	Escala
General PG= ¿Como se aplica la Norma ISO 27001 en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023? Específico PE1= ¿Como se describe la aplicación de la Norma ISO 27001 en la dimensión confidencialidad e la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023? PE2= ¿Como caracterizar la aplicación de la Norma ISO 27001 en la dimensión integridad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023? PE3= ¿Como se describir la aplicación de la Norma ISO 27001 en la dimensión disponibilidad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023?	General OG=Determinar la aplicación de la Norma ISO 27001 en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023. Específico OE1=Describir la aplicación de la Norma ISO 27001 de la dimensión confidencialidad e la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023. OE2=Caracterizar la aplicación de la Norma ISO 27001 de la dimensión integridad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023. OE3=Describir la aplicación de la Norma ISO 27001 de la dimensión disponibilidad en la mejora continua del sistema de gestión de seguridad de información en las cajas de ahorro y crédito Juliaca 2023.	La investigación no tiene hipótesis ya que es de nivel descriptivo donde es invariable por ende no existe la relación de ningún tipo de causa y efecto. La relación de una hipótesis en más referido a la respuesta a una pregunta de investigación y los dos aspectos son más directos Hernández (2014)	Enfoque Cualitativo Tipo Básico Nivel Descriptivo Diseño No experimental	Técnicas Observación Instrumentos Cuestionario	Norma ISO 27001	Confidencialidad Integridad Disponibilidad	1= Deficiente 2= Malo 3= Regular 4= Bueno 5= Excelente

Apéndice 02 Instrumentos

CUESTIONARIO ISO 27001

No	Ítems	Opción de respuesta				
		1	2	3	4	5
Dimensión Confidencialidad						
01	¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?					
02	¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?					
03	¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?					
04	¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?					
05	¿Qué opina Usted sobre el manejo responsable sobre los activos?					
06	¿Qué opina Usted sobre la clasificación que se realiza de la información?					
07	¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?					
Dimensión Integridad						
08	¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?					
09	¿Qué opina Usted sobre la protección conveniente contra código malicioso?					
10	¿Qué opina Usted sobre el manejo de copias de seguridad?					
11	¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?					
12	¿Qué opina Usted sobre el control de software de explotación?					
13	¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?					
14	¿Qué opina Usted sobre las consideraciones de la auditorías de los sistemas de información?					
15	¿Qué opina Usted sobre el manejo de los controles criptográficos?					
Dimensión Disponibilidad						
16	¿Qué opina Usted sobre la gestión de seguridad en redes?					
17	¿Qué opina Usted sobre el intercambio seguro de información con partes externas?					
18	¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?					
19	¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?					
20	¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?					

Apéndice 03 Valides de Instrumentos EXPERTO 01

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

Para cada ítem del contenido del instrumento que revisa, marque usted con un check (✓) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad*, *Pertinencia* o *Relevancia*.

Dimensiones	Claridad ¹		Pertinencia ²		Relevancia ³		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?	x		x		x		
6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?	x		x		x		
Dimensión 2: Integridad							
8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
10. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
12. ¿Qué opina Usted sobre el control de software de explotación?	x		x		x		
13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	x		x		x		
14. ¿Qué opina Usted sobre las consideraciones de la auditorías de los sistemas de información?	x		x		x		



15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?	x		x		x		
Dimensión 3: Disponibilidad							
16. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x		x		
20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	x		x		x		

¹Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

²Pertinencia: Si el ítem pertenece a la dimensión.

³Relevancia: El ítem es apropiado para representar a la dimensión específica del constructo.

Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Observaciones: Es suficiente	
Opinión de aplicabilidad	
Aplicable [x]	Aplicable después de corregir [] No aplicable []
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Especialidad del evaluador	Tecnologías de la información
 DNI: 18161457	
Trujillo, 18 de junio del 2022	

EXPERTO 02

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

Para cada ítem del contenido del instrumento que revisa, marque usted con un check (✓) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad*, *Pertinencia* o *Relevancia*.

Dimensiones	Claridad ¹		Pertinencia ²		Relevancia ³		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?	x		x		x		
6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?	x		x		x		
Dimensión 2: Integridad							
8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
10. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
12. ¿Qué opina Usted sobre el control de software de explotación?	x		x		x		
13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	x		x		x		
14. ¿Qué opina Usted sobre las consideraciones de la auditorías de los sistemas de información?	x		x		x		



15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?	x		x		x		
Dimensión 3: Disponibilidad							
16. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x			x	
20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	x		x			x	

¹**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

²**Pertinencia:** Si el ítem pertenece a la dimensión.

³**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Observaciones: Es suficiente	
Opinión de aplicabilidad	
Aplicable [x]	Aplicable después de corregir [] No aplicable []
Apellidos y nombres del juez evaluador	Dr. Mendoza Rivera, Ricardo Darío
Especialidad del evaluador	Gestión de Proyectos
 DNI: 18070765 Trujillo, 18 de junio del 2022	

EXPERTO 03

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

Para cada ítem del contenido del instrumento que revisa, marque usted con un check (✓) o un aspa (X) la opción SÍ o NO que elija según el criterio de *Claridad*, *Pertinencia* o *Relevancia*.

Dimensiones	Claridad ¹		Pertinencia ²		Relevancia ³		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
5. ¿Qué opina Usted sobre el manejo responsable sobre los activos?	x		x		x		
6. ¿Qué opina Usted sobre la clasificación que se realiza de la información?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de los soportes de almacenamiento?	x		x		x		
Dimensión 2: Integridad							
8. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
9. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
10. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
11. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
12. ¿Qué opina Usted sobre el control de software de explotación?	x		x		x		
13. ¿Qué opina Usted sobre la gestión de las vulnerabilidades técnicas?	x		x		x		
14. ¿Qué opina Usted sobre las consideraciones de la auditorías de los sistemas de información?	x		x		x		



15. ¿Qué opina Usted sobre el manejo de los controles criptográficos?	x		x		x		
Dimensión 3: Disponibilidad							
16. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
17. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
18. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
19. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x		x		
20. ¿Qué opina Usted sobre la protección de los datos utilizados en pruebas?	x		x			x	

¹**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

²**Pertinencia:** Si el ítem pertenece a la dimensión.

³**Relevancia:** El ítem es apropiado para representar a la dimensión específica del constructo.

Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Observaciones: Es suficiente	
Opinión de aplicabilidad	
Aplicable [x]	Aplicable después de corregir [] No aplicable []
Apellidos y nombres del juez evaluador	Ms. Córdova Otero, Juan Luis
Especialidad del evaluador	Sistemas de información
 DNI: 18122765	
Trujillo, 18 de junio del 2022	



Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	18	100,0
	Excluido	0	,0
	Total	18	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,884	20



Apéndice 04 Base de Datos

Sujeto	Variable ISO 27001																							
	Confidencialidad							Integridad								Disponibilidad								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20				
1	3	3	1	3	2	3	3	3	2	3	3	3	3	3	2	2	2	4	5	3	3	3	3	3
2	3	4	1	2	3	3	4	3	2	3	3	4	3	4	2	2	2	3	4	4	3	3	3	3
3	3	3	2	3	2	2	3	3	2	3	3	2	3	2	2	2	3	3	3	4	3	3	3	3
4	2	4	2	3	3	3	4	3	1	2	3	2	3	3	2	2	4	3	3	4	3	2	3	3
5	4	3	1	2	2	2	3	2	1	2	3	2	4	3	2	1	4	2	4	3	2	2	3	2
6	3	2	2	2	3	3	4	2	2	2	2	2	4	2	1	1	3	2	3	4	3	2	3	3
7	3	3	1	3	3	3	4	2	2	2	2	3	3	2	1	2	3	4	3	2	3	2	3	3
8	2	3	1	3	2	3	4	3	1	2	3	3	2	3	2	2	3	4	3	3	3	2	3	3
9	3	4	2	2	2	2	4	1	2	2	3	3	4	3	1	2	3	2	3	4	3	2	3	3
10	3	4	2	3	3	3	3	1	1	2	2	3	2	3	1	1	3	3	2	3	3	2	2	2



ANEXO 1
FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS
TRABAJOS DE INVESTIGACIÓN
EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital ☒

Fecha de entrega: 05-12-2025

1. Datos del autor (es):

Nombres y Apellidos:	Miriam Yaneth Lupaca Valeriano
Dirección:	Barrio Pilcuyo
DNI/Carné de Extranjería/Pasaporte N°:	73586893
Teléfono:	950307022
email:	myanethlupaca@gmail.com
Nombres y Apellidos:	
Dirección:	
DNI/Carné de Extranjería/Pasaporte N°:	
Teléfono:	
email:	
Facultad y/o Escuela de Posgrado:	Maestría en Derecho
Escuela Profesional o Mención:	Derecho Civil y Empresarial
Título o Grado Académico a optar:	Maestro en Derecho
Asesor:	Dra. Yenny Rosario Acero Apaza
Esta obra se encuentra dentro de las siguientes denominaciones:	
Trabajo de Investigación ☐	Tesis ☒
Trabajo de Suficiencia Profesional ☐	Trabajo Académico ☐
Título: Aplicación de la norma ISO 27001 en el sistema de gestión de seguridad de información en cajas de ahorro y crédito Juliaca - 2024	
Palabras claves, (3 a 5 términos): Aplicación, Norma ISO 27001, microfinanzas	
¿Esta obra se desarrolló en la UANCV ^{1, 2} ?	
2	

¹ Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entre otros relacionados.

² Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.



2. Referencia de tesis:

☐ Bachiller ☐ Título ☐ 2da Especialidad ☒ Maestría ☐ Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción Intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

- ☒ Sí, autorizo que se deposite inmediatamente.
- ☐ Sí, autorizo que se deposite a partir de la fecha (d/m/a): _____
- ☐ No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comerciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

- ☒ Sí autorizo
- ☐ No autorizo



Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción “internacional” o una adaptada a su jurisdicción, como para el caso peruano.

La opción “internacional” emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción “internacional” goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral.** Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

☐

Internacional

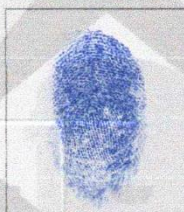
☒

Nacional

Línea de investigación:

Derecho Privado - P38

Firma de Autor



huella digital

05-12-2025

Fecha