

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
ESCUELA DE POSGRADO
MAESTRÍA EN GESTIÓN TECNOLÓGICA DE LA INFORMACIÓN



TESIS

“Infraestructura de un data center para la seguridad de la información (ISO 27001) de la
Municipalidad Provincial de Huaraz – 2021”

AUTOR:

Huaney Tinoco, Julio Cesar

PARA OPTAR EL GRADO ACADÉMICO DE

Maestro en Gestión Tecnológica de la Información

ASESOR:

Mg. Jhony Alex Zárate Bocanegra

ORCID iD 0000-0001-6440-0108

LIMA - PERÚ

2022

Dedicatoria

A mi hermosa hija, una bella persona que me llena de alegrías el día a día, al verla sonreír, por su gran amor, su gran personalidad, su hermoso carácter y por ser mi inspiración el día a día. A mi madre por su cariño incondicional, su apoyo constante en todo momento. A mi padre por el mi ejemplo de buena persona al cual quiero llegar a ser. A mi esposa por su comprensión diaria y su cariño.

Agradecimiento

A Dios, por darme salud y vida, a mis padres por su apoyo incondicional, y a mi esposa y mi hija, ellas son el motor de mi superación constante.

Índice

Caratula.....	i
Dedicatoria	ii
Agradecimiento	iii
Índice	iv
Índice de tablas	vii
Índice de figuras	viii
Resumen	ix
Abstract	x
Introducción	1
CAPÍTULO I	3
1. PLANTEAMIENTO DEL PROBLEMA	3
1.1 Descripción de la realidad problemática	3
1.2 Definición del problema	4
1.2.1 Problema general	5
1.2.2 Problemas específicos	6
1.3 Objetivos de la investigación	6
1.3.1 Objetivo general	6
1.3.2 Objetivos específicos	6
1.4 Formulación de hipótesis	7
1.4.1 Hipótesis general	7
1.4.2 Hipótesis específicas	7
1.5 Variables y dimensiones	8
1.6. Justificación de la Investigación:	10

CAPÍTULO II	12
2. MARCO TEÓRICO	12
2.1 Antecedentes de la investigación	12
2.2 Bases teóricas	17
2.3 Definición de términos	31
CAPÍTULO III	33
3. DISEÑO METODOLÓGICO	33
3.1 Tipo de investigación	33
3.2 Diseño de la investigación	34
3.3 Población y muestra	34
3.4 Técnicas para la recolección de datos	35
3.4.1 Descripción de los instrumentos	35
3.4.2 Validez y confiabilidad de los instrumentos	36
3.4.3 Técnicas para el procesamiento y análisis de los datos	36
CAPÍTULO IV	38
4. PRESENTACIÓN DE RESULTADOS	38
4.1 Presentación e interpretación de resultados en tablas y figuras	38
4.1.1 Resultados de los objetivos	39
4.1.2 Prueba de normalidad	45
4.2 Contrastación de hipótesis de la investigación	46
CAPÍTULO V	51
5. DISCUSIÓN	51
5.1 Discusión de resultados obtenidos	51
5.2 Conclusiones	59
5.3 Recomendaciones	61
Referencias bibliográficas	63
ANEXOS	71

Anexo 1. Matriz de consistencia	71
Anexo 2. Instrumentos para la recolección de datos	74
Anexo 3. Validación del instrumento.....	76
Anexo 4. Base de datos	82
Anexo 5. Evidencia digital de similitud	95
Anexo 6. Autorización de publicación en el repositorio	96

Índice de tablas

Tabla 1. Variable dependiente seguridad de la información (ISO 27001)	19
Tabla 2. Variable independiente infraestructura de un data center	10
Tabla 3. Demostrar como la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.	39
Tabla 4. Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	40
Tabla 5. Comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	41
Tabla 6. Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	43
Tabla 7. Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	44
Tabla 8. Prueba de normalidad de datos.....	45
Tabla 9. Prueba para comprobar la hipótesis general.....	46
Tabla 10. Prueba para comprobar la hipótesis específica 1.....	56
Tabla 11. Prueba para comparar la hipostesis específica 2.....	57
Tabla 12. Prueba para comprar la hipostesis específica 3.....	58
Tabla 13. Prueba para comprar la hipostesis específica 4.....	59

Índice de figuras

Figura 1. Frecuencia de la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.	39
Figura 2. Barra de los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	40
Figura 3. los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	42
Figura 4. Barra de los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	43
Figura 5. Barra de los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	44

Resumen

El estudio presenta como objetivo general: “Demostrar como la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021”, para ello se ubica dentro del paradigma positivista, enfoque cuantitativo, diseño experimental – pre experimental, con alcance longitudinal, para ello se aplicó una población de 280 y una muestra probabilística conformada por 162 trabajadores, aplicando la técnica de la encuesta y como instrumento el cuestionario, logrando concluir: Con los resultados se ha demostrado que la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021, mostrando una mejorar de 50.6% para el nivel alto, en el caso del nivel regular se ha demostrado una mejorar del 15.4% y para el nivel bajo se ha reducido en 35.2 %, además de ello se ha logrado comprobar la hipótesis.

Palabras clave: Data center, seguridad de la información, ISO 27001, sistemas informáticos

Abstract

The study presents as general objective: To demonstrate how the infrastructure of a data center affects information security (ISO 27001) of the provincial municipality of Huaraz - 2021, for this it is located within the positivist paradigm, quantitative approach, experimental design - pre experimental, with longitudinal scope, for this a population of 280 and a probabilistic sample made up of 162 workers were applied, applying the survey technique and the questionnaire as an instrument, managing to conclude: With the results it has been shown that the infrastructure of a data center affects the information security (ISO 27001) of the provincial municipality of Huaraz - 2021, showing an improvement of 50.6% for the high level, in the case of the regular level an improvement of 15.4% has been shown and for the low level has been reduced by 35.2%, in addition to this, the hypothesis has been verified by finding.

Keywords: Data center, information security, ISO 27001, computer systems

Introducción

Los centros de datos o Data Center, se considera fundamentales para el tráfico, procesamiento y el acaparamiento de datos de la entidad. Por ello, que deben asegurar, además de ser confiable y asegurar el tiempo de respuesta de datos para que la gestión de la entidad se realice como lo esperan los usuarios internos y externos.

Durante el proceso de diseño del Data Center se deben tener en cuenta los criterios lógicos y físicos para su correcta implementación, siguiendo los estándares y normativas que garanticen el correcto funcionamiento y aseguren la información que tenga la entidad.

La municipalidad cuenta con la necesidad de mejorar sus procesos de data, que aseguren la información y garanticen la disponibilidad de datos.

Durante el estudio se plantea realizar una descripción detallada de la problemática que se presenta en el estudio, luego se tiene la formulación de los objetivos que se desean alcanzar, planteando las hipótesis y segmentando las variables en dimensiones, finalizando justificando las razones por las que se desarrollan el estudio, todo lo mencionado pertenece al capítulo I que se denomina planteamiento del problema.

Luego en el Capítulo II que se denomina marco teórico, involucra los aspectos de la indagación de estudios que presenten similares características, luego se desarrollan las bases teóricas y se culmina con la definición de los principales términos del estudio.

Durante el desarrollo del capítulo III que se basa en el diseño metodológico, se tomaron en cuenta el tipo de investigación, mencionando la alineación que presenta el estudio, luego se presenta el diseño del estudio, de ahí se describen la población y la muestra que se utilizó en el estudio, comentando sobre la técnica e instrumentos a utilizar, finalizando comentando sobre las técnicas y procesamiento de análisis de datos.

En el Capítulo IV que se denomina presentación de resultados se basa en el análisis de las opiniones que brinden las personas que formaron parte del estudio realizando la descripción del procesamiento estadístico y la comprobación de hipótesis.

Finalmente, en el capítulo V que se denomina discusión, se plantea la comparación de los resultados con los antecedentes y el marco teórico, luego se detallan las conclusiones y se finaliza con las recomendaciones del estudio.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la realidad problemática

En la actualidad a raíz de la pandemia del Covid-19, las empresas y entidad públicas se han visto obligadas a realizar cambios rotundos en la modalidad de trabajo y de ofrecer sus servicios a sus usuarios, uno de estos aspectos es el sector público, donde se evidencia poco interés en invertir y mejorar su capacidad tecnológica, a ello se tiene los problemas de vulneración de información y de manejo de herramientas tecnológica por parte de los servidores públicos.

En este sentido Graf (2020), argumenta que las empresas de Argentina han comenzado adoptar nuevas medidas para que la pandemia no afecte sus procesos y servicios que brindan a sus usuarios, es por ello que se enfocaron a brindar a sus trabajadores los recursos y accesos necesarios para que sigan desarrollando su trabajo de manera normal, implementando Data Center para que el acceso a la información de las empresas sea seguro. Por otro lado Hernández (2019), comenta que en México ocurrió algo similar que las empresas están afrontando una nueva modalidad de ofrecer sus servicios y para ello necesitan tener alcance a todos ellos, presentando como soporte a la incorporación de las

tecnologías para que se pueda lograr, uno de estos elementos es la implementación de normas ISO que fortalezcan sus medidas de seguridad como es la ISO 27001, que presenta los procesos que deben seguir las empresas para que aseguren el servicio que brindan.

En Colombia desde la perspectiva de Martelo et al (2018), hace mención que las empresas requieren servicios tecnológicos que garanticen a sus clientes el alcance a la información, para ello presentan que las principales problemáticas que se presentan en las empresas es la ausencia de seguridad de la información, presentando muchas veces vulneración interna y externa de los datos. Carvajal et al. (2019), en la misma línea registran que los problemas de las empresas es la falta de preocupación por mejorar su capacidad tecnológica y dejan de lado la inversión en sistema informáticos, lo que ocasiona que sus procesos sean extensos y generen incomodidad en los usuarios por el tiempo que les toma ser atendidos.

En el Caso de Perú Rodríguez et al. (2020), evidencian los problemas tecnológicos por lo que afrontan las empresas del país y en el sector público se hace más evidente, porque gran parte de las entidades públicas no se preocupan por optimizar sus procesos por medio de implementación de soluciones tecnológicas, presentando que no cuentan con un plano de red, no se tiene protocolos de seguridad y acceso a la información que maneja las entidades públicas. Con el análisis se tiene que los problemas por lo que se afronta nuestro país por la pandemia ha puesto en evidencia la falta de preocupación por la capacidad tecnológica que se presenta las entidades públicas del país.

Los gobiernos locales de las zonas alejadas de la capital son las más presentan estas dificultades tecnológicas y los servicios que brindaban fueron paralizadas durante la pandemia.

1.2 Definición del problema

De lo mencionado en los diferentes contextos se tiene que la Municipalidad Provincial de Huaraz, al igual que toda entidad pública presenta inconvenientes en el campo

tecnológico, evidenciándose en la ausencia de la seguridad de la información, al no contar con equipos tecnológicos que aseguren a la información que se maneja en la entidad, por otro lado se puede evidenciar que el cuarto de telecomunicaciones no cuenta con los protocolos de seguridad necesarios que aseguren a la información que se maneja en la entidad, además de ello el personal no se encuentra capacitado para que pueda administrar de manera eficiente los recursos con los que se cuenta. Los servidores se encuentran desfasados tecnológicamente, además el cableado actual presenta un desorden en cuanto a tiempo de vida y las modificaciones realizadas con el pasar de los años. A lo mencionado se suma que no se cuenta con un UPS que garantice la estabilidad eléctrica de los equipos del data center, por lo cual se encuentra expuesto a pérdida de información y fallas de los equipos.

Lo mencionado ha ocasionado que los usuarios sientan insatisfacción frente al servicio que brinda el área de informática porque se ha evidenciado que, en algunas áreas críticas como renta, logística, entre otras donde se realizan operaciones a diarias con el sistema de la entidad, se ha perdido la conexión y generado que se retrase con los trabajos que se realizan a diario.

Todo lo descrito hace referencia que existe la necesidad de contar con una solución tecnológica que garantice la estabilidad y seguridad de la información que se maneja en la entidad.

1.2.1 Problema general

¿Cómo la infraestructura de un data center índice en la seguridad de la información (ISO 27001) de la Municipalidad Provincial de Huaraz – 2021?

1.2.2 Problemas específicos

1. ¿De qué manera la infraestructura de un data center índice en la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021?
2. ¿De qué manera la infraestructura de un data center índice en la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021?
3. ¿De qué manera la infraestructura de un data center índice en los controles de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021?
4. ¿De qué manera la infraestructura de un data center índice en las acciones de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Demostrar como la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

1.3.2 Objetivos específicos

1. Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.

2. Comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.
3. Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.
4. Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.

1.4 Formulación de hipótesis

1.4.1 Hipótesis general

Hi: La infraestructura de un data center incide significativamente en la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

1.4.2 Hipótesis específicas

H1i: La infraestructura de un data center incide significativamente en la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

H2i: La infraestructura de un data center incide significativamente en la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

H3i: La infraestructura de un data center incide significativamente en los controles de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

H4i: La infraestructura de un data center incide significativamente en las acciones de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

1.5 Variables y dimensiones

Variable dependiente: Seguridad de la información (ISO 27001)

Variable independiente: Infraestructura de un data center

Definición conceptual de la seguridad de la información (ISO 27001)

Consiste en velar por la confidencialidad, integridad y disponibilidad de datos y para ello propone la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita tanto la gestión del azar como el control de la propiedad de datos con la que cuenta la empresa, además de la capacidad profesional que se cuenta para administrar y monitorear cada proceso (Gil y Gil, 2017).

Definición operacional de la seguridad de la información (ISO 27001)

Se refiere a forma de administrar los datos e información que se maneja dentro de la municipalidad por parte de las autoridades y del personal de informática, para ello en el estudio se analizó mediante la aplicación de un instrumento que permite su alcance y utilidad.

Definición conceptual de la infraestructura de un data center

Un centro de datos, o "Data Center" es una gran instalación, creación o construcción donde se alojan y mantienen numerosos dispositivos digitales que incluyen servidores, amantes, conexiones y diferentes activos necesarios que podrían usarse para mantener una red o un dispositivo de computadora sistemas, hechos, conexiones y estadísticas de una o más corporaciones (Said et al., 2015).

Definición operacional de la infraestructura de un data center

Se considera a la capacidad física con la cuenta la municipalidad, desglosado en los procesos que se deben seguir para su implementación y monitorio de los procesos seleccionados durante el proceso de funcionamiento.

Operacionalización de variables:

Tabla 1. Variable dependiente seguridad de la información (ISO 27001)

Dimensiones	Indicadores	Ítems	Escala y valores	Niveles
D1: planificación	Política de seguridad	1	1. Nunca	Deficiente
	Alcance del SGSI	2	2. Casi nunca	Regular
	Análisis de riesgo	3	3. A veces	Eficiente
	Selección de controles	4	4. Casi siempre	
	Competencias profesionales	5	5. Siempre	
	Mapa de procesos	6		
	Funciones y responsabilidades	7		
D2: Implementación de la seguridad	Gestión de riesgos	8,9		
	Administración del SGSI	10,11		
	Implementación de controles	12,13		
D3: Implementación de los controles	Revisión del SGSI	14		
	Auditorías internas	15,16		
	Medidas correctivas	17,18		

	Supervisión de la gerencia	19
D4: Implementación de las acciones	Acciones correctivas	20,21
	Optimización de los procesos	22,23

Fuente: ISO 27001

Tabla 2. Variable independiente infraestructura de un data center

Dimensiones	Indicadores	Escala y valores	Niveles y rango
D1: Espacio del sitio y su disposición	Cuarto de Entrada	En el caso del estudio no se considera escala y valores porque se desarrolla la estrategia para aplicar y diseñar el data center, evidenciando el efecto que tendrá en la seguridad de la información.	Al ser la variable que se manipula no presenta niveles y rangos para ser analizados.
	Área de distribución principal (Main distribution área MDA)		
	Área de distribución (Horizontal distribution area HDA)		
	Área de distribución de zonas (Zone distribution área ZDA)		
D2: Infraestructura del cableado	Área de distribución de los equipos (Equipmenet distribution área EDA)		
	Racks y gabinetes		
	Sistemas de tendido de cable		
D3: Tier y niveles de disponibilidad	TIER I: Centro de datos Básico		
	TIER II: Centro de datos Redundante		
	TIER III: Centro de datos Concurrentemente Mantenibles		
	TIER IV: Centro de datos Tolerante a fallos		
D4: Consideraciones ambientales	Energía eléctrica		
	Sistema de Enfriamiento		

Fuente: Norma TIA/EIA-942

1.6. Justificación de la Investigación:

La justificación se considera por Sánchez y Reyes (2015), como por qué y para que se desarrolla el estudio en el campo social, campo practico, luego en el campo metodológico

y finalmente en el campo teórico. Para ello se tiene que en el campo social el estudio al ser desarrollado beneficia tanto a la municipalidad, como a los usuarios que recurren a realizar sus trámites, porque al implementar el Data center permitió que los procesos que contaba la municipalidad se mejoren y algunos de estos se automaticen, por medio de la aplicación de sistemas informáticos que faciliten la interacción de los usuarios con los procesos administrativos que brinda la entidad. Por otro lado, en el campo practico al desarrollar el estudio se tiene resultados estadísticos comparativos de antes y después de la implementación con lo que se puede asegurar los procesos mejorados de la municipalidad y el impacto que presento la implementación del data center en la seguridad de la información de la municipalidad. Luego al desarrollar la justificación metodológica se tiene que al desarrollar el estudio se requiere que se desarrolle un instrumento que permita el análisis del impacto de la propuesta tecnológica basada en el desarrollo del DATA center con los protocolos que involucran la norma ISO 27001, finalmente dentro del desarrollo de la justificación teórico, el estudio presento conclusiones que fueron de gran importancia para entidad y que pueden ser utilizados en futuros estudios como antecedentes para seguir profundizando sobre esta problemática que ocurre en diferentes partes del país.

CAPÍTULO II

2. MARCO TEÓRICO

2.1 Antecedentes de la investigación

2.1.1 Antecedentes nacionales

Montaño y Bustíos (2020), realizaron un estudio que se basa en desarrollar un análisis y la propuesta de un Data Center para un gobierno local de Lambayeque, con las consideraciones necesarios para asegurar la información de la municipalidad, durante este proceso se tomó en cuenta los procesos del lineamiento que se establece en el método científico, logrando concluir: Se hizo viable optimizar y mejorar sistemas informáticos como “SIAF, SIGA, SISGEDO y SiSPLANI”, los más importantes, ya que se generó un sistema rápido en términos de procesamiento y transferencia de registros con diseño comunitario jerárquico, el uso de equipos contemporáneos y ancho de banda de trescientos Mbps, que garantizan mejoras de respuesta en transferencias monetarias, movimientos de presupuesto, consultas a bases de datos y reportes del componente ejecutivo, comunes a estos enfoques informáticos del Municipio.

Taco (2019), presento en Tacna un estudio que se basa en desarrollar una propuesta tecnológica que fortalezca la comunicación de datos de una empresa eléctrica de la ciudad, para ello presento como objetivo general implementar una solución tecnológico que garantice la información de la empresa y proteja la seguridad de datos, durante este proceso se encamino en el enfoque cuantitativo, presentados resultados comparativos del antes y después de la implementación propuesta, logrando concluir: “Fue viable decidir que la herramienta RACKTABLES DCIM permite optimizar la gestión de equipos Data Center de una empresa energética dentro de la ciudad de Tacna”, en este ejemplo a partir de la aplicación de RACKTABLES DCIM. Esto se pone a prueba a nivel estadístico dado el nivel de importancia calculado bajo 0.05, lo que verifica en grado cuantitativo que la Gestión de los equipos que integran un Data Center es sumamente crucial para generar ventajas en los niveles de gestión de las ofertas y deseos del empleador. Fortalecimiento empresarial en la metrópoli de Tacna.

Flores (2018), realizo una propuesta de una red de datos para un instituto de Apurímac, para ello se basó en los lineamientos del método científico, presentando como objetivo analizar y determinar los puntos vulnerables de la entidad, luego realizar la propuesta tecnológica que permita resolver la situación actual de la empresa, para ello se basó en el enfoque cuantitativo, presentando resultados numéricos de los hallazgos que se presenten en el estudio, logrando concluir: La propuesta técnica y económica para implementar la red de datos y el centro de datos es viable de ser implantada por Instituto de Educación Superior Tecnológico Público Todas las Artes, ya que se realizó un análisis de costos y perfiles técnicos de todos los dispositivos y elementos necesarios para construir la red de datos con cableado estructurado y el centro de datos.

Velasco (2019), presento su estudio con la finalidad de analizar y desarrollar una propuesta tecnológica basado en un Data Center con la norma ANSI/BICSI-002-2014 para

una empresa de Lima, para ello presento como principal objetivo conocer la situación actual de la empresa, detallando los problemas más relevantes y planteando la solución tecnológica que ayude a resolver los problemas registrados, logrando concluir: con el análisis se pudo evidenciar los problemas de vulneración de información que presentaba la empresa, luego al realizar la propuesta tecnológica y de implementarla se pudo dar a conocer las mejoras que se presentó y los beneficios que trajo para la empresa, asegurando la información y manteniéndola disponible.

Gil y Maihouri (2018), realizando un estudio que se basa en el análisis de un Data Center para una empresa de Lima, para ello presento como objetivo conocer como se encuentra actualmente la empresa y a través de los problemas que se encuentre establecer los lineamientos de una solución tecnológica que favorezcan a su manejo, logrando concluir: “Desacuerdo con el nivel de satisfacción de los empleados de la empresa Venus Peruana S.A.C. concluimos que se mejoró en 52 el número de empleados que opinan Muy de acuerdo sobre el nivel de satisfacción de los empleados de la empresa Venus Peruana S.A.C”.

2.1.2 Antecedentes internacionales

En esta parte del estudio se basa en la indagación de estudio similares en diferentes países y que brinde el soporte necesario para la viabilidad del estudio, detallando lo siguiente:

En Ecuador Espinoza (2021), desarrolló un estudio que se basa en “el diseño de un Data Center bajo la norma ANSI/TIA 942 para una empresa privada de Guayaquil”, para ello se basó en los lineamientos que se establecen en los estudios cuantitativos, presentando resultados estadísticos como resultados, luego se enfocó en el diseño experimental, presentando como conclusión: El diseño propuesto del intermedio de hechos

de Clase II cumple plenamente con lo estipulado en la ANSI / TIA 942 general hecha para cada subsistema: mencionando que para el subsistema que pertenece al área de telecomunicaciones se establece en: cables, racks, estantes y vías; en los subsistemas eléctricos que constituyen redundancia, topología de UPS y sistemas de puesta a tierra; En el subsistema mecánico, averiguando la cobertura adecuada en las cercanías del dispositivo de aire acondicionado, cumpliendo con todas estas sugerencias de diseño, la disponibilidad y confiabilidad se pueden suministrar dentro de los servicios brindados por Azotel S.A.

Del mismo modo se tiene el estudio de Juma (2017), en Ecuador desarrollo un estudio que se basa en el diseño de un Data Center para un gobierno local de Ibarra bajo la norma ANSI/TIA-942, para ello presento como objetivo general implementar el data center y ver efecto que tiene en el manejo de la información municipal, realizándolo bajo el enfoque cuantitativo, presentando resultados estadísticos antes y después de la implementación, logrando concluir: Con los resultados presentados de la comparación del antes y después de la implementación del Data Center se puede evidenciar mejoras significativas en la gestión de información de la municipalidad, además la seguridad aplicada en la implementación cumple con los estándares requeridos en todo el proceso. Por otro lado, la capacitación que recibió el personal fue de gran aporte porque favorece al trabajo que realizan en la administración del centro de datos.

Endara (2016), desarrolló una investigación que se basa en el análisis de un data center de una empresa privada de Ecuador, durante este proceso se basó en los procedimientos que se detallan en el método científico, aplicando el enfoque cuantitativo como estrategia para obtener datos, mostrando como objetivo conocer cómo se evidencia la infraestructura actual de la empresa y mejorarla con una propuesta tecnológica, logrando arribar a la conclusión: La arquitectura del centro de datos de Cisco tiene altos costos en comparación con las arquitecturas de otros fabricantes, sin embargo, es una de las mejores

del mercado en términos de infraestructura integrada. Al igual que el garaje, EMC VNX ocupa un lugar destacado en el cuadrante de Gartner de almacenamiento sólido. En cuanto a las licencias de virtualización, existen exquisitas alternativas disponibles en el mercado: VMware e Hyper V. Aunque Hyper-V tiene tarifas de bajo costo dentro del mercado, VMware es la generación más sólida en el mercado de la virtualización porque tiene funciones superiores. Una forma de mejorar el uso de fuentes de máquinas digitales mediante la optimización de la cantidad de RAM y procesador que devoran.

Mendoza y Moran (2017), se encargaron de desarrollar el estudio en Ecuador con el propósito de “implementar y realizar las configuraciones necesarias para un Data Center bajo la norma de una empresa de Ecuador”, para el desarrollo del estudio se basaron en los lineamientos que presentan los estudio cuantitativos, con ello se presentó los resultados de manera numérica y lograron concluir: Bajo la norma Normas TÍA 942 se logró implementar de manera eficiente el Data Center con los protocolos necesarios para que se brinde la seguridad de la información de la empresa, además de ello se presentó los problemas por los que afrontan las empresas, además en la fase de monitoreo se pudo evidenciar las fortalezas que género.

Bajo la misma línea se tiene a Mosquera (2016), con su estudio que se basó en el “análisis de los estándares internacionales para analizar la implementación de un Data Center”, con ello se presentó bajo los lineamientos que se establecen en el método científico, además bajo el diseño no experimental, encontrando como conclusión: Se considera que el centro de información de la PUCESE presenta debilidades en términos de infraestructura y seguridad de la información; Debido a la escasez de regulaciones de mitigación de peligros, que además pueden tener un efecto sobre la integridad y disponibilidad de las ofertas que se administran desde el centro de información de la

organización, se advierte en consecuencia trabajar en la implementación de los controles que reducen el peligro antes de materializando las vulnerabilidades citadas anteriormente.

2.2 Bases teóricas

Infraestructura de Data Center

En esta parte se detallan los lineamientos y fuentes teóricas registradas sobre la variable, mencionando lo siguiente:

“Los Centros de Datos o Centros de Procesamiento de Datos son salas especiales preparadas con mecanismos eléctricos, ambientales y de gestión del hogar en los que se alojan los sistemas de procedimientos, comunicación y almacenamiento de hechos” (Plazzotta et al., 2015).

Se basan en normas y requisitos globales para asegurar su funcionamiento y seguridad dentro del enfrentamiento de información, de acuerdo con las normas IEEE 802.3 y ANSI / TIA-942, la infraestructura de ayuda de un centro de registros debe estar compuesta por cuatro subestructuras, que incluyen, telecomunicaciones, arquitectura, sistema eléctrico y máquina mecánica, configurando cuatro niveles en función de la redundancia importante para llegar a esos niveles, que van desde el TIER1 hasta el TIER4 más alto, en el que se alcanza una disponibilidad de hasta el noventa y nueve,995% (Ramírez, et al., 2020).

El Data Center o conocido como centro de datos facilitan el procesamiento de información y datos de manera sistemática, que se logra mediante el uso de dispositivos de alta capacidad como servidores. Según Arizala y Ortiz (2010), delinean un medio de datos como: “El lugar donde se concentran todas las fuentes esenciales para el procesamiento de información de una empresa comercial, que adquiere la persona de Alta Disponibilidad cuando cumple con una secuencia de medidas. orientados a asegurar la disponibilidad del servicio, es decir, a que el proveedor opere las 24 horas del día”.

Estos Data Centers normalmente se realizan y mantienen a través de agencias masivas para que se pueda acceder a los registros necesarios para sus operaciones. Sin embargo, casi todas las empresas medianas o grandes cuentan con instalaciones de datos que durante los casos máximos no cumplen con los estándares mínimos importantes para asegurar la integridad en sus estructuras, siendo este un punto vital dentro de sus grupos (Plasencia y Calderón, 2016).

Los centros de datos no se describen a través de su longitud física o estilo. Las pequeñas corporaciones pueden funcionar de manera eficiente con más de un servidor y estructuras de garajes comunitarios dentro de un conveniente armario o sala pequeña, mientras que las grandes organizaciones de computación, incluidas Facebook, Amazon o Google, pueden llenar un área de almacén masiva con el sistema. Infraestructura y centro de información. "En otros casos, los centros de estadísticas pueden establecerse en instalaciones celulares, incluidas las cajas de entrega, también llamado centro de datos de un solo contenedor" (Godinho & Bigelow, 2017).

El diseño del centro de datos también debe contratar prácticas de seguridad y protección. Por ejemplo, la protección a menudo se refleja en el diseño de la entrada a las puertas y pasillos, que deben adaptarse al movimiento de equipos portátiles grandes y difíciles de manejar, así como permitir que los empleados accedan y reparen la infraestructura. La extinción de incendios es cualquier otra área clave de protección, y el uso generalizado de sistemas eléctricos y electrónicos sensibles y de potencia excesiva se opone a los rociadores no inusuales. En cambio, los centros de datos suelen utilizar estructuras químicas de extinción de incendios que no dañan el medio ambiente, que eliminan de forma eficaz una chimenea de oxígeno al tiempo que mitigan los daños colaterales al dispositivo. Dado que el centro de información también es un negocio intermedio activo, las medidas de seguridad integrales, junto con los naipes de acceso y la

videovigilancia, ayudan a localizar y evitar la apropiación indebida de personal, contratistas e intrusos (Alcocer, 2010).

La norma TIA/EIA-942 Cubre las siguientes áreas:

La primera región es la distancia del sitio web y su diseño tiene los siguientes componentes: Sala de entrada, alberga los equipos de los operadores telefónicos. Puede estar en el centro de registros, pero la norma recomienda que esté o no en una habitación separada por razones de seguridad. Vecindad de distribución principal (MDA), la red de distribución primaria alberga el factor de conexión de paso significativo para la máquina de cableado estructurado del centro de datos. Esta ubicación debe colocarse en un lugar importante para evitar que se excedan las distancias de cableado aprobadas. Ubicación de distribución (ubicación de distribución horizontal HDA), “la ubicación de distribución horizontal es el lugar de las interconexiones horizontales, el punto de distribución para el cableado a las áreas de distribución de dispositivos”. El lugar de distribución de zona (ZDA) es la red del cableado dependiente para el dispositivo que va al piso y no puede recibir paneles de conexión. El área de distribución de equipos (ubicación de distribución de Equipmenet EDA), es el lugar de los gabinetes y racks de dispositivos. “La regla precisa es que los estantes y racks deben ubicarse en una configuración de pasillo cálido / pasillo frío para que disipen correctamente el calor del dispositivo electrónico” (Amoroso y Costales, 2016).

La segunda área es infraestructura del cableado, corresponde a los racks y gabinetes, la gestión de cables comienza con los racks y estantes, que deberían ofrecer un control de cables horizontal y vertical generalizado. El control adecuado ahora no mantiene el cableado organizado de la mejor manera, sino que también mantiene el equipo frío al eliminar los límites del movimiento del aire. Estas características de los administradores de cables deben proteger los cables, asegurarse de que los límites del radio de curvatura no se

entreguen y controlar la holgura del cable de manera eficaz. “Los sistemas de enrutamiento de cables, una clave para lograr el enrutamiento de cables ideal es tener tremendas rutas de cables por encima y por debajo del suelo. Utilice el curso bajo el piso para el cableado permanente y la dirección del pináculo para el cableado transitorio” (Vázquez, 2015).

La tercera área es Tier y niveles de disponibilidad, proporciona medidas específicas para el medio estadístico sobre la oferta de los servicios que ofrece. Establece 4 etapas (TIERs), esos niveles sugieren el nivel de confiabilidad del centro de datos relacionado con 4 grados de disponibilidad descritos, los cuales pueden ser: TIER I: Información básica media; NIVEL II: Centro de datos redundante; NIVEL III: Centro de datos de mantenimiento simultáneo; “NIVEL IV: Centro de datos tolerante a fallas; Cada nivel de Tier se subdivide en 4 subsistemas basados en Telecomunicaciones; Arquitectura; Sistema eléctrico y sistema mecánico” (Plasencia y Calderón, 2016).

La cuarta área hace referencia a consideraciones ambientales, existen condiciones ambientales que se deben considerar, estas incluyen:

La energía eléctrica determina los requisitos de fuerza basados totalmente en la disponibilidad y puede consistir en uno o más recursos de fuerza, UPS, etc. Para estimar la ingesta de electricidad de la electricidad se debe completar una evaluación de regalos y también pensar en la redundancia y el auge futuro. Sistema de enfriamiento, se recomienda usar un dispositivo de enfriamiento adecuado. Además, “indica que los estantes y estantes deben ordenarse teniendo en cuenta el nuevo pasillo y la muestra del pasillo sin sangre. En los pasillos fríos, los grupos pueden organizarse cara a cara. En pasillos cálidos, el sistema se puede organizar de manera contraria” (Orozco, 2016).

Características de un Data Center de Alta Disponibilidad, muchos son los rasgos que determinan los rasgos de un Data Center de Alta Disponibilidad, apoyándose en los niveles de seguridad deseados o el flujo de estadísticas en la red, sin embargo, sin importar si es de

un Data Center destinado para sostener las notas de los estudiosos de una pequeña escuela o si hablamos del Centro de Datos de la NASA, sus rasgos se pueden resumir de la siguiente manera: “Conectividad de red, Protección física y lógica, Fiabilidad de la información, Disponibilidad permanente, Escalabilidad de la infraestructura, Protección del medio ambiente y gestión de riesgos” (Moreira, et al., 2017).

Conectividad de red, las redes de portátiles son el principal mecanismo de conectividad en un entorno electrónico. Una comunidad está formada por varios sistemas informáticos vinculados de forma estresada o inalámbrica para que los registros u otros activos puedan pasar por alto para ser compartidos. Cuando hablo de Conectividad en la comunidad, entonces se refiere al nivel de eficiencia con el que los dispositivos digitales logran vincularse dentro de la comunidad para lograr su objetivo fundamental de compartir fuentes. Normalmente existen cinco formas de redes desde el punto de vista de su lugar de efecto: “Red de área personal (PAN), Red de área local (LAN), Red de área de campo (CAN), Red de área metropolitana (MAN) y Área amplia Red (WAN)”, aunque también se pueden categorizar según la época utilizada para la interconexión. Sin embargo, el máximo aspecto imprescindible a tener en cuenta para lograr una conectividad excesiva es el uso de protocolos de comunicación. En una red, los formatos de estadísticas únicos se comparten por medio de diferentes estructuras de computadoras portátiles, que tienen numerosas especificaciones de programas de “hardware y software”, los protocolos de comunicación intentan romper esta disparidad y, como resultado, la información se puede compartir y procesar de manera adecuada (Vega, et al., 2020).

La protección física y lógica, el potencial para defender físicamente las pertenencias y los activos es una consideración vital en la estrategia de seguridad de una organización. Ya sea porque su tema principal es la seguridad de su fuerza laboral, la seguridad de sus hechos y sistemas, o la protección de su dispositivo clave. Entre los requisitos de seguridad

física que se pueden tomar en consideración se encuentran las estructuras de alarma, rastreo, personal en el sitio web las 24 horas de la tarde e incluso la implementación de biometría de acceso a las estructuras; “En cuanto a lo que tiene que ver con la seguridad lógica, mencionaremos la periodicidad de las actualizaciones de la máquina, réplicas de disco, autenticación y autorización de cuentas, cifrado, instalación de firewalls, antivirus, etc., que dan la certeza de la confiabilidad del sistema de información” (Camargo, et al., 2015).

La confiabilidad de la información, en informática, se refiere a la confiabilidad como la capacidad de un dispositivo para realizar y conservar sus funciones en situaciones habituales, adversas o repentinas durante un cierto período de tiempo; Es un atributo de cualquier factor relacionado con la computadora portátil (software, hardware, comunidad, etc.) que se adapta continuamente a sus especificaciones. En principio, un producto confiable está totalmente libre de errores; en el ejercicio, pero la fiabilidad de un dispositivo se expresa con frecuencia como un porcentaje. “Los productos informáticos están evolucionando continuamente en variaciones (después de un período de tiempo gigante) que normalmente se puede considerar como de mayor confiabilidad, los centros de datos de alta disponibilidad buscan minimizar los tiempos de inactividad y para esto utilizan recursos como la redundancia de datos y la virtualización de la información” (Couto, 2016).

La redundancia son las pertenencias de los mensajes supuestamente para la conversación que consisten en tener partes predecibles a partir de la relajación del mensaje y que consecuentemente en sí mismos no aportan nuevos hechos ni "repiten" una parte de los registros. En muchas aplicaciones, la redundancia es una estrategia ampliamente utilizada para evitar malentendidos o errores de descifrado. Descriptivamente, “la redundancia constituye un tema comunicativo estratégico que consiste en intensificar,

subrayar y repetir las estadísticas contenidas dentro del mensaje para que el ruido no provoque una falta esencial de datos, esto se logra con la implementación de sistema incluyendo routers, switches, y muchos otros” (Turgut y Kürat, 2014).

“La virtualización se refiere a la abstracción de las fuentes de una computadora, conocida como Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware del dispositivo físico (host)” y el dispositivo en ejecución del sistema digital (máquina virtual, visitante). , siendo un medio para crear una versión virtual de una herramienta o recurso útil, incluido un servidor, una herramienta de almacenamiento, una comunidad o tal vez un dispositivo operativo, en el que el recurso se divide en uno o más entornos de ejecución. “El dispositivo virtual preferido es un sistema en ejecución completo que se ejecuta como si estuviera instalado en una plataforma de hardware independiente. Normalmente, muchas máquinas digitales se simulan en una PC importante” (Vargas, 2020).

Para que funcione el dispositivo de ejecución "invitado", la simulación debe ser lo suficientemente grande (“siempre dependiendo del tipo de virtualización”). Los entornos virtualizados permiten a las agencias transportar desde un servidor simple o un modelo de aplicación fácil, “a una versión que puede proporcionar activos para múltiples aplicaciones virtualizadas dentro de un servidor corporal, reduciendo los gastos de trabajo, el consumo de energía y el área corporal” (Couto, 2016).

La disponibilidad permanente, la disponibilidad excesiva (alta disponibilidad) es un protocolo de diseño de dispositivo y su implementación asociada que garantiza un diploma casi absoluto de continuidad operativa a lo largo de una duración de medición determinada. El período de tiempo Disponibilidad o "Tiempo de actividad" se refiere a la capacidad de la red de consumidores para ingresar al sistema, publicar nuevos trabajos, reemplazar o alterar los trabajos actuales o recopilar los resultados de trabajos anteriores, es mucho la

capacidad de una computadora o computadora portátil para funcionar absolutamente sin interrupciones. “La disponibilidad y el rendimiento energético son dos de los estándares asociados con un centro de datos que puede estar motivado al máximo al organizar los requisitos iniciales para una nueva misión o al evaluar una configuración actual” (Vargas, 2020).

Escalabilidad de la infraestructura, “se refiere a la capacidad del dispositivo de PC para alternar su longitud o configuración para evolucionar a situaciones cambiantes”. Por ejemplo, una universidad que establece una red de consumo de Internet para un maestro que construye y no solo desea que su dispositivo portátil tenga la capacidad de acomodar a los clientes actuales, que son todos instructores, sino también a los clientes que pueda tener dentro del destino. Dado que hay profesores itinerantes que requieren de la comunidad para algunos paquetes educativos, para esto es vital implementar respuestas que apoyen el aumento de la red sin disminuir la oportunidad de su uso y reutilización, o que sea capaz de cambiar su configuración. sí es esencial; “La infraestructura de un centro de datos de alta disponibilidad debe ofrecer la flexibilidad importante para permitir que dichos ajustes se realicen a partir de su diseño” (Camargo, et al., 2015).

El diseño de un Data Center comienza con la selección de su área geográfica, y exige una estabilidad entre diferentes factores: costo monetario, infraestructuras a tener cerca, riesgo, etc., una vez que se ha decidido la región, es vital encontrar dependencias adecuadas a su causa, ya sea un local de nueva construcción o uno actual para comprar o alquilar. Aunque se disponga de las premisas adecuadas, siempre es imprescindible el despliegue de alguna infraestructura en el interior: “falsos suelos y falsos techos, cableado comunitario y de telefonía móvil, instalación de alarmas, control de temperatura y humedad con avisos SNMP o SMTP, y muchos otros”. Una parte especialmente importante de estas infraestructuras son las destinadas a la protección física de la

instalación, que incluye: cerraduras electromagnéticas, cámaras de seguridad, naipes de identidad, etc. Una vez acondicionada la cabina, se montan los ordenadores, redes de lugares cercanos, etc. Este desafío exige un diseño lógico de las redes y los entornos, especialmente por motivos de protección. Por lo general, todos los servidores enormes se concentran típicamente en una sala denominada "cámara fría", "refrigerador", "pecera" (o sitio). Esta sala requiere una máquina de enfriamiento seleccionada para mantener una temperatura baja (entre 21 y 23 rangos Celsius *), esencial para evitar averías en el portátil por sobrecalentamiento. Según los estándares internacionales, la temperatura exacta debería ser de 22,3 grados Celsius (Vargas, 2020).

La protección del medio ambiente, la moda de los nuevos Data Centers, patronizando el medio ambiente, está más cerca de los Green Data Centers ("Centros de Datos Ecológicos"), en los que la mecánica, las luces, la fuerza y los sistemas informáticos están diseñados para cosechar la máxima electricidad verde y el mínimo impacto ambiental. La producción y operación de esas instalaciones consiste en avances y estrategias tecnológicas, que incluyen el uso de sustancias de construcción de bajas emisiones, reciclaje de residuos, instalación de convertidores catalíticos en molinos de respaldo, uso de vehículos híbridos o eléctricos, etc. La construcción de un centro de datos ecológico con licencia puede ser una pieza costosa, sin embargo, al final, los ahorros se pueden ver en los gastos de operación y mantenimiento. "Otro beneficio es el hecho de que las instalaciones sin experiencia ofrecen al personal un ambiente de trabajo relajado y saludable, además de mejorar las relaciones con las comunidades del vecindario" (Camargo, et al., 2015).

Gestión de riesgos, el fallo de una máquina informática puede provocar pérdidas de productividad y de efectivo y, en determinados casos esenciales, incluso pérdidas de ropa y de personas. Por este motivo, es fundamental valorar los peligros asociados al mal

funcionamiento (avería) de uno de los aditivos de un dispositivo portátil y anticipar el acercamiento y las medidas para evitar incidencias o restaurar el portador en un tiempo aceptable. Como se sabe, una máquina informática comunitaria puede fallar de muchas formas (Luzbet y Laurencio, 2020).

Dado que los desastres no se pueden prevenir por completo, existe un enfoque para configurar los mecanismos de redundancia mediante la duplicación de fuentes vitales. La capacidad de un dispositivo para funcionar a pesar de que algunos de sus componentes fallan se conoce como tolerancia a fallas. “Cuando uno de los activos falla, los otros activos siguen funcionando mientras los administradores del sistema buscan una estrategia para evitar problemas”. Esto se conoce como "Servicio de protección contra fallas" (FOS). Idealmente, si ocurre una falla en la tela, los objetos de tela defectuosos deberían ser intercambiables en caliente, es decir, capaces de ser eliminados y reemplazados sin interrupción en el servicio.

“La configuración de una arquitectura redundante garantiza la disponibilidad de los registros del dispositivo, pero no lo protege de los errores del consumidor o de los errores naturales, como incendios, inundaciones o tal vez terremotos”. Por lo tanto, es muy importante proporcionar mecanismos de respaldo (preferiblemente lejanos) para garantizar la continuidad de los hechos. Además, también se puede utilizar un mecanismo de respaldo para comprar documentos, es decir, para comprar estadísticas en un país que corresponde a una fecha positiva (Luzbet y Laurencio, 2020).

Seguridad de la información

En esta parte se detallan los lineamientos y fuentes teóricas registradas sobre la variable, mencionando lo siguiente:

Godoy (2014): “La seguridad de la información está destinada a proteger las estructuras de datos y acceso, uso, divulgación, interrupción o destrucción no autorizados. La seguridad es un concepto asociado con la actualidad, la pérdida de amenaza o la contingencia”. Ser capaz de entender como seguridad de una empresa de cualquier gadget o forma de hechos (portátil o ahora no) que indique que esta máquina o información está libre de riesgo, daño o amenaza. Entender como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados adquiridos. Al mismo tiempo, considera que la seguridad de la información es el conjunto de medidas preventivas y reactivas de las corporaciones y estructuras tecnológicas que permiten resguardar y blindar los hechos, buscando preservar su confidencialidad, disponibilidad e integridad.

De acuerdo con la ISO 27001: 2013 ISO (Estándar) (“Organización Internacional de Normas”) (2013): “Seguridad de la información, evita las informaciones de una amplia gama de amenazas, si desea asegurar la continuidad de la empresa, minimizando el daño y maximizando la retorno de inversiones y nuevas posibilidades”. Asimismo, considera la vida de los hechos en numerosas formas que incluyen; publicado o escrito en papel, acumulado electrónicamente, transmitido con la ayuda de manera electrónica, presentado en instantáneas o expuesto en comunicado. Cualquiera que sea la forma de las estadísticas, o el medio por el cual se distribuyen o centralizan (almacenamiento), siempre deben estar protegidas y salvaguardadas de manera adecuada con la intención de mantener la confidencialidad, integridad y disponibilidad de los términos que constituyen la base. En el que se fundamenta todo el edificio de la seguridad estadística. Y para asegurarse de que la seguridad de los registros se gestiona de forma eficiente, se debe utilizar, documentar y reconocer de manera sistemática a través de toda la empresa, desde un enfoque de riesgo empresarial. Esta forma es lo que constituye un SGSI.

Según Fernández (2012): La información es tan importante para las empresas como si hubiera sido la máquina circulatoria de las propias agencias y tal es el caso que requiere su seguridad ante cualquier asalto o amenaza, que ponga en peligro la empresa, tanto pública como personal, considerando que en cualquier otro caso se puede quebrar la salud organizacional. De hecho, las corporaciones enfrentan actualmente una gama excesiva de amenazas de falta de confianza provenientes de fuentes extraordinarias, entre las que podrían estar los nuevos negocios y equipos de TIC (“Tecnologías de la Información y la Comunicación”), que los CEO (“directores generales”) y CIO (“Directores de Tecnología de la Información”) deben seguir. y que la estadística, como una de las principales pertenencias de las empresas, debe ser cubierta mediante la implementación, protección y desarrollo de medidas de seguridad para que cualquier corporación logre sus objetivos comerciales, asegure el cumplimiento penitenciario, el prestigio y la imagen de la agencia.

Máquina de gestión de protección de la información ISO 27001. “Se argumenta que las informaciones, siendo un activo principal de las agencias, deben protegerse contra cualquier casualidad, mediante el mantenimiento y las medidas de seguridad de datos avanzadas”, es decir, tienen que proteger la salud organizacional con la ayuda de establecer Medidas preventivas de seguridad de registros debido al hecho de que las agencias están atravesando un alto nivel de amenaza e incertidumbres por la expansión de las fuentes, por lo que los “CEO y CIO” deben utilizar las herramientas de las Tecnologías de la Información para adquirir sus objetivos empresariales comerciales, prestigio, fotografiar y garantizar el cumplimiento penitenciario de la corporación.

Pallas, (2009): “El pilar principal de cualquier dispositivo de seguridad estadística o técnica de control de peligros y de la ISO / IEC 27001 de moda en sí misma, es la trilogía hecha de confidencialidad, integridad y disponibilidad, y debe enmarcarse dentro del entorno empresarial comercial”. El método organizacional y el marco del delito,

igualmente, sugiere que la protección estadística es un factor relevante más que un emprendimiento de representación estratégica, por lo tanto, debe prevalecer un criterio de desarrollo de Costo / Beneficio minimizando los riesgos, con el motivo de maximizar el resultado final. de los objetivos, y en línea con las prioridades determinadas por las empresas.

Godoy (2014), consideró los siguientes rasgos como pilares de la Seguridad de la Información. Confidencialidad: asegura que solo aquellas personas que tienen la autorización adecuada, puedan tener derecho de entrada a los registros. “Integridad: busca mantener la integridad de los datos y evitar cambios no autorizados. Disponibilidad: es el derecho de acceso a los sistemas y hechos en el tiempo requerido mediante el uso de hombres y mujeres autorizados”.

Areitio (2008), recuerdo que: Cada versión de protección se divide en tres áreas predominantes: “sistema de gestión de peligros, método de ingeniería de seguridad y procedimiento de garantía, áreas que funcionan juntas en un esfuerzo por asegurarse de que el proceso de seguridad logre sus objetivos”.

Proceso de riesgos: “Identifica y prioriza los riesgos inherentes a la mejora de un producto, sistema o empresa comercial, y es responsable de identificar y cuantificar la posibilidad de que ocurran amenazas y organizar los niveles deseables de peligro para la agencia”, pensando en el impacto de la capacidad de un incidente indeseable. Proceso de ingeniería: determina e implementa respuestas a los problemas provistos a través de amenazas y peligros, se desarrolla en fases especiales desde el concepto, diseño, implementación, verificación, implementación, operación y preservación hasta su eliminación. El equipo de ingenieros de protección trabaja con los clientes (“altos directivos, empleados, usuarios, compañeros de la empresa o entidades externas”) para identificar todas las necesidades de seguridad. Proceso de aseguramiento: determina el

grado de confianza en uno mismo que satisfacen las necesidades de seguridad; corrección, eficiencia, robustez y verificación. Proveedor de seguridad: permiten hacer cumplir la política de seguridad de una organización que organiza sistemas informáticos, seres humanos, gadgets, etc. Dentro de las estructuras de información. Con el objetivo de proteger todas las entidades identificables.

Burgos (2008), considero: que a pesar de que la versión PDCA es la ISO formal de moda, se trata de millas construidas sobre una base que no necesariamente observa a todas las agencias, en particular cuando ahora no se han preocupado por las estrategias relacionadas con las normas ISO, en consecuencia, sobre una base práctica. Se suministra la siguiente versión, que no pasa por alto ni restringe las actividades señaladas dentro del modelo formal, sino que las utiliza para ayudar a un trazado sensato de los deportes que deben ser incluidos para adquirir un nivel adecuado de protección estadística dentro de las regiones de TIC en cualquier tipo de empresa.

En el caso de las dimensiones de la variable se consideró al ciclo PHVA, al mencionar a la norma internacional se inclina al modelo de proceso "Planificar-Hacer-Verificar-Actuar" (PHVA) o la "rueda de Deming", eso se aplica a la estructura de todos los procesos de un dispositivo de control. A partir de lo anterior, tenemos cómo una máquina de control hace uso de los requerimientos y expectativas de los fascinados como input, y la forma, con los movimientos y estrategias importantes, se producen las consecuencias de seguridad de los hechos que satisfacen las necesidades y expectativas.

Planificar (“establecer el sistema de gestión”): “Establecer la política, objetivos, técnicas y procesos asociados con la gestión de peligros y la mejora de la protección estadística para proporcionar efectos consistentes con las reglas y objetivos globales de la empresa” (ISO 27001:2013).

Hacer (“implementar y operar el sistema de gestión”): “Implementar y hacer funcionar la política, los controles, los procedimientos y los procedimientos del dispositivo de gestión” (ISO 27001:2013).

Verificar (“monitorear y revisar el sistema de gestión”): Evaluar y, si corresponde, medir el desempeño de los procedimientos contra la política, los objetivos y disfrutar de manera realista y presentar los resultados a la gerencia para su evaluación (ISO 27001:2013).

Actualizar (mantener y mejorar el sistema de gestión): Realizar movimientos correctivos y preventivos, en base a los efectos de la evaluación de auditoría y control interno, o diferentes estadísticas aplicables para la mejora continua de dicho dispositivo (ISO 27001:2013).

2.3 Definición de términos

Estándar TIA-942

La TIA publica el TIA-942 Telecommunications Infrastructure Standard for Data Centers (“Estándar para la infraestructura de telecomunicaciones de centros de datos”), con la intención de unificar los criterios en el diseño de centros de datos. “El estándar especifica las características para la infraestructura de telecomunicaciones en el centro de datos y los servicios relacionados que serán el soporte para la tecnología de la información a instalar”, cubriendo aspectos como el Tiering, y la redundancia que harán que un centro de datos sea menos susceptible a las interrupciones debido a la falta de suministro de energía a los equipos activos.

ISO 27001

Se considera como una de las normas internacionales, divulgada durante el año 2005 y siendo revisada durante el 2006, que conceptualiza una agrupación de requerimientos para la implementación de un sistema basado en la gestión de seguridad de la información. Para

ello su aceptación por la ISO, esta norma era reconocida como BS 17799 Parte 2, que fue divulgada originalmente en 1999.

ISO/IEC 27002

Este es un manual de buenas prácticas para el control de la seguridad de los registros, este extendido anteriormente tenía el llamado de “ISO 17799: 2005 hasta 2007, donde pasó a llamarse ISO / IEC 27002: 2005”. Este preferido define los objetivos y sugerencias con respecto a la protección de la información y se anticipa a la globalización. preocupaciones de las empresas relacionadas con la seguridad de las estadísticas para sus actividades en moda. Lleva 39 objetivos de manipulación y 133 controles agrupados en 11 nombres de dominio. “Se publica en España como UNE-ISO / IEC 27002: 2009, en Venezuela Fondo ISO / IEC 27002, Argentina IRAM-ISOIEC 27002, Chile NHC-ISO27002, Perú NTP-ISO / IEC 27002: 2007”.

CAPÍTULO III

3. DISEÑO METODOLÓGICO

3.1 Tipo de investigación

De acuerdo a los lineamientos que presenta el estudio se encuentra dentro del paradigma positivista expuesto por Baena (2017), como un paradigma que se basa en analizar estudios en base a resultados números, dentro de este tipo de paradigma se encuentra el enfoque cuantitativo.

Según las características que presenta el estudio se considera de tipo aplicada, puesto que para desarrollar el estudio se realizan indagaciones y recopilación de información que sirvan de sustento para respaldar el estudio, seleccionado la información más relevante y planteando una solución a la problemática analizada en la municipalidad (Cabezas et al., 2018).

Con lo mencionado se ubica dentro del enfoque cuantitativo, porque se presentan resultados numéricos para dar respuesta a cada uno de los objetivos planteados en el desarrollo del estudio (Cohen y Gómez, 2019).

3.2 Diseño de la investigación

El diseño que se adapta al estudio es el experimental, porque se realiza la manipulación de una de las variables, para ello se encuentra dentro de ello en el pre experimental, porque se analiza al estudio en dos momentos, antes y después de la aplicación de la propuesta de solución que se basa en la implementación de una infraestructura de Data Center (Concepción, et al., 2019).

Con ello se tiene que presentó un alcance temporal longitudinal, porque se realiza el recojo de información en un primer momento que es antes de la aplicación de la infraestructura de data center y luego posterior a su implementación y se evidencia el efecto que causa en la seguridad de la información (Gallardo, 2017).

Para ello se tiene el siguiente esquema:

$$G: O_{Y_1} \quad x \quad O_{Y_2}$$

Donde:

G. : Grupo de estudio

O_{Y₁} : Observación de seguridad de información (Fase de diagnóstico)

O_{Y₂} : Observación de seguridad de información (Fase evaluativa)

3.3 Población y muestra

3.3.1 Población

Según Hernández y Mendoza (2018), “se considera a la totalidad de sujetos que integran una problemática y presentan las experiencias requeridas para responder a las interrogantes propuestas en el estudio”. En el caso del estudio la población estuvo conformada por 280 trabajadores nombrados de la municipalidad, quienes realizan labores administrativas y presentan experiencias con los sistemas y la infraestructura actual de la red.

3.3.2 Muestra

La muestra se considera por Montalván et al. (2019), como una porción o fragmento de la población que se extrae de manera probabilística, porque se aplican técnicas estadísticas que permiten su cálculo y determinación. En la selección de la muestra se aplicó la siguiente fórmula:

$$\text{Tamaño de la muestra: } n \cong 162; n = \frac{N \cdot 0,5^2}{\frac{(N-1) \cdot E^2}{C^2} + 0,5^2}$$

Donde: E = 0,05 = 5% (Error); C = 1,96 (Nivel de confianza)

Con los cálculos realizados se ha determinado que la muestra en el estudio la conforman 162 trabajadores nombrados de la municipalidad.

3.4 Técnicas para la recolección de datos

Técnica: Para el desarrollo del estudio se aplicó como técnica para el recojo de datos a la encuesta, definida por Navarro et al. (2017), expresan que se considera como “acción que se realiza en el estudio con el propósito de recopilar información que permita analizar cómo se presenta una problemática a través de percepciones que se recogen en el instrumento seleccionado para el estudio”.

Instrumento: En el caso del instrumento se utilizó el cuestionario, definida por Ochoa (2019), “como el medio tangible que tienen contacto los sujetos que presentan los conocimientos necesarios para que se pueda analizar una problemática”.

3.4.1 Descripción de los instrumentos

El instrumento se encuentra conformado por 23 ítems, para lo cual se tomó en consideración a la dimensión planificación que contiene a 7 preguntas, luego se tiene a la dimensión implementación de la seguridad que la componen del ítems 8 al 13, de ahí se tiene a la dimensiones implementación de controles que presenta las preguntas del 14 al 19, finalmente podemos ubicar a la dimensión implementación de acciones que componen

las preguntas del 20 al 23, para todo ello se considera una escala Likert de 5 opciones de respuesta.

3.4.2 Validez y confiabilidad de los instrumentos

Validez: En el caso de la validación se recurrió al juicio de expertos conformados por 3 profesionales con grado académico de maestría, a quienes se les entregó el formato de validación otorgado por la universidad, luego de ellos dieron su veredicto para determinar si el instrumento presenta las condiciones necesarias para ser aplicado al estudio.

APELLIDOS Y NOMBRES	CALIFICATIVO
Dr. Ing. Elvis Jerson Ponte Quiñones	ACEPTADO
Ms. Medina Lopez Walter Junior	ACEPTADO
Ms. Cacha Arana Cristhian Max	ACEPTADO

Confiabilidad: Para este proceso se recurrió a una prueba estadística determinar por el método de Alfa de Cronbach, para ello se tomó en cuenta a 15 trabajadores de la municipalidad que fueron excluido de la muestra; a estas personas se les aplicó el instrumento para luego ser tabulados en el programa SPSS 26.0, y poder calcular el Alfa de Cronbach, que determinar el grado de confiabilidad de un instrumento.

3.4.3 Técnicas para el procesamiento y análisis de los datos

En esta parte del estudio se detallan la manera y medios utilizados para analizar la información proporcionada por los sujetos de la muestra, para ello se tuvo en cuenta el uso del programa Excel 2019 y junto a el programa SPSS V. 26.0. En el caso de la tabulación de opiniones se realizó en Excel, luego por medio de la estadística descriptiva mostrar los resultados en tablas y figuras de frecuencias que permitan su análisis. Finalmente, para realizar la prueba de hipótesis se tuvo en consideración al método no paramétrico de

Wilcoxon con el cual se demostró el impacto que tuvo la implementación del Data Center en la seguridad de información de la empresa.

CAPÍTULO IV

4. PRESENTACIÓN DE RESULTADOS

En esta parte del estudio se dan respuesta a cada uno de los objetivos propuestos, presentándolos en tablas y figuras que permitan sus análisis de manera cuantitativa, por ubicarse en el enfoque cuantitativo, como primera parte se realiza el análisis por cada uno de los objetivos establecidos, luego de ello se realiza una prueba de normalidad para dar a conocer el método estadístico más adecuado para el estudio para realizar la prueba de hipótesis.

4.1 Presentación e interpretación de resultados en tablas y figuras

En esta parte del estudio se realizó un análisis comparativo de los resultados presentados en el pre test con los resultados alcanzados en el pos test, además se evidencia la variación obtenida entre ambos aspectos analizados, todo ello se realiza por medio de la estadística descriptiva.

4.1.1 Resultados de los objetivos

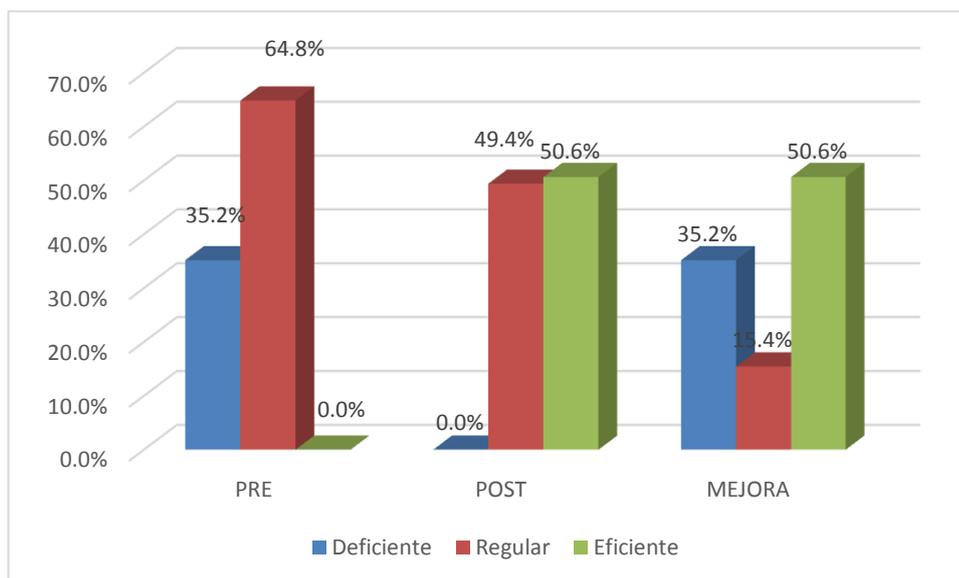
Según los resultados para el objetivo general:

Tabla 3. Demostrar como la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

Criterio	SEGURIDAD DE LA INFORMACION (ISO 27001)					
	PRE		POST		MEJORA	
	f _i	%	f _i	%	f _i	%
Deficiente	57	35.2%	0	0.0%	57	35.2%
Regular	105	64.8%	80	49.4%	25	15.4%
Eficiente	0	0.0%	82	50.6%	82	50.6%
Total	162	100.0%	162	100.0%		

Fuente: Aplicación de las encuestas a los trabajadores nombrados de la municipalidad.

Figura 1. Frecuencia de la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.



Fuente: Tabla 1.

Interpretación:

A través de la aplicación del instrumento se tiene que la implementación de la seguridad de la información (ISO 27001) presento diferencias entre el pre test y el pos test, para ello se

tiene que en el nivel bajo se registró que en el pre test se encontró que 57 trabajadores que representan el 35.2%, luego en el pos test se encontró que no se registró datos, minimizando el nivel en 35.2 %. Luego se registró que 105 trabajadores que conforman el 64.8% lo considera como regular en el pre test, luego en el pos test se encontró que 80 trabajadores que conforman el 49.4% lo ubican como regular, mejorando en 15.4%, luego se tiene que no se registran datos para el nivel alto, luego en el pos test se registró que 82 trabajadores que integran el 50.6% lo perciben como alto, obteniendo una mejora de 50.6%.

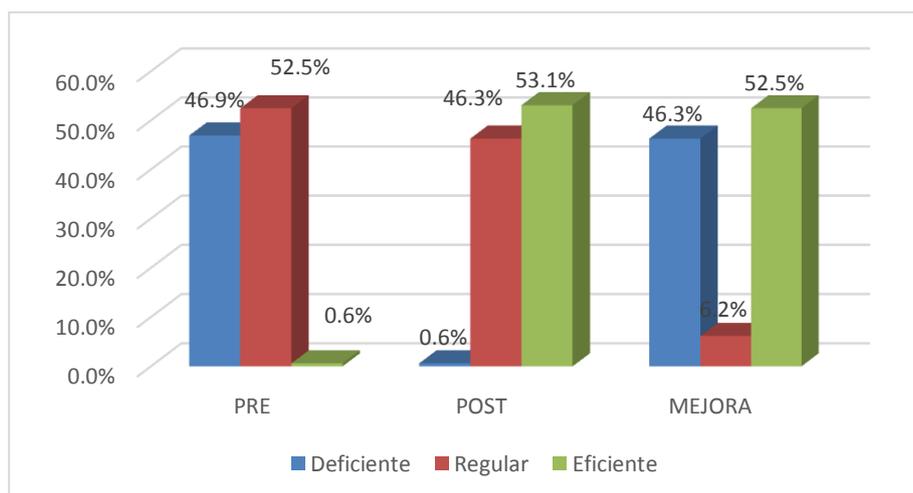
Según los resultados para el objetivo específico 1:

Tabla 4. Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.

Criterio	Planificación					
	PRE		POST		MEJORA	
	f _i	%	f _i	%	f _i	%
Deficiente	76	46.9%	1	0.6%	75	46.3%
Regular	85	52.5%	75	46.3%	10	6.2%
Eficiente	1	0.6%	86	53.1%	85	52.5%
Total	162	100.0%	162	100.0%		

Fuente: Aplicación de las encuestas a los trabajadores nombrados de la municipalidad.

Figura 2. Barra de los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.



Fuente: Tabla 2.

Interpretación:

A través de la aplicación del instrumento se tiene que la implementación de las acciones presento diferencias entre el pre test y el pos test para la planificación, mostrando que en el pre test se registró que 76 trabajadores que conforman el 46.9% lo encuentran en el nivel bajo, luego en el pos test se registró que 1 trabajador que conforma el 0.6% para el nivel bajo. Luego se tiene que 85 trabajadores que integran el 52.5% lo ubican en el nivel regular en el pre test, en comparación a 75 trabajadores que integran el 46.3% en el pos test, obteniendo una mejora de 6.2%. Al realizar el análisis del nivel alto se tiene que en el pre test se registró que 1 trabajador que conforma el 0.6%, en comparación a 86 trabajadores que integran el 53.1%, obteniendo una mejora del 52.5%.

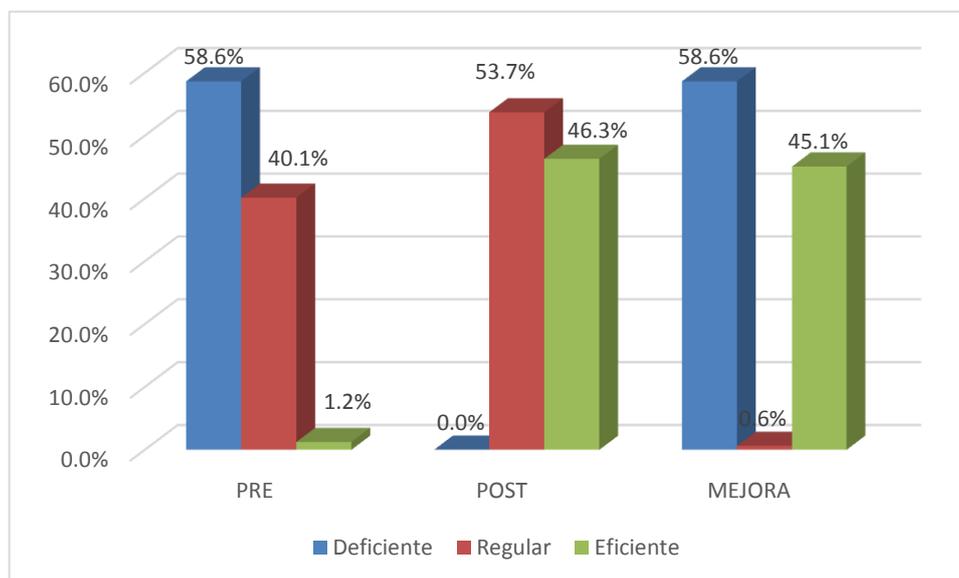
Según los resultados para el objetivo específico 2:

Tabla 5. Comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.

Criterio	Implementación de la seguridad					
	PRE		POST		MEJORA	
	f _i	%	f _i	%	f _i	%
Deficiente	95	58.6%	0	0.0%	95	58.6%
Regular	65	40.1%	87	53.7%	1	0.6%
Eficiente	2	1.2%	75	46.3%	73	45.1%
Total	162	100.0%	162	100.0%		

Fuente: Aplicación de las encuestas a los trabajadores nombrados de la municipalidad.

Figura 3. los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.



Fuente: Tabla 3.

Interpretación:

A través de la aplicación del instrumento se tiene que la implementación de las acciones presento diferencias entre el pre test y el pos test para la dimensión implementación de la seguridad, mostrando que en el pre test se registró que 95 trabajadores que integran el 58.6% lo encuentran como bajo, luego en el pos test se registró que ningún trabajador lo ubica en este nivel, minimizando en comparación del pre y pos test en 58.6%, luego se tiene que 65 trabajadores que corresponde al 40.1% lo encuentra como regular en el pre test, luego en el pos test se registró que 87 trabajadores que conforman el 53.7% lo ubican como regular, obteniendo una diferencia del 0.6%. Al realizar el análisis del nivel alto se tiene que 2 trabajadores que conforman el 1.2% lo encuentran en este nivel, en comparación al pos test que 75 trabajadores que conforman el 46.3% lo ubican en este nivel, haciendo una diferencia de 45.1%.

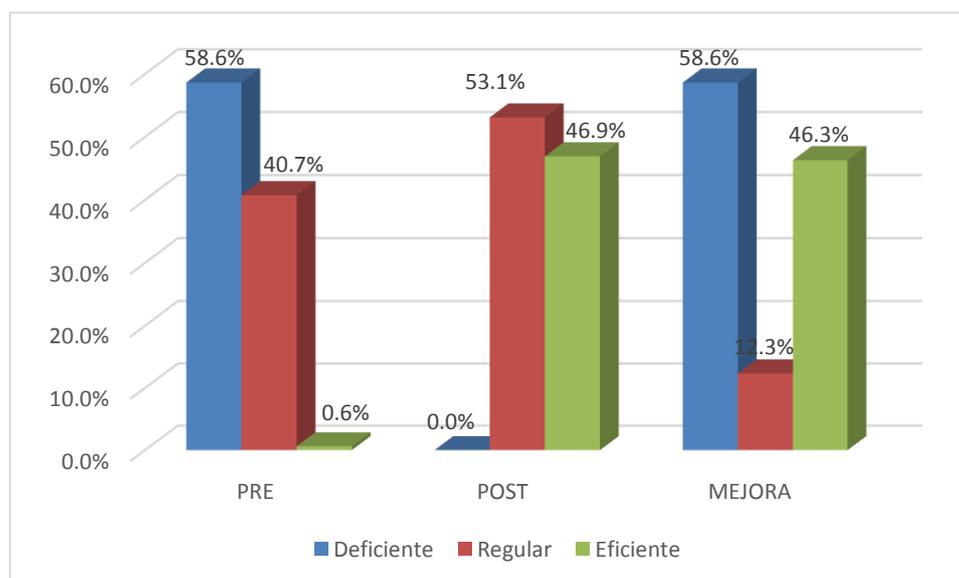
Según los resultados para el objetivo específico 3:

Tabla 6. Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.

Criterio	Implementación de los controles					
	PRE		POST		MEJORA	
	f _i	%	f _i	%	f _i	%
Deficiente	95	58.6%	0	0.0%	95	58.6%
Regular	66	40.7%	86	53.1%	20	12.3%
Eficiente	1	0.6%	76	46.9%	75	46.3%
Total	162	100.0%	162	100.0%		

Fuente: Aplicación de las encuestas a los trabajadores nombrados de la municipalidad.

Figura 4. Barra de los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.



Fuente: Tabla 4.

Interpretación:

A través de la aplicación del instrumento se tiene que la implementación de los controles presento diferencias entre el pre test y el pos test, evidenciando que para el nivel bajo presento en el pre test a 95 trabajadores que conforman el 58.6%, luego en el pos test no presento trabajadores para este nivel, haciendo una diferencia de 58.6%. Luego para el

nivel regular se registró que en el pre test se encontró que 66 trabajadores que conforman el 40.7%, luego en el pos test registro que 86 trabajadores que conforman el 53.1%, haciendo una diferencia del 12.3%. Para el nivel alto se tiene que 1 trabajador que conforman el 0.6%, luego en el pos test se registró que 76 trabajadores que conforman el 46.9%, haciendo una diferencia del 46.3%.

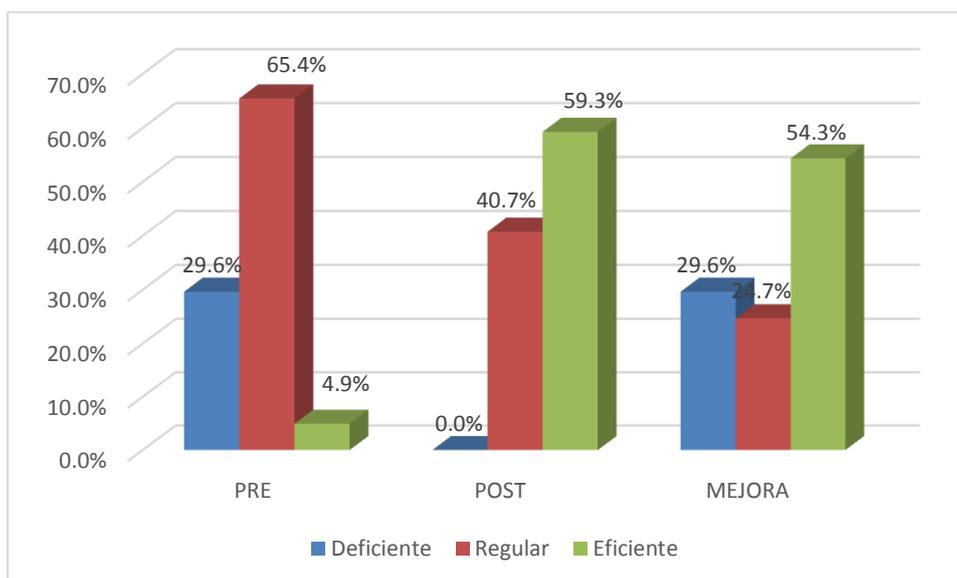
Según los resultados para el objetivo específico 4:

Tabla 7. Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.

Criterio	Implementación de las acciones					
	PRE		POST		MEJORA	
	f _i	%	f _i	%	f _i	%
Deficiente	48	29.6%	0	0.0%	48	29.6%
Regular	106	65.4%	66	40.7%	40	24.7%
Eficiente	8	4.9%	96	59.3%	88	54.3%
Total	162	100.0%	162	100.0%		

Fuente: Aplicación de las encuestas a los trabajadores nombrados de la municipalidad.

Figura 5. Barra de los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.



Fuente: Tabla 5.

Interpretación:

A través de la aplicación del instrumento se tiene que la implementación de las acciones presento diferencias entre el pre test y el pos test, evidenciando que para el nivel bajo presento en el pre test a 48 trabajadores que conforman el 29.6%, luego en el pos test no presento trabajadores para este nivel, haciendo una diferencia de 29.6%. Luego para el nivel regular se registró que en el pre test se encontró que 106 trabajadores que conforman el 65.4%, luego en el pos test registro que 66 trabajadores que conforman el 40.7%, haciendo una diferencia del 24.7%. Para el nivel alto se tiene que 8 trabajador que conforman el 4.9%, luego en el pos test se registró que 96 trabajadores que conforman el 59.3%, haciendo una diferencia del 54.3%.

4.1.2 Prueba de normalidad

En esta parte del estudio se realizó la prueba de normalidad de Kolmogorov-Smirnov^a para muestras superiores a 50, con ello se conoció la distribución de la muestra y la selección del método estadístico más adecuado para realizar la prueba de hipótesis.

Tabla 8. Prueba de normalidad de datos

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRE TEST	,101	162	,000	,929	162	,000
POS TEST	,074	162	,030	,975	162	,005

a. Corrección de significación de Lilliefors

Interpretación:

Para determinar el método estadístico más adecuado para realizar la comprobación de la hipótesis se realizó una prueba de normalidad de datos mediante el método de

Kolmogorov-Smirnov^a, por ser una muestra superior a 50, para ello se ha obtenido un valor de significancia de 0.000 para el pre test y en el pos test se ha registrado un valor de 0.030, en promedio el valor obtenido se ubica por debajo del 0.05, con lo cual se considera como sustento suficiente para afirmar que la muestra presenta una distribución no paramétrica y por ser un estudio pre experimental se determina que el método estadístico más adecuado es Wilcoxon para realizar la comprobación de la hipótesis.

4.2 Contrastación de hipótesis de la investigación

Tabla 9. Prueba para comprobar la hipótesis general

seguridad de la información (ISO 27001) Pre y Pos test	
Z	-11,051 ^b
Sig. asintótica(bilateral)	,001

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Interpretación:

Al realizar el análisis de la hipótesis se tiene en cuenta el valor de la significancia obtenido en el estudio, donde se registró un valor de 0.001, ubicado por debajo del 0.05, siendo de sustento suficiente para afirmar que hay una influencia, por lo tanto se procede con el rechazo de la hipótesis nula y se comprueba la hipótesis propuesta donde se afirma: La Infraestructura de un data center influye significativamente la seguridad de la información (ISO 27001) de la Municipalidad Provincial de Huaraz – 2021.

Tabla 10. Prueba para comprobar la hipótesis específica 1

Planificación de la seguridad de la información (ISO 27001) Pre y Pos test	
Z	-9,241 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Interpretación:

Al realizar el análisis de la hipótesis se tiene en cuenta el valor de la significancia obtenido en el estudio, donde se registró un valor de 0.001, ubicado por debajo del 0.05, siendo de sustento suficiente para afirmar que hay una influencia, por lo tanto se procede con el rechazo de la hipótesis nula y se comprueba la hipótesis propuesta donde se afirma: La infraestructura de un data center incide significativamente en la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

Tabla 11. Prueba para comprobar la hipótesis específica 2

Seguridad de la seguridad de la información (ISO 27001) Pre y	
Pos test	
Z	-10,570 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Interpretación:

Al realizar el análisis de la hipótesis se tiene en cuenta el valor de la significancia obtenido en el estudio, donde se registró un valor de 0.000, ubicado por debajo del 0.05, siendo de sustento suficiente para afirmar que hay una influencia, por lo tanto se procede con el rechazo de la hipótesis nula y se comprueba la hipótesis propuesta donde se afirma: La infraestructura de un data center incide significativamente en la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

Tabla 12. Prueba para comprobar la hipótesis específica 3

Seguridad de la seguridad de la información (ISO 27001) Pre y	
Pos test	
Z	-8,820 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Interpretación:

Al realizar el análisis de la hipótesis se tiene en cuenta el valor de la significancia obtenido en el estudio, donde se registró un valor de 0.000, ubicado por debajo del 0.05, siendo de sustento suficiente para afirmar que hay una influencia, por lo tanto se procede con el rechazo de la hipótesis nula y se comprueba la hipótesis propuesta donde se afirma: La infraestructura de un data center incide significativamente en los controles de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

Tabla 13. Prueba para comprobar la hipótesis específica 4

Acciones de la seguridad de la información (ISO 27001) Pre y	
Pos test	
Z	-10,025 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Interpretación:

Al realizar el análisis de la hipótesis se tiene en cuenta el valor de la significancia obtenido en el estudio, donde se registró un valor de 0.000, ubicado por debajo del 0.05, siendo de sustento suficiente para afirmar que hay una influencia, por lo tanto se procede con el rechazo de la hipótesis nula y se comprueba la hipótesis propuesta donde se afirma: La infraestructura de un data center incide significativamente en las acciones de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.

CAPÍTULO V

5. DISCUSIÓN

5.1 Discusión de resultados obtenidos

En esta parte del estudio se realiza la triangulación de información comparando los resultados obtenidos en el estudio con los trabajos preliminares y se realiza el sustento teórico que respalde el estudio, detallando lo siguiente:

Con referencia a lo propuesto como objetivo general que se basa en demostrar como la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021, se obtuvo como resultado que a través de la aplicación del instrumento se tiene que la través de la aplicación del instrumento se tiene que la implementación de la seguridad de la información (ISO 27001) presento diferencias entre el pre test y el pos test, para ello se tiene que en el nivel bajo se registró que en el pre test se encontró que 57 trabajadores que representan el 35.2%, luego en el pos test se encontró que no se registró datos, minimizando el nivel en 35.2 %. Luego se registró que 105 trabajadores que conforman el 64.8% lo considera como regular en el pre test, luego en el pos test se encontró que 80 trabajadores que conforman el 49.4% lo ubican como regular, mejorando en 15.4%, luego se tiene que no se registran datos para el nivel alto,

luego en el pos test se registró que 82 trabajadores que integran el 50.6% lo perciben como alto, obteniendo una mejora de 50.6%, datos que en comparación con lo registrado por Juma (2017), en Ecuador desarrollo un estudio que se basa en el diseño de un Data Center para un gobierno local de Ibarra bajo la norma ANSI/TIA-942, para ello presento como objetivo general implementar el data center y ver efecto que tiene en el manejo de la información municipal, realizándolo bajo el enfoque cuantitativo, presentando resultados estadísticos antes y después de la implementación, logrando concluir: Con los resultados presentados de la comparación del antes y después de la implementación del Data Center se puede evidenciar mejoras significativas en la gestión de información de la municipalidad, además la seguridad aplicada en la implementación cumple con los estándares requeridos en todo el proceso. Por otro lado, la capacitación que recibió el personal fue de gran aporte porque favorece al trabajo que realizan en la administración del centro de datos. Con ello se puede evidenciar el soporte tecnológico que brinda implementar Data center en las empresas porque favorece a su gestión y optimización de procesos, por otro lado, los Centros de Datos o Centros de Procesamiento de Datos son salas especiales preparadas con mecanismos eléctricos, ambientales y de gestión del hogar en los que se alojan los sistemas de procedimientos, comunicación y almacenamiento de hechos (Plazzotta et al., 2015).

Luego se presenta el análisis del objetivo específico que se basa en comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center, se obtuvo como resultado que través de la aplicación del instrumento se tiene que la implementación de las acciones presento diferencias entre el pre test y el pos test para la planificación, mostrando que en el pre test se registró que 76 trabajadores que conforman el 46.9% lo encuentran en el nivel bajo, luego en el pos test se

registró que 1 trabajador que conforma el 0.6% para el nivel bajo. Luego se tiene que 85 trabajadores que integran el 52.5% lo ubican en el nivel regular en el pre test, en comparación a 75 trabajadores que integran el 46.3% en el pos test, obteniendo una mejora de 6.2%. Al realizar el análisis del nivel alto se tiene que en el pre test se registró que 1 trabajador que conforma el 0.6%, en comparación a 86 trabajadores que integran el 53.1%, obteniendo una mejora del 52.5%, datos que en comparación con lo registrado por Endara (2016), con su estudio que se basa en el análisis de un data center de una empresa privada de Ecuador, durante este proceso se basó en los lineamientos que se establecen en el método científico, aplicando el enfoque cuantitativo como estrategia para obtener datos, presentando como objetivo conocer cómo se presenta la infraestructura actual de la empresa y mejorarla con una propuesta tecnológica, logrando arribar a la conclusión: La arquitectura del centro de datos de Cisco tiene altos costos en comparación con las arquitecturas de otros fabricantes, sin embargo, es una de las mejores del mercado en términos de infraestructura integrada. Al igual que el garaje, EMC VNX ocupa un lugar destacado en el cuadrante de Gartner de almacenamiento sólido. En cuanto a las licencias de virtualización, existen exquisitas alternativas disponibles en el mercado: VMware e Hyper V. Aunque Hyper-V tiene tarifas de bajo costo dentro del mercado, VMware es la generación más sólida en el mercado de la virtualización porque tiene funciones superiores. Una forma de mejorar el uso de fuentes de máquinas digitales mediante la optimización de la cantidad de RAM y procesador que devoran. De lo mostrado se puede decir que la seguridad es una parte esencial en toda organización porque garantiza que su información no será divulgada por personas extrañas a la entidad, además el Data Center o conocido como centro de datos facilitan el procesamiento de información y datos de manera sistemática, que se logra mediante el uso de dispositivos de alta capacidad como servidores. Según Arizala y Ortiz (2010), delimitan un medio de datos como: El lugar donde

se concentran todas las fuentes esenciales para el procesamiento de información de una empresa comercial, que adquiere la persona de Alta Disponibilidad cuando cumple con una secuencia de medidas. orientados a asegurar la disponibilidad del servicio, es decir, a que el proveedor opere las 24 horas del día.

De ahí se tiene el análisis del objetivo específico que se basa en comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center, se obtuvo como resultado que a través de la aplicación del instrumento se tiene que la implementación de las acciones presento diferencias entre el pre test y el pos test para la dimensión implementación de la seguridad, mostrando que en el pre test se registró que 95 trabajadores que integran el 58.6% lo encuentran como bajo, luego en el pos test se registró que ningún trabajador lo ubica en este nivel, minimizando en comparación del pre y pos test en 58.6%, luego se tiene que 65 trabajadores que corresponde al 40.1% lo encuentra como regular en el pre test, luego en el pos test se registró que 87 trabajadores que conforman el 53.7% lo ubican como regular, obteniendo una diferencia del 0.6%. Al realizar el análisis del nivel alto se tiene que 2 trabajadores que conforman el 1.2% lo encuentran en este nivel, en comparación al pos test que 75 trabajadores que conforman el 46.3% lo ubican en este nivel, haciendo una diferencia de 45.1%, datos que en comparación con lo registrado por Espinoza (2021), estuvo a cargo de desarrollar un estudio que se basa en el diseño de un Data Center bajo la norma ANSI/TIA 942 para una empresa privada de Guayaquil, para ello se basó en los lineamientos que se establecen en los estudios cuantitativos, presentando resultados estadísticos como resultados, luego se enfocó en el diseño experimental, presentando como conclusión: El diseño propuesto del intermedio de hechos de Clase II cumple plenamente con las recomendaciones de la ANSI / TIA 942 general hecha para cada subsistema: para

el subsistema de telecomunicaciones se establece en: cables, racks, estantes y vías; en los subsistemas eléctricos que constituyen redundancia, topología de UPS y sistemas de puesta a tierra; En el subsistema mecánico, averiguando la cobertura adecuada en las cercanías del dispositivo de aire acondicionado, cumpliendo con todas estas sugerencias de diseño, la disponibilidad y confiabilidad se pueden suministrar dentro de los servicios brindados por Azotel S.A. Estos Data Centers normalmente se realizan y mantienen a través de agencias masivas para que se pueda acceder a los registros necesarios para sus operaciones. Sin embargo, casi todas las empresas medianas o grandes cuentan con instalaciones de datos que durante los casos máximos no cumplen con los estándares mínimos importantes para asegurar la integridad en sus estructuras, siendo este un punto vital dentro de sus grupos (Plasencia y Calderón, 2016).

De ahí se tiene el análisis del objetivo específico que se basa en comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center, se obtuvo como resultado que a través de la aplicación del instrumento se tiene que la implementación de los controles presentó diferencias entre el pre test y el pos test, evidenciando que para el nivel bajo presentó en el pre test a 95 trabajadores que conforman el 58.6%, luego en el pos test no presentó trabajadores para este nivel, haciendo una diferencia de 58.6%. Luego para el nivel regular se registró que en el pre test se encontró que 66 trabajadores que conforman el 40.7%, luego en el pos test registro que 86 trabajadores que conforman el 53.1%, haciendo una diferencia del 12.3%. Para el nivel alto se tiene que 1 trabajador que conforman el 0.6%, luego en el pos test se registró que 76 trabajadores que conforman el 46.9%, haciendo una diferencia del 46.3%, datos que en comparación con lo registrado por Montaña y Bustíos (2020), realizaron un estudio que se basa en desarrollar un análisis y la propuesta de un Data Center para un

gobierno local de Lambayeque, con las consideraciones necesarios para asegurar la información de la municipalidad, durante este proceso se tomó en cuenta los procesos del lineamiento que se establece en el método científico, logrando concluir: Se logró optimizar y mejorar los procesos informáticos tales como el SIAF, SIGA, SISGEDO, y SiSPLANI, entre los más importantes, ya que se generó un sistema rápido en materia de procesamiento y transferencia de datos con el diseño de red jerárquico, la utilización de equipos modernos y el ancho de banda de 300 Mbps, que garantizan mejoras de respuesta en las transferencias financieras, movimientos presupuestales, consultas de base de datos y reportes de la parte administrativa, propios de estos procesos informáticos de la Municipalidad de José Leonardo Ortiz. Los centros de datos no se describen a través de su longitud física o estilo. Las pequeñas corporaciones pueden funcionar de manera eficiente con más de un servidor y estructuras de garajes comunitarios dentro de un conveniente armario o sala pequeña, mientras que las grandes organizaciones de computación, incluidas Facebook, Amazon o Google, pueden llenar un área de almacén masiva con el sistema. Infraestructura y centro de información. "En otros casos, los centros de estadísticas pueden establecerse en instalaciones celulares, incluidas las cajas de entrega, también llamado centro de datos de un solo contenedor" (Godinho & Bigelow, 2017).

De ahí se tiene el análisis del objetivo específico que se basa en comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center, se obtuvo como resultado que través de la aplicación del instrumento se tiene que la implementación de las acciones presento diferencias entre el pre test y el pos test, evidenciando que para el nivel bajo presento en el pre test a 48 trabajadores que conforman el 29.6%, luego en el pos test no presento trabajadores para este nivel, haciendo una diferencia de 29.6%. Luego para el nivel regular se registró que en

el pre test se encontró que 106 trabajadores que conforman el 65.4%, luego en el pos test registro que 66 trabajadores que conforman el 40.7%, haciendo una diferencia del 24.7%. Para el nivel alto se tiene que 8 trabajador que conforman el 4.9%, luego en el pos test se registró que 96 trabajadores que conforman el 59.3%, haciendo una diferencia del 54.3%, datos que en comparación con lo registrado por Taco (2019), presento en Tacna un estudio que se basa en desarrollar una propuesta tecnológica que fortalezca la comunicación de datos de una empresa eléctrica de la ciudad, para ello presento como objetivo general implementar una solución tecnológico que garantice la información de la empresa y proteja la seguridad de datos, durante este proceso se encamino en el enfoque cuantitativo, presentados resultados comparativos del antes y después de la implementación propuesta, logrando concluir: Fue viable decidir que la herramienta RACKTABLES DCIM permite optimizar la gestión de equipos Data Center de una empresa energética dentro de la ciudad de Tacna, en este ejemplo a partir de la aplicación de RACKTABLES DCIM. Esto se pone a prueba a nivel estadístico dado el nivel de importancia calculado bajo 0.05, lo que verifica en grado cuantitativo que la Gestión de los equipos que integran un Data Center es sumamente crucial para generar ventajas en los niveles de gestión de las ofertas y deseos del empleador. Fortalecimiento empresarial en la metrópoli de Tacna. El diseño del centro de datos también debe contratar prácticas de seguridad y protección. Por ejemplo, la protección a menudo se refleja en el diseño de la entrada a las puertas y pasillos, que deben adaptarse al movimiento de equipos portátiles grandes y difíciles de manejar, así como permitir que los empleados accedan y reparen la infraestructura. La extinción de incendios es cualquier otra área clave de protección, y el uso generalizado de sistemas eléctricos y electrónicos sensibles y de potencia excesiva se opone a los rociadores no inusuales. En cambio, los centros de datos suelen utilizar estructuras químicas de extinción de incendios que no dañan el medio ambiente, que eliminan de forma eficaz una chimenea de oxígeno al

tiempo que mitigan los daños colaterales al dispositivo. “Dado que el centro de información también es un negocio intermedio activo, las medidas de seguridad integrales, junto con los naipes de acceso y la videovigilancia, ayudan a localizar y evitar la apropiación indebida de personal, contratistas e intrusos” (Alcocer, 2010).

5.2 Conclusiones

Luego de realizar la implementación del data Center se tiene las siguientes conclusiones que responden a los objetivos trazados en el estudio:

Conclusión general:

Con los resultados se ha demostrado que la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021, mostrando una mejoría de 50.6% para el nivel alto, en el caso del nivel regular se ha demostrado una mejoría del 15.4% y para el nivel bajo se ha reducido en 35.2 %, además de ello se ha logrado comprobar la hipótesis.

Conclusiones específicas:

- ✓ Al realizar la comparación de la información obtenida se ha registrado que la planificación de la seguridad presentó diferencias entre el pre test y el pos test presentando una reducción del 46.3% para el nivel bajo, luego en el nivel regular se ha mejorado el 6.2% y en el nivel alto se ha obtenido una mejora de 52.5%, con ello se puede evidenciar la efectividad que presentó el data center en la municipalidad.
- ✓ Al realizar la comparación de la información obtenida se ha registrado que la implementación de la seguridad presentó diferencias entre el pre test y el pos test presentando una reducción del 46.3% para el nivel bajo, luego en el nivel regular se ha mejorado el 6.2% y en el nivel alto se ha obtenido una mejora de 52.5%, con ello se puede evidenciar la efectividad que presentó el data center en la municipalidad.
- ✓ Al realizar la comparación de la información obtenida se ha registrado que la implementación de controles presentó diferencias entre el pre test y el pos test

presentando una reducción del 58.6% para el nivel bajo, luego en el nivel regular se ha mejorado el 12.3% y en el nivel alto se ha obtenido una mejora de 46.3%, con ello se puede evidenciar la efectividad que presentó el data center en la municipalidad.

- ✓ Al realizar la comparación de la información obtenida se ha registrado que la implementación de acciones presentó diferencias entre el pre test y el pos test presentando una reducción del 29.6% para el nivel bajo, luego en el nivel regular se ha mejorado el 24.7% y en el nivel alto se ha obtenido una mejora de 54.3%, con ello se puede evidenciar la efectividad que presentó el data center en la municipalidad.

5.3 Recomendaciones

Luego de obtener las conclusiones se recomienda las siguientes acciones que pueden ayudar a mitigar los problemas con la gestión de información en la municipalidad y darle uso a la implementación realizada del Data center, para resguardar los datos de los usuarios internos de la entidad:

- ✓ Al administrador de la municipalidad continuar invirtiendo en tecnología que facilite la gestión de información entre los usuarios internos y externos de la municipalidad, que permitan que los datos que se mantengan, presenten la seguridad requerida.
- ✓ Al jefe del área de informática de la municipalidad realizar capacitaciones sobre la administración de Data Center, para que cuente con los conocimientos necesarios para poder administrar el área y los sistemas que se utilizan además de darles el soporte físico (hardware) a los usuarios.
- ✓ A los usuarios internos de la municipalidad informar al área de informática ante cualquier suceso extraño que se presente en el manejo de información para que puedan aplicar las acciones preventivas y correctivas de ser necesario para evitar vulneración de información de la municipalidad.
- ✓ Al personal de informática están en contante revisión de los sistemas y los protocolos que se encuentran en la red, además de administrar y supervisar los equipos como switches y servidores para evitar intrusos en la red que puedan vulnerar la información que se cuenta en los sistemas.
- ✓ En la misma línea al personal realizar las copias de seguridad pertinentes y de manera periódica a los servidores para que garantice la información que se cuenta en la entidad.

- ✓ Al jefe de personal realizar evaluaciones de manejo de herramientas tecnológicas a todo el personal para evidenciar si todo el personal cuenta con las competencias necesarias para hacer uso de los sistemas informáticos de la municipalidad y garantizar la disponibilidad de información.

Referencias bibliográficas

- Amoroso, Y. y Costales, D. (2016). Big Data: a tool for public administration. 47 (3).
<https://www.redalyc.org/pdf/1814/181452084001.pdf>
- Areitio (2008). Seguridad de la Información Redes, Informática y sistemas de Información.
Madrid: Editorial Paraninfo S.A. Universidad de Deusto
- Arizala, C. & Ortiz, B. (2010). Distribución correcta de computadores desktop en el rack para un gran centro de datos [fotografía].
<http://dspace.esPOCH.edu.ec/bitstream/123456789/557/1/18T00449.pdf>
- Alcocer, A. (2010). Cloud Computing. Características de las Aplicaciones en Cloud.
<http://www.societic.com/2010/03/cloud-computing-caracteristicas-de-lasaplicaciones-en-cloud/>
- Baena, G. (2017). *Metodología de la investigación*. ISBN ebook: 978-607-744-748-1.
Recuperado de
http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf
- Burgos J, (2008). Modelo para el Control de Riesgos de Seguridad de la Información en Áreas de Tecnologías de la Información y Comunicaciones (TIC). Chile: Universidad del Bío-Bío - Concepción.
- Cabezas, E., Andrade, A. y Torres, J. (2018). *Introducción a la metodología de la investigación científica*. ISBN: 978-9942-765-44-4. Recuperado de
<http://repositorio.espe.edu.ec/jspui/bitstream/21000/15424/1/Introduccion%20a%20a%20Metodologia%20de%20la%20investigacion%20cientifica.pdf>
- Camargo, J., Camargo, F. y Joyanes, L. (2015). Conociendo Big Data. 24 (38).
<https://www.redalyc.org/pdf/4139/413940775006.pdf>

- Carvajal, D., Cardona, A. y Valencia, F. (2019). A proposal for the management of the information security applied to a Colombian public entity. 13(25). http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672019000100068
- Castillo, G. (2018). Modelo de optimización de recursos de un data center que brinda infraestructura como servicio (IAAS) de manera controlable y auditable a pymes de la Provincia del Santa. Universidad Nacional del Santa. <http://repositorio.uns.edu.pe/handle/UNS/3151>
- Cohen, N. y Gómez, G. (2019). Metodología de la investigación, ¿para qué?: la producción de los datos y los diseños. ISBN 978-987-723-190-8. Editorial Teseo. Recuperado de http://biblioteca.clacso.edu.ar/clacso/se/20190823024606/Metodologia_para_que.pdf
- Concepción, D., González, E., García, R. y Miño, J. (2019). Investigation methodology: Origin and construction of a doctoral thesis. 6(1). 76-87. <http://scielo.iics.una.py/pdf/ucsa/v6n1/2409-8752-ucsa-6-01-76.pdf>
- Couto, F. (2016). Infraestructuras y políticas internacionales de desarrollo para gestión de los datos de investigación. 63 (1). <https://www.redalyc.org/pdf/161/16146347004.pdf>
- Endara, D. (2016). Caso de Estudio: Renovación Data Center; Infraestructura, Servicios Y Comunicaciones. Universidad San Francisco De Quito USFQ. <https://repositorio.usfq.edu.ec/bitstream/23000/6259/1/128452.pdf>
- Espinoza, M. (2021). Estudio y diseño de un data center aplicando la norma ANSI/TIA 942 para ISP AZOTEL S.A. Tesis de posgrado. <http://201.159.223.180/bitstream/3317/16622/1/T-UCSG-POS-MTEL-196.pdf>
- Flores, S. (2018). Propuesta para la implementación de una red de datos para mejorar la comunicación de las áreas del instituto de educación superior tecnológico publico

todas las Artes – 2018. Universidad Nacional José María Arguedas.
https://repositorio.unajma.edu.pe/bitstream/handle/123456789/548/Sandy_Tesis_Bachiler_2018.pdf?sequence=1&isAllowed=y

Fernández, CM. (2012). La Norma ISO 27001 del Sistema de Gestión de Seguridad de Información, garantía de confidencialidad, Integridad y disponibilidad. España: Asociación Española de Normalización y Certificación.

Gallardo, E. (2017). Metodología de la Investigación. Manual Autoformativo Interactivo. ISBN electrónico n.º 978-612-4196.
https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Gil, V. y Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. 22 (2).
<https://www.redalyc.org/pdf/849/84953103011.pdf>

Gil, J. y Maihuiri, L. (2018). Implementación de un data center virtual en Cloud Computing para mejorar los servicios del departamento de ti en la empresa venus peruana S.A.C. Universidad Autónoma.
<http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/603/1/Gil%20Izurriga%20Jose%20Edu%2c%20y%20Maihuiri%20Vargas%2c%20Lenin%20Alex.pdf>

Godinho, R. & Bigelow, S. (2017). Data Center. Recuperado de
<http://searchdatacenter.techtarget.com/definition/data-center>

Godoy, R. (2014). Seguridad de Información. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica

- Graf, C. (2020). Information and communication technologies (ICTs). First step for the implementation of TeleSalud and telemedicine. 6(1).
http://scielo.iics.una.py/scielo.php?script=sci_arttext&pid=S2413-43412020000100001
- Hernández, R. y Mendoza, C. (2018). *Metodología de la investigación- rutas cuantitativa-cualitativa-mixta*. ISBN 1456260960. Editor McGraw-Hill Interamericana
- International Organization for Standardization. (2008). ISO 9001: Sistemas de gestión de la Calidad - Requisitos (4ta 2008-11-15 ed.). Ginebra, Suiza: Secretaria Central de ISO.
- Juma, G. (2017). Diseño de un data center tipo TIER I para el gobierno autónomo descentralizado municipal de Otavalo bajo la norma ANSI/TIA-942. Universidad Técnica del Norte.
<http://repositorio.utn.edu.ec/bitstream/123456789/6982/2/ARTICULO.pdf>
- Hernández, F. (2019). The risks of information and communication technologies.
<https://www.medigraphic.com/pdfs/conamed/con-2019/con194d.pdf>
- Luzbet, F. y Laurencio, A. (2020). Virtualization as an Alternative for Postgraduate Education. 39 (3). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0257-43142020000300017
- Martelo, R., Tovar, L. y Maza, D. (2018). Basic Logical Safety Model. Study Case: The Network Laboratory of the University of Cartagena in Colombia. 29(1).
https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100003
- Mendoza, M. y Moran, J. (2017). Implementación y configuración de los servicios de un mini data center en el laboratorio de desarrollo de software en la universidad técnica

de Cotopaxi extensión la Maná. Universidad Técnica De Cotopaxi.
<http://repositorio.utc.edu.ec/bitstream/27000/4132/1/UTC-PIM-000056.pdf>

Montalván, J., Soria, C., Hopkins, A., Ascue, R. y Ajito, E. (2019). *Guía de investigación*. ISBN: 978-612-4439-09-4. Primera edición digital. Recuperado de <https://cdn02.pucp.education/investigacion/2016/06/12214732/guia-de-investigacion-en-diseno.pdf>

Mosquera, C. (2016). Gestión de riesgo del data center de la Pucese basada en estándares internacionales. Pontificia Universidad Católica Del Ecuador Sede Esmeraldas. <https://repositorio.pucese.edu.ec/bitstream/123456789/799/1/MOSQUERA%20RIVA%20CARMEN.pdf>

Moreira, C., Zambrano, W., Guamán, R. y Cuenca, W. (2017). Low-Cost Solutions Using the Infrastructure as a Service with High Availability and Virtualization Model. 8 (1). <https://www.redalyc.org/journal/5722/572262176014/html/>

Montaño, R. y Bustíos, J. (2020). Diseño de un data center con arquitectura convergente para optimizar los procesos informáticos de la municipalidad distrital de José Leonardo Ortiz. Universidad Nacional Pedro Ruiz Gallo. https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/8862/Monta%c3%b1o_Guerrero_Richard_Alan_y_Bust%c3%ados_Arteaga_Jorge_Luis_Jes%c3%bas.pdf?sequence=1&isAllowed=y

Navarro, E., Jiménez, E. y Rappoport, S. (2017). *Fundamentos de la investigación y la innovación educativa*. ISBN: 978-84-16602-55-1. Recuperado de https://www.unir.net/wp-content/uploads/2017/04/Investigacion_innovacion.pdf

Orozco, J. (2016). La nueva era de los negocios: computación en la nube. 15 (2). <https://www.redalyc.org/pdf/784/78457627005.pdf>

- Ochoa, C. (2019). Diseño y análisis en investigación. ISBN: 978-84-7867-685-9.
Recuperado de https://www.aepap.org/sites/default/files/documento/archivos-adjuntos/artl_2019_libro_diseno_y_analisis_de_investigacion.pdf
- Plazzotta, F., Luna, D. y González, F. (2015). Health Information Systems: Integrating clinical data in different scenarios and users. 32 (2).
http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1726-46342015000200020
- Plasencia, L. y Calderón, C. (2016). Referencial architecture of Big Data for the management of telecommunications. 25 (4).
<https://scielo.conicyt.cl/pdf/ingeniare/v25n4/0718-3305-ingeniare-25-04-00566.pdf>
- Pallas, G. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Uruguay: Universidad de la Republica
- Ramírez, G., Ovando, C. y Lino, J. (2020). Model of cloud computing services management for consumer product companies. 11 (23).
http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-07052019000200020
- Rodríguez, L., Cruzado, C., Mejía, C. y Alarcón, M. (2020). Application of ISO 27001 and its influence on the information security of a Peruvian private company. 8(3).
http://www.scielo.org.pe/scielo.php?pid=S2307-79992020000400011&script=sci_arttext
- Said, Y., Gonzales, C. y Lecuona, C. (2015). HMI/ SCADA standards in the design of data center interfaces: A network operations center case study. 82(193).
<http://www.scielo.org.co/pdf/dyna/v82n193/v82n193a23.pdf>

- Taco, R. (2019). Uso de racktables DCIM como herramienta para optimizar la gestión de los equipos que conforman el DC de una empresa eléctrica en la ciudad de Tacna, 2019. Universidad Privada De Tacna. <https://repositorio.upt.edu.pe/bitstream/handle/20.500.12969/1218/Taco-Coayla-Renzo.pdf?sequence=1&isAllowed=y>
- Turgut, Y. y Kürat, P. (2014). Symmetry and Rotation Skills of Prospective Elementary Mathematics. 28 (48). <https://repositorio.minedu.gob.pe/bitstream/handle/20.500.12799/3013/Symmetry%20and%20Rotation%20Skills%20of%20Prospective%20Elementary%20Mathematics%20Teachers.pdf?sequence=1&isAllowed=y>
- Vargas, G. (2020). Virtualization of academic content in distance Learning Environments. 61 (2). http://www.scielo.org.bo/scielo.php?pid=S1652-67762020000200009&script=sci_arttext
- Vázquez, S. (2015). Tecnologías de almacenamiento de información en el ambiente digital. 5 (2). <https://www.redalyc.org/pdf/4768/476847248008.pdf>
- Vega, et al. (2020). Red de monitorización para automatizar el sistema de enfriamiento de un centro de datos. 24 (1). <https://www.redalyc.org/journal/5055/505563460010/505563460010.pdf>
- Velasco, L. (2019). Diseño de data center basado en el estándar ANSI/BICSI-002-2014 para el funcionamiento de los servicios y aplicaciones de la Cooperativa Nuevo Milenio. Universidad Inca Garcilaso de la Vega. http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/4504/TESIS_VELASCO_LUIS.pdf?sequence=1&isAllowed=y

ANEXOS

ANEXOS

Anexo 1. Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODOLOGÍA
<p>Problema principal: ¿Cómo la infraestructura de un data center incide en la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021?</p>	<p>Objetivo general: Demostrar como la infraestructura de un data center incide la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.</p>	<p>Hipótesis general: La infraestructura de un data center incide significativamente en la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.</p>	<p>Variable I: Infraestructura de un data center</p>	<p>D1: Espacio del sitio y su disposición</p>	<ul style="list-style-type: none"> • Cuarto de Entrada • Área de distribución principal (Main distribution área MDA) • Área de distribución (Horizontal distribution area HDA) • Área de distribución de zonas (Zone distribution área ZDA) • Área de distribución de los equipos (Equipmenet distribution área EDA) • Racks y gabinetes • Sistemas de tendido de cable • TIER I: Centro de datos Básico 	<p>Tipo de investigación Aplicada</p> <p>DISEÑO Experimental – Pre experimental</p> <p>POBLACIÓN 280 trabajadores</p> <p>MUESTRA 162 trabajadores</p> <p>TÉCNICA Encuesta</p> <p>INSTRUMENTOS Cuestionarios</p>
<p>Problemas secundarios: ¿De qué manera la infraestructura de un data center incide en los controles de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021?</p>	<p>Objetivos específicos: Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center. Comparar los resultados de la implementación de la</p>	<p>Hipótesis específicas: La infraestructura de un data center incide significativamente en la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021. La infraestructura de un data center incide significativamente en la implementación de</p>		<p>D2: Infraestructura del cableado</p>		

<p>¿De qué manera la infr</p>	<p>seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.</p> <p>Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.</p> <p>Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación</p>	<p>la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.</p> <p>La infraestructura de un data center incide significativamente en los controles de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.</p> <p>La infraestructura de un data center incide significativamente en las acciones de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021.</p>	<p>Variable D: Seguridad de la información (ISO 27001)</p>	<p>D3: Tier y niveles de disponibilidad</p> <p>D4: Consideraciones ambientales</p>	<ul style="list-style-type: none"> • TIER II: Centro de datos Redundante • TIER III: Centro de datos Concurrentemente Mantenibles • TIER IV: Centro de datos Tolerante a fallos • Energía eléctrica • Sistema de Enfriamiento 	
<p>D1: Planificación</p> <p>D2: Implementación de la seguridad</p> <p>D3:</p>	<ul style="list-style-type: none"> • Política de seguridad • Alcance del SGSI • Análisis de riesgo • Selección de controles • Competencias profesionales • Mapa de procesos • Funciones y responsabilidades • Gestión de riesgos • Administración del SGSI • Implementación de controles • Revisión del SGSI 					

	de la infraestructura de un data center.			Implementación de los controles D4: Implementación de las acciones	<ul style="list-style-type: none">• Auditorías internas• Medidas correctivas• Supervisión de la gerencia• Acciones correctivas• Optimización de los procesos	
--	--	--	--	--	--	--

Anexo 2. Instrumentos para la recolección de datos

“INFRAESTRUCTURA DE UN DATA CENTER PARA LA SEGURIDAD DE LA INFORMACION (ISO 27001) DE LA MUNICIPALIDAD PROVINCIAL DE HUARAZ - 2021”

I. PARTE INFORMATIVA

INSTRUCCIÓN: A continuación, se te presenta una determinada cantidad de preguntas. Marque con una (x) el enunciado.

N°	INDICADORES	ESCALA DE VALORACION				
		S	CS	A	CN	N
		1	2	3	4	5
	DIMENSION: Planificación					
1	La municipalidad cuenta con políticas de seguridad a la hora de trabajar con información.					
2	El área de informática les brinda las instrucciones de seguridad ante cualquier vulneración de datos.					
3	Cuando presenta algún problema o inconsistencia con el sistema que utiliza en la municipalidad, informa de manera inmediata al área de informática.					
4	El área de informática aplica controles de seguridad a los usuarios.					
5	Los trabajadores de la municipalidad cuentan con las competencias necesarias para que resguarden la seguridad de información de la entidad.					
6	Los trabajadores cuentan con el mapa de procesos de información de la municipalidad para que se pueda articular el trabajo.					
7	Se evidencia en la municipalidad que el área de informática supervisa los datos que se manejan en la municipalidad y resguardan la seguridad.					
	DIMENSION: Implementación de la seguridad					
8	La red actual garantiza la seguridad de información que manejan los usuarios internos.					
9	Considera que pueden ocurrir casos de vulneraciones de datos con el data center que se cuenta.					
10	Considera que el área de informática administra de manera adecuada la seguridad de la red de datos.					
11	Se cuenta con respaldo de datos ante cualquier vulneración de información que pueda sufrir la municipalidad.					
12	El área de informática aplica controles de vulneración de datos					

	de manera periódica					
13	Los trabajadores del área de informática brindan charlas a los trabajadores de la manera que pueden sufrir vulneraciones de datos.					
DIMENSION: Implementación de los controles						
14	Se supervisión el sistema de seguridad de la municipalidad.					
15	El área de informática realiza auditorías internas a los usuarios de las vulneraciones que puedan sufrir.					
16	Cada área administrativa solicita al área de informática que revisen la seguridad de sus equipos de trabajo.					
17	Cuando se detectan problemas en el sistema, el área de informática le informa los mecanismos que deben seguir los usuarios.					
18	Es importante que el área de informática revise la seguridad de los equipos de manera periódica.					
19	La gerencia solita al área de informática y informa a los trabajadores de las áreas que pueden a ver sufrido ataques.					
DIMENSION: Implementación de las acciones						
20	El área de informática comunica a los trabajadores sobre las acciones que deben seguir ante cualquier vulneración de datos.					
21	Es necesario que los trabajadores conozcan las vulneraciones que puedan sufrir durante su trabajo cotidiano.					
22	Cuando se producen problemas en la red, los trabajadores del área de informática realizan mejoras y monitorean que no vuelva a ocurrir.					
23	Los trabajadores de la municipalidad presentan las habilidades tecnológicas para identificar los problemas de vulneración de información.					

Gracias por tu aportación

Anexo 3. Validación del instrumento

MATRIZ PARA VALIDACIÓN POR JUICIO DE EXPERTOS

Objetivo específico	Variable	N° Ítem	CONTENIDO		Observaciones
			Claridad	Congruencia	
Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	planificación	7	C	C	
Comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de la seguridad	6	C	C	
Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de los controles	5	C	C	
Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de las acciones	5	C	C	

CRITERIO:

Validez de criterio, por medio de la CLARIDAD Y CONGRUENCIA de cada ítem y se realiza mediante juicio de expertos

INSTRUCCIONES:

En las columnas de CLARIDAD Y CONGRUENCIA indique con una "C" si se considera CORRECTA o con una "I" si se considera INCORRECTA, la relación de cada aspecto con el ítem, en función de la variable correspondiente.
Si lo cree conveniente, adicione sus observaciones

**DATOS DE IDENTIFICACIÓN DEL
EXPERTO**

Apellidos y nombres: Medina López, Walter Junior

DNI: 42953649

Grado Académico:

Maestro en Ciencias e Ingeniería con mención en “Tecnología de la información y Sistemas Informáticos”

Profesión:

Ing. De Sistemas e Informática

Firma: _____



MATRIZ PARA VALIDACIÓN POR JUICIO DE EXPERTOS

Objetivo específico	Variable	N° Ítem	CONTENIDO		Observaciones
			Claridad	Congruencia	
Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	planificación	7	C	C	
Comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de la seguridad	6	C	C	
Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de los controles	5	C	C	
Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de las acciones	5	C	C	

CRITERIO:

Validez de criterio, por medio de la CLARIDAD Y CONGRUENCIA de cada ítem y se realiza mediante juicio de expertos

INSTRUCCIONES:

En las columnas de CLARIDAD Y CONGRUENCIA indique con una "C" si se considera CORRECTA o con una "I" si se considera INCORRECTA, la relación de cada aspecto con el ítem, en función de la variable correspondiente.
Si lo cree conveniente, adicione sus observaciones

**DATOS DE IDENTIFICACIÓN DEL
EXPERTO**

Apellidos y nombres: CACHA ARANA CRISTHIAN MAX

DNI: 45082546

Grado Académico:

Maestro en Ciencias e Gestión
Tecnológica de la Información

Profesión:

Ing. De sistemas

Firma: _____



MATRIZ PARA VALIDACIÓN POR JUICIO DE EXPERTOS

Objetivo específico	Variable	N° Ítem	CONTENIDO		Observaciones
			Claridad	Congruencia	
Comparar los resultados de la planificación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	planificación	7	C	C	
Comparar los resultados de la implementación de la seguridad de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de la seguridad	6	C	C	
Comparar los resultados de la implementación de los controles de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de los controles	5	C	C	
Comparar los resultados de la implementación de las acciones de la información (ISO 27001) de la municipalidad provincial de Huaraz – 2021 antes y después de la implementación de la infraestructura de un data center.	Implementación de las acciones	5	C	C	

CRITERIO:

Validez de criterio, por medio de la CLARIDAD Y CONGRUENCIA de cada ítem y se realiza mediante juicio de expertos

INSTRUCCIONES:

En las columnas de CLARIDAD Y CONGRUENCIA indique con una "C" si se considera CORRECTA o con una "I" si se considera INCORRECTA, la relación de cada aspecto con el ítem, en función de la variable correspondiente.
Si lo cree conveniente, adicione sus observaciones

**DATOS DE IDENTIFICACIÓN DEL
EXPERTO**

Apellidos y nombres: PONTE QUIÑONES ELVIS JERSON

DNI: 44199834

Grado Académico:

Doctor en Educación
Maestro en ingeniería de sistemas con mención en
Tecnológica de la Información

Profesión:

Ing. De sistemas

Firma: _____



Anexo 4. Base de datos

PRE-TEST VARIABLE: SEGURIDAD DE LA INFORMACION (ISO 27001)																												
N°	D1: Planificación							SUB	D2: Implementación de la seguridad						SUB	D3: Implementación de los controles						SUB	D4: Implementación de las acciones				SUB	TOTAL
	1	2	3	4	5	6	7		8	9	10	11	12	13		14	15	16	17	18	19		20	21	22	23		
1	3	3	2	2	1	2	3	16	1	2	1	2	3	2	11	1	3	2	4	2	2	14	2	2	2	2	8	49
2	2	2	3	3	2	3	2	17	1	1	2	3	2	3	12	3	2	3	2	2	2	14	2	3	1	1	7	50
3	2	2	2	2	2	3	2	15	1	2	1	4	2	2	12	1	2	2	3	3	5	16	2	3	4	3	12	55
4	2	2	2	2	3	2	2	15	1	2	2	2	2	2	11	2	2	2	1	2	2	11	2	3	3	4	12	49
5	3	2	3	3	2	3	2	18	3	4	3	3	2	3	18	4	2	3	1	3	2	15	2	4	2	2	10	61
6	2	2	2	2	3	2	1	14	1	2	2	1	2	2	10	4	2	2	2	2	3	15	2	1	1	1	5	44
7	3	3	2	3	2	3	2	18	1	2	2	2	3	2	12	2	3	2	3	3	2	15	2	2	3	2	9	54
8	2	2	2	2	3	2	1	14	1	4	1	3	2	2	13	1	2	2	2	2	1	10	2	1	3	3	9	46
9	3	2	2	3	2	3	3	18	1	4	2	4	2	2	15	2	2	2	3	3	3	15	2	3	3	2	10	58
10	3	2	2	2	3	2	2	16	1	2	2	2	2	2	11	2	2	2	4	2	2	14	2	3	2	3	10	51
11	1	2	2	2	2	3	2	14	1	2	2	3	2	2	12	1	2	2	2	3	2	12	3	2	2	2	9	47
12	2	3	2	3	3	2	1	16	3	5	2	2	4	3	19	3	2	1	3	2	2	13	2	2	2	2	8	56
13	2	2	2	1	2	3	2	14	2	3	3	1	3	3	15	2	3	1	3	3	3	15	4	2	3	2	11	55
14	2	3	2	2	3	2	1	15	3	1	2	2	2	2	12	1	3	1	2	2	2	11	2	3	2	4	11	49
15	2	3	3	1	2	3	2	16	2	3	4	3	3	3	18	2	2	1	3	3	3	14	3	2	4	3	12	60
16	2	2	2	2	1	2	3	14	2	2	3	2	2	2	13	2	3	2	2	2	2	13	2	3	2	2	9	49
17	3	2	3	3	2	3	2	18	2	3	2	3	1	3	14	2	2	3	3	1	3	14	3	2	3	1	9	55
18	2	2	2	2	3	2	3	16	2	2	1	2	3	2	12	2	3	1	2	2	2	12	2	3	2	3	10	50
19	3	3	3	3	2	3	2	19	2	3	1	3	2	3	14	2	2	3	4	3	3	17	3	2	3	2	10	60

20	2	2	1	2	3	2	3	15	1	2	1	2	3	2	11	2	2	2	3	2	2	13	2	3	2	3	10	49
21	3	3	2	3	1	3	1	16	2	3	1	3	2	3	14	3	2	3	2	3	1	14	3	2	3	2	10	54
22	2	3	1	2	2	2	2	14	1	1	2	2	3	2	11	2	2	3	3	2	2	14	2	1	2	3	8	47
23	3	3	2	1	3	3	3	18	2	3	3	3	2	3	16	3	3	2	3	2	3	16	3	2	5	2	12	62
24	2	2	3	2	2	2	2	15	1	4	2	2	3	1	13	2	2	3	1	3	2	13	5	3	4	4	16	57
25	3	2	3	3	3	3	3	20	2	3	3	3	2	2	15	3	3	2	2	2	3	15	4	2	2	5	13	63
26	2	3	3	2	2	2	2	16	2	3	2	2	1	3	13	2	2	3	2	3	2	14	2	3	3	2	10	53
27	2	3	1	3	3	3	3	18	3	2	3	3	1	2	14	3	2	2	2	2	3	14	3	2	2	3	10	56
28	1	3	1	2	2	2	2	13	1	3	2	2	1	4	13	2	2	3	2	3	2	14	4	3	2	3	12	52
29	2	2	1	3	3	3	3	17	2	2	3	3	3	2	15	3	2	4	2	3	2	16	3	2	3	2	10	58
30	2	3	2	2	2	2	2	15	3	3	2	2	2	3	15	2	2	2	3	2	3	14	5	3	1	3	12	56
31	2	2	3	3	1	3	3	17	2	2	3	3	3	2	15	3	3	1	2	3	2	14	4	2	2	2	10	56
32	2	3	1	2	2	2	2	14	3	3	2	2	2	3	15	2	2	2	3	2	3	14	2	3	2	3	10	53
33	2	2	3	4	3	3	3	20	2	2	3	3	3	5	18	3	1	3	2	3	2	14	3	2	1	2	8	60
34	2	2	2	3	2	2	2	15	3	3	2	2	2	2	14	2	2	2	3	2	3	14	2	3	2	3	10	53
35	3	2	3	2	3	1	3	17	2	2	3	3	3	3	16	3	3	3	2	1	2	14	3	2	3	2	10	57
36	2	2	2	1	2	3	2	14	3	3	2	2	2	2	14	3	1	2	2	2	2	12	2	3	2	3	10	50
37	3	2	3	1	3	2	3	17	2	2	3	2	3	3	15	2	3	3	1	3	3	15	1	2	3	2	8	55
38	3	1	2	1	2	3	2	14	3	1	2	2	2	2	12	3	2	2	1	2	2	12	2	3	2	3	10	48
39	3	2	3	1	3	2	3	17	2	3	3	1	3	3	15	4	3	3	2	3	3	18	3	2	3	2	10	60
40	1	1	1	2	2	3	2	12	3	2	2	1	2	2	12	2	2	2	3	2	2	13	2	4	2	3	11	48
41	1	2	3	3	3	2	3	17	3	3	2	2	1	2	13	3	2	3	2	3	2	15	3	5	3	2	13	58
42	1	1	4	2	2	3	1	14	2	2	3	3	2	3	15	2	2	2	2	2	3	13	2	2	2	4	10	52
43	2	2	3	3	3	2	2	17	2	2	2	2	2	3	13	2	2	2	2	3	2	13	3	3	3	3	12	55
44	2	2	2	2	2	3	3	16	2	2	2	2	3	2	13	3	2	3	3	2	3	16	2	2	4	2	10	55
45	3	2	3	3	3	2	2	18	3	2	3	3	2	3	16	2	2	2	2	3	2	13	3	4	2	3	12	59
46	2	3	1	2	2	3	3	16	2	2	2	2	3	2	13	3	3	2	3	2	3	16	2	5	3	2	12	57
47	3	2	2	3	3	2	2	17	3	3	2	3	2	3	16	2	2	2	2	3	2	13	3	4	2	3	12	58

48	2	3	3	2	3	2	3	18	2	2	2	2	3	2	13	2	2	3	3	2	3	15	2	3	3	2	10	56
49	3	2	2	3	1	3	2	16	3	2	2	3	2	3	15	2	2	2	2	2	3	13	3	2	2	1	8	52
50	2	3	3	2	2	2	3	17	3	2	2	2	3	2	14	2	2	2	2	3	2	13	2	3	3	2	10	54
51	2	2	2	3	2	3	2	16	3	3	2	3	3	2	16	3	2	3	3	2	3	16	3	2	2	3	10	58
52	2	3	2	2	2	2	3	16	2	2	3	2	2	3	14	2	2	2	2	3	2	13	5	4	3	2	14	57
53	3	2	2	3	2	3	2	17	2	3	2	3	2	4	16	3	3	2	3	2	3	16	4	3	2	3	12	61
54	2	3	2	4	2	3	2	18	2	2	2	2	3	2	13	2	2	2	2	3	2	13	2	2	3	2	9	53
55	3	2	2	2	3	2	3	17	2	2	2	3	2	2	13	3	2	2	3	2	3	15	4	1	2	2	9	54
56	2	3	3	1	2	3	2	16	2	3	3	2	3	2	15	3	2	2	2	3	2	14	5	1	3	3	12	57
57	3	2	2	2	3	2	3	17	2	2	2	2	2	1	11	1	2	2	2	2	3	12	5	3	2	2	12	52
58	2	3	1	3	2	3	2	16	2	3	2	3	2	2	14	2	3	2	3	3	2	15	4	2	4	3	13	58
59	3	2	2	2	3	2	3	17	3	2	3	4	3	3	18	2	2	2	1	2	3	12	2	3	2	2	9	56
60	2	3	3	3	2	1	2	16	2	4	2	2	2	2	14	2	2	2	4	2	2	14	3	2	3	3	11	55
61	3	2	2	2	3	2	3	17	3	2	3	3	3	4	18	1	2	2	2	3	2	12	1	3	2	2	8	55
62	4	3	3	3	2	2	2	19	2	3	2	2	2	5	16	3	2	1	3	2	2	13	2	2	3	4	11	59
63	2	2	2	2	3	3	3	17	3	2	3	3	4	4	19	2	3	1	3	3	3	15	3	3	2	2	10	61
64	3	3	3	3	2	2	2	18	2	3	2	2	5	2	16	1	3	1	2	2	2	11	2	2	1	1	6	51
65	2	2	2	2	2	3	3	16	3	2	4	3	4	3	19	2	2	1	3	3	3	14	3	3	2	2	10	59
66	3	4	3	3	1	2	2	18	2	3	5	4	2	2	18	2	3	2	2	2	2	13	2	2	3	1	8	57
67	2	3	2	2	1	3	3	16	1	2	2	2	2	2	11	2	2	3	3	1	3	14	3	1	2	2	8	49
68	3	2	3	3	1	2	2	16	3	4	3	3	2	3	18	1	2	2	3	2	2	12	5	3	3	3	14	60
69	1	3	2	2	1	4	3	16	1	2	2	1	2	2	10	3	5	2	2	4	3	19	4	2	1	2	9	54
70	2	2	3	3	3	2	2	17	1	2	2	2	3	2	12	2	3	3	1	3	3	15	2	3	2	3	10	54
71	3	3	2	2	2	3	3	18	1	4	1	3	2	2	13	3	1	2	2	2	2	12	3	2	3	2	10	53
72	2	2	3	3	3	2	2	17	1	4	2	4	2	2	15	2	3	4	3	3	3	18	2	3	2	3	10	60
73	3	3	2	2	2	3	3	18	1	2	2	2	2	2	11	2	2	3	2	2	2	13	3	2	3	2	10	52
74	2	2	3	3	3	5	2	20	1	2	2	3	2	2	12	2	3	2	3	1	3	14	2	4	2	1	9	55
75	3	3	2	2	2	2	1	15	3	5	2	2	4	3	19	2	2	1	2	3	2	12	3	5	3	2	13	59

76	2	2	3	3	3	3	2	18	2	3	3	1	3	3	15	2	3	1	3	2	3	14	2	3	2	3	10	57
77	3	3	2	2	2	2	3	17	2	3	3	1	3	3	15	1	2	1	2	3	2	11	3	2	3	1	9	52
78	2	2	3	2	3	3	2	17	3	1	2	2	2	2	12	2	2	2	2	3	2	13	4	2	3	1	10	52
79	3	1	2	2	2	2	3	15	2	3	4	3	3	3	18	3	2	3	3	2	1	14	2	3	2	2	9	56
80	2	3	3	1	3	3	2	17	2	2	3	2	2	2	13	2	2	1	2	3	2	12	3	2	3	2	10	52
81	3	2	2	1	2	2	3	15	2	3	2	3	1	3	14	3	2	2	3	2	1	13	1	3	4	2	10	52
82	4	3	3	2	3	3	2	20	2	2	1	2	3	2	12	3	3	1	2	3	2	14	2	2	2	4	10	56
83	2	2	2	3	2	2	3	16	2	3	1	3	2	3	14	2	2	2	1	2	3	12	3	3	3	5	14	56
84	3	2	3	2	3	2	4	19	1	2	1	2	3	2	11	2	3	3	2	3	2	15	2	2	2	2	8	53
85	2	2	2	2	2	3	2	15	2	3	1	3	2	3	14	2	2	2	3	2	3	14	3	1	5	3	12	55
86	2	2	2	2	3	2	2	15	1	1	2	2	3	2	11	3	3	3	2	3	2	16	2	3	4	2	11	53
87	3	2	3	3	2	3	2	18	2	3	3	3	2	3	16	2	1	2	3	2	3	13	3	2	2	3	10	57
88	2	2	2	2	3	2	1	14	1	4	2	2	3	1	13	3	2	3	1	3	1	13	2	3	3	2	10	50
89	3	3	2	3	2	3	2	18	2	3	3	3	2	2	15	3	2	3	2	2	2	14	3	2	2	3	10	57
90	2	2	2	2	3	2	1	14	2	2	2	2	3	3	14	1	2	2	3	3	5	16	2	3	3	2	10	54
91	3	2	2	2	3	2	3	17	2	3	3	3	2	2	15	2	2	2	1	2	2	11	5	2	2	4	13	56
92	2	3	3	1	2	3	2	16	3	1	2	2	3	3	14	4	2	3	1	3	2	15	4	3	3	5	15	60
93	3	2	2	2	3	2	3	17	2	2	2	3	3	2	14	4	2	2	2	2	3	15	2	2	1	3	8	54
94	2	3	1	3	2	3	2	16	2	3	3	2	2	3	15	2	3	2	3	3	2	15	3	1	2	2	8	54
95	3	2	2	2	3	2	3	17	2	2	2	3	3	5	17	1	2	2	2	2	1	10	2	3	3	4	12	56
96	2	3	3	3	2	1	2	16	3	2	3	2	2	2	14	2	2	2	3	3	3	15	3	2	2	1	8	53
97	3	2	2	2	3	2	3	17	2	2	2	3	3	3	15	2	2	2	4	2	2	14	2	3	3	2	10	56
98	3	3	2	3	2	3	2	18	2	2	3	2	2	2	13	1	2	1	4	2	2	12	3	2	2	3	10	53
99	2	2	2	2	3	2	1	14	2	2	2	2	3	3	14	1	2	2	2	2	2	11	2	4	3	2	11	50
100	3	2	2	2	3	2	3	17	2	2	2	2	2	2	12	3	4	3	3	2	3	18	3	5	2	4	14	61
101	2	3	3	1	2	3	2	16	3	2	3	1	3	3	15	1	2	2	1	2	2	10	2	3	3	5	13	54
102	2	3	1	2	2	2	2	14	2	2	1	1	2	2	10	1	2	2	2	3	2	12	3	2	2	4	11	47
103	2	2	3	4	3	3	3	20	3	2	2	2	3	3	15	1	4	1	3	2	2	13	2	3	2	3	10	58

104	2	2	2	3	2	2	2	15	3	3	1	3	2	2	14	1	4	2	4	2	2	15	4	2	3	3	12	56
105	3	2	3	2	3	1	3	17	2	2	2	2	3	2	13	1	2	2	2	2	2	11	2	3	2	2	9	50
106	2	2	2	1	2	3	2	14	2	3	3	2	2	3	15	1	2	2	3	2	2	12	3	2	1	1	7	48
107	3	2	3	1	3	2	3	17	2	2	2	2	3	2	13	3	5	2	2	4	3	19	1	3	2	3	9	58
108	3	1	2	1	2	3	2	14	3	3	3	3	2	3	17	2	3	3	1	3	3	15	2	2	3	2	9	55
109	3	2	3	1	3	2	3	17	2	1	2	2	3	2	12	3	1	2	2	2	2	12	3	1	2	3	9	50
110	1	1	1	2	2	3	2	12	3	2	2	3	2	2	14	2	2	2	2	2	2	12	2	3	4	2	11	49
111	1	2	3	3	3	2	3	17	3	1	3	2	3	3	15	2	2	3	2	3	2	14	3	2	2	3	10	56
112	1	1	4	2	2	3	1	14	2	2	2	1	2	2	11	3	3	2	3	4	3	18	2	3	3	2	10	53
113	2	2	2	2	3	2	3	16	4	1	3	1	3	3	15	2	2	4	2	2	2	14	5	2	2	4	13	58
114	3	3	3	3	2	3	2	19	4	2	2	1	2	2	13	3	3	2	3	3	3	17	4	3	3	2	12	61
115	2	2	1	2	3	2	3	15	2	2	3	1	3	3	14	2	2	3	2	2	2	13	2	2	5	3	12	54
116	3	3	2	3	1	3	1	16	2	2	1	2	2	2	11	3	3	2	3	3	4	18	3	3	4	1	11	56
117	2	3	1	2	2	2	2	14	5	2	3	3	3	4	20	2	2	3	2	2	5	16	2	2	2	3	9	59
118	3	3	2	1	3	3	3	18	3	3	4	2	2	2	16	3	3	2	4	3	4	19	3	3	3	2	11	64
119	2	2	3	2	2	2	2	15	3	3	3	3	3	2	17	2	2	3	5	4	2	18	1	2	2	3	8	58
120	3	2	3	3	3	3	3	20	1	2	2	2	2	4	13	3	3	2	4	5	3	20	2	1	3	2	8	61
121	2	3	3	2	2	2	2	16	3	4	3	3	3	4	20	2	2	3	5	4	2	18	3	2	2	1	8	62
122	2	3	1	3	3	3	3	18	2	3	1	2	2	2	12	3	4	2	4	2	4	19	2	3	3	2	10	59
123	4	3	3	3	2	2	2	19	3	2	2	3	3	2	15	2	3	3	2	2	3	15	3	2	2	3	10	59
124	2	2	2	2	3	3	3	17	2	1	3	2	3	5	16	2	3	3	3	2	1	14	2	3	3	2	10	57
125	3	3	3	3	2	2	2	18	3	1	2	3	1	3	13	3	2	2	2	3	2	14	4	3	2	2	11	56
126	2	2	2	2	2	3	3	16	2	1	3	2	2	3	13	3	3	2	3	2	3	16	2	2	3	4	11	56
127	3	4	3	3	1	2	2	18	3	1	2	3	2	1	12	2	2	2	2	3	2	13	3	3	5	5	16	59
128	2	3	2	2	1	3	3	16	1	2	2	2	2	3	12	3	2	2	2	3	2	14	5	2	4	3	14	56
129	3	2	3	3	1	2	2	16	2	3	1	3	2	3	14	2	3	3	1	2	3	14	4	3	2	2	11	55
130	1	3	2	2	1	4	3	16	3	2	2	2	3	2	14	2	3	3	3	2	2	15	2	2	3	3	10	55
131	2	2	3	3	3	2	2	17	2	3	3	3	2	1	14	3	2	2	2	3	3	15	3	3	2	2	10	56

132	3	3	2	2	2	3	3	18	3	2	2	2	3	2	14	2	3	3	3	2	2	15	2	2	3	3	10	57
133	2	2	3	2	2	2	2	15	3	3	2	3	2	3	16	3	2	2	2	3	3	15	3	1	2	2	8	54
134	3	2	3	3	3	3	3	20	2	2	2	2	3	2	13	2	3	3	3	5	2	18	2	3	3	1	9	60
135	2	3	3	2	2	2	2	16	3	2	2	2	3	2	14	3	2	2	2	2	1	12	3	2	2	3	10	52
136	2	3	1	3	3	3	3	18	2	3	3	1	2	3	14	2	3	3	3	3	2	16	2	3	3	2	10	58
137	4	3	3	3	2	2	2	19	2	3	1	2	2	2	12	3	2	2	2	2	3	14	3	2	2	3	10	55
138	2	2	2	2	3	3	3	17	2	2	3	4	3	3	17	2	3	2	3	3	2	15	2	4	3	2	11	60
139	3	3	3	3	2	2	2	18	2	2	2	3	2	2	13	1	2	2	2	2	3	12	3	5	4	4	16	59
140	2	2	2	2	2	3	3	16	2	3	3	1	3	3	15	3	2	2	3	2	3	15	1	2	2	5	10	56
141	3	2	2	1	2	2	3	15	3	2	2	1	2	2	12	3	2	2	2	3	2	14	2	3	3	3	11	52
142	4	3	3	2	3	3	2	20	3	3	2	2	1	2	13	3	3	2	3	3	2	16	3	2	1	2	8	57
143	2	2	2	3	2	2	3	16	2	2	3	3	2	3	15	2	2	3	2	2	3	14	2	3	2	3	10	55
144	3	2	3	2	3	2	4	19	2	2	2	2	2	3	13	2	3	2	3	2	4	16	3	2	3	2	10	58
145	2	2	2	2	2	3	2	15	2	2	2	2	3	2	13	2	2	2	2	3	2	13	5	5	4	4	18	59
146	2	2	2	2	3	2	2	15	3	2	3	3	2	3	16	2	2	2	3	2	2	13	4	5	5	5	19	63
147	3	2	3	3	2	3	2	18	2	2	2	2	3	2	13	2	3	3	2	3	2	15	2	3	2	3	10	56
148	4	5	4	5	4	5	4	31	4	5	5	4	5	4	27	2	2	2	2	2	1	11	2	2	3	2	9	78
149	2	2	3	2	3	2	2	16	4	5	4	5	4	3	25	2	3	2	3	2	2	14	2	3	2	3	10	65
150	3	3	2	3	4	3	3	21	3	3	3	2	3	2	16	3	2	3	4	3	3	18	5	4	5	4	18	73
151	2	2	4	2	2	2	2	16	2	2	2	4	2	3	15	2	3	2	2	2	3	14	4	5	4	5	18	63
152	3	3	2	3	3	3	4	21	3	3	3	3	3	2	17	4	5	4	5	4	5	27	2	3	4	2	11	76
153	2	2	3	2	2	2	5	18	2	2	2	2	2	3	13	4	3	2	2	2	3	16	2	2	2	3	9	56
154	3	3	2	3	3	4	4	22	3	3	3	3	3	2	17	2	2	3	4	3	2	16	3	3	3	2	11	66
155	2	2	3	2	2	5	2	18	1	2	2	2	4	3	14	3	3	1	3	4	3	17	2	2	2	3	9	58
156	3	3	2	4	3	4	3	22	2	3	3	2	2	2	14	2	2	2	2	2	2	12	1	3	3	2	9	57
157	2	2	3	5	4	2	2	20	3	2	2	3	3	1	14	3	3	3	3	3	3	18	2	2	2	3	9	61
158	3	3	2	4	5	3	3	23	2	3	3	2	2	2	14	2	2	2	2	2	2	12	3	1	1	2	7	56
159	2	2	3	5	4	2	2	20	3	2	2	4	3	3	17	5	4	3	3	3	4	22	4	3	2	4	13	72

160	3	4	2	4	2	4	3	22	2	4	3	3	2	2	16	4	5	2	2	2	3	18	2	2	3	2	9	65
161	2	3	3	2	2	3	2	17	3	3	2	2	3	4	17	2	3	3	4	3	2	17	3	3	2	3	11	62
162	3	2	2	3	3	2	3	18	2	2	2	3	2	3	14	3	2	2	3	2	3	15	2	2	3	2	9	56

POS-TEST VARIABLE: SEGURIDAD DE LA INFORMACION (ISO 27001)																												
N°	D1: Planificación							SUB	D2: Implementación de la seguridad						SUB	D3: Implementación de los controles						SUB	D4: Implementación de las acciones				SUB	TOTAL
	1	2	3	4	5	6	7		8	9	10	11	12	13		14	15	16	17	18	19		20	21	22	23		
1	4	5	4	5	4	5	4	31	5	4	5	4	3	4	25	5	3	4	4	4	4	24	4	4	4	4	16	96
2	4	4	5	3	4	4	5	29	5	5	4	3	4	3	24	3	4	3	4	4	4	22	4	3	5	5	17	92
3	4	5	4	5	4	3	4	29	5	4	5	4	4	4	26	5	4	4	3	3	5	24	4	3	4	3	14	93
4	4	3	4	4	3	4	3	25	5	4	4	4	4	4	25	4	4	4	5	4	4	25	4	3	3	4	14	89
5	3	4	3	4	3	4	3	24	3	4	3	3	4	3	20	4	4	3	5	3	4	23	4	4	4	4	16	83
6	4	4	4	3	4	3	4	26	5	4	4	5	4	4	26	4	4	4	4	4	3	23	4	5	5	5	19	94
7	3	3	4	3	4	3	4	24	5	4	4	4	3	4	24	4	3	4	3	3	4	21	4	4	3	4	15	84
8	4	4	4	4	3	4	5	28	5	4	5	3	4	4	25	5	4	4	4	4	5	26	4	5	3	3	15	94
9	3	4	4	3	4	3	3	24	5	4	4	4	4	4	25	4	4	4	3	3	3	21	4	3	3	4	14	84
10	3	4	4	4	3	4	4	26	5	4	4	4	4	4	25	4	4	4	4	4	4	24	4	3	4	3	14	89
11	5	4	4	4	4	3	4	28	5	4	4	3	4	4	24	5	4	4	4	3	4	24	3	4	4	4	15	91
12	4	3	4	3	3	4	5	26	3	5	4	4	4	3	23	3	4	5	3	4	4	23	4	4	4	4	16	88
13	4	4	4	5	4	3	4	28	4	3	3	5	3	3	21	4	3	5	3	3	3	21	4	4	3	4	15	85
14	4	3	4	4	3	4	5	27	3	5	4	4	4	4	24	5	3	5	4	4	4	25	4	3	4	4	15	91
15	4	3	3	5	4	3	4	26	4	3	4	3	3	3	20	4	4	5	3	3	3	22	3	4	4	3	14	82
16	4	4	4	4	5	4	3	28	4	4	3	4	4	4	23	4	3	4	4	4	4	23	4	3	4	4	15	89
17	3	4	3	3	4	3	4	24	4	3	4	3	5	3	22	4	4	3	3	5	3	22	3	4	3	5	15	83

18	4	4	4	4	3	4	3	26	4	4	5	4	3	4	24	4	3	5	4	4	4	24	4	3	4	3	14	88
19	3	3	3	3	4	3	4	23	4	3	5	3	4	3	22	4	4	3	4	3	3	21	3	4	3	4	14	80
20	4	4	5	4	3	4	3	27	5	4	5	4	3	4	25	4	4	4	3	4	4	23	4	3	4	3	14	89
21	3	3	4	3	5	3	5	26	4	3	5	3	4	3	22	3	4	3	4	3	5	22	3	4	3	4	14	84
22	4	3	5	4	4	4	4	28	5	5	4	4	3	4	25	4	4	3	3	4	4	22	4	5	4	3	16	91
23	3	3	4	5	3	3	3	24	4	3	3	3	4	3	20	3	3	4	3	4	3	20	3	4	5	4	16	80
24	4	4	3	4	4	4	4	27	5	4	4	4	3	5	25	4	4	3	5	3	4	23	5	3	4	4	16	91
25	3	4	3	3	3	3	3	22	4	3	3	3	4	4	21	3	3	4	4	4	3	21	4	4	4	5	17	81
26	4	3	3	4	4	4	4	26	4	3	4	4	5	3	23	4	4	3	4	3	4	22	4	3	3	4	14	85
27	4	3	5	3	3	3	3	24	3	4	3	3	5	4	22	3	4	4	4	4	3	22	3	4	4	3	14	82
28	5	3	5	4	4	4	4	29	5	3	4	4	5	4	25	4	4	3	4	3	4	22	4	3	4	3	14	90
29	4	4	5	3	3	3	3	25	4	4	3	3	3	4	21	3	4	4	4	3	4	22	3	4	3	4	14	82
30	4	3	4	4	4	4	4	27	3	3	4	4	4	3	21	4	4	4	3	4	3	22	5	3	5	3	16	86
31	4	4	3	3	5	3	3	25	4	4	3	3	3	4	21	3	3	5	4	3	4	22	4	4	4	4	16	84
32	4	3	5	4	4	4	4	28	3	3	4	4	4	3	21	4	4	4	3	4	3	22	4	3	4	3	14	85
33	4	4	3	4	3	3	3	24	4	4	3	3	3	5	22	3	5	3	4	3	4	22	3	4	5	4	16	84
34	4	4	4	3	4	4	4	27	3	3	4	4	4	4	22	4	4	4	3	4	3	22	4	3	4	3	14	85
35	3	4	3	4	3	5	3	25	4	4	3	3	3	3	20	3	3	3	4	5	4	22	3	4	3	4	14	81
36	4	4	4	5	4	3	4	28	3	3	4	4	4	4	22	3	5	4	4	4	4	24	4	3	4	3	14	88
37	3	4	3	5	3	4	3	25	4	4	3	4	3	3	21	4	3	3	5	3	3	21	5	4	3	4	16	83
38	3	5	4	5	4	3	4	28	3	5	4	4	4	4	24	3	4	4	5	4	4	24	4	3	4	3	14	90
39	3	4	3	5	3	4	3	25	4	3	3	5	3	3	21	4	3	3	4	3	3	20	3	4	3	4	14	80
40	5	5	5	4	4	3	4	30	3	4	4	5	4	4	24	4	4	4	3	4	4	23	4	4	4	3	15	92
41	5	4	3	3	3	4	3	25	3	3	4	4	5	4	23	3	4	3	4	3	4	21	3	5	3	4	15	84
42	5	5	4	4	4	3	5	30	4	4	3	3	4	3	21	4	4	4	4	4	3	23	4	4	4	4	16	90
43	4	4	3	3	3	4	4	25	4	4	4	4	4	3	23	4	4	4	4	3	4	23	3	3	3	3	12	83
44	4	4	4	4	4	3	3	26	4	4	4	4	3	4	23	3	4	3	3	4	3	20	4	4	4	4	16	85
45	3	4	3	3	3	4	4	24	3	4	3	3	4	3	20	4	4	4	4	3	4	23	3	4	4	3	14	81

46	4	3	5	4	4	3	3	26	4	4	4	4	3	4	23	3	3	4	3	4	3	20	4	5	3	4	16	85
47	3	4	4	3	3	4	4	25	3	3	4	3	4	3	20	4	4	4	4	3	4	23	3	4	4	3	14	82
48	4	3	3	4	3	4	3	24	4	4	4	4	3	4	23	4	4	3	3	4	3	21	4	3	3	4	14	82
49	3	4	4	3	5	3	4	26	3	4	4	3	4	3	21	4	4	4	4	4	3	23	3	4	4	5	16	86
50	4	3	3	4	4	4	3	25	3	4	4	4	3	4	22	4	4	4	4	3	4	23	4	3	3	4	14	84
51	4	4	4	3	4	3	4	26	3	3	4	3	3	4	20	3	4	3	3	4	3	20	3	4	4	3	14	80
52	4	3	4	4	4	4	3	26	4	4	3	4	4	3	22	4	4	4	4	3	4	23	5	4	3	4	16	87
53	3	4	4	3	4	3	4	25	4	3	4	3	4	4	22	3	3	4	3	4	3	20	4	3	4	3	14	81
54	4	3	4	4	4	3	4	26	4	4	4	4	3	4	23	4	4	4	4	3	4	23	4	4	3	4	15	87
55	3	4	4	4	3	4	3	25	4	4	4	3	4	4	23	3	4	4	3	4	3	21	4	5	4	4	17	86
56	4	3	3	5	4	3	4	26	4	3	3	4	3	4	21	3	4	4	4	3	4	22	5	5	3	3	16	85
57	3	4	4	4	3	4	3	25	4	4	4	4	4	5	25	5	4	4	4	4	3	24	5	3	4	4	16	90
58	4	3	5	3	4	3	4	26	4	3	4	3	4	4	22	4	3	4	3	3	4	21	4	4	4	3	15	84
59	3	4	4	4	3	4	3	25	3	4	3	4	3	3	20	4	4	4	5	4	3	24	4	3	4	4	15	84
60	4	3	3	3	4	5	4	26	4	4	4	4	4	4	24	4	4	4	4	4	4	24	3	4	3	3	13	87
61	3	4	4	4	3	4	3	25	3	4	3	3	3	4	20	5	4	4	4	3	4	24	5	3	4	4	16	85
62	4	3	3	3	4	4	4	25	4	3	4	4	4	5	24	3	4	5	3	4	4	23	4	4	3	4	15	87
63	4	4	4	4	3	3	3	25	3	4	3	3	4	4	21	4	3	5	3	3	3	21	3	3	4	4	14	81
64	3	3	3	3	4	4	4	24	4	3	4	4	5	4	24	5	3	5	4	4	4	25	4	4	5	5	18	91
65	4	4	4	4	4	3	3	26	3	4	4	3	4	3	21	4	4	5	3	3	3	22	3	3	4	4	14	83
66	3	4	3	3	5	4	4	26	4	3	5	4	4	4	24	4	3	4	4	4	4	23	4	4	3	5	16	89
67	4	3	4	4	5	3	3	26	5	4	4	4	4	4	25	4	4	3	3	5	3	22	3	5	4	4	16	89
68	3	4	3	3	5	4	4	26	3	4	3	3	4	3	20	5	4	4	3	4	4	24	5	3	3	3	14	84
69	5	3	4	4	5	4	3	28	5	4	4	5	4	4	26	3	5	4	4	4	3	23	4	4	5	4	17	94
70	4	4	3	3	3	4	4	25	5	4	4	4	3	4	24	4	3	3	5	3	3	21	4	3	4	3	14	84
71	3	3	4	4	4	3	3	24	5	4	5	3	4	4	25	3	5	4	4	4	4	24	3	4	3	4	14	87
72	4	4	3	3	3	4	4	25	5	4	4	4	4	4	25	4	3	4	3	3	3	20	4	3	4	3	14	84
73	3	3	4	4	4	3	3	24	5	4	4	4	4	4	25	4	4	3	4	4	4	23	3	4	3	4	14	86

74	4	4	3	3	3	5	4	26	5	4	4	3	4	4	24	4	3	4	3	5	3	22	4	4	4	5	17	89
75	3	3	4	4	4	4	5	27	3	5	4	4	4	3	23	4	4	5	4	3	4	24	3	5	3	4	15	89
76	4	4	3	3	3	3	4	24	4	3	3	5	3	3	21	4	3	5	3	4	3	22	4	3	4	3	14	81
77	3	3	4	4	4	4	3	25	4	3	3	5	3	3	21	5	4	5	4	3	4	25	3	4	3	5	15	86
78	4	4	3	4	3	3	4	25	3	5	4	4	4	4	24	4	4	4	4	3	4	23	4	4	3	5	16	88
79	3	5	4	4	4	4	3	27	4	3	4	3	3	3	20	3	4	3	3	4	5	22	4	3	4	4	15	84
80	4	3	3	5	3	3	4	25	4	4	3	4	4	4	23	4	4	5	4	3	4	24	3	4	3	4	14	86
81	3	4	4	5	4	4	3	27	4	3	4	3	5	3	22	3	4	4	3	4	5	23	5	3	4	4	16	88
82	4	3	3	4	3	3	4	24	4	4	5	4	3	4	24	3	3	5	4	3	4	22	4	4	4	4	16	86
83	4	4	4	3	4	4	3	26	4	3	5	3	4	3	22	4	4	4	5	4	3	24	3	3	3	5	14	86
84	3	4	3	4	3	4	4	25	5	4	5	4	3	4	25	4	3	3	4	3	4	21	4	4	4	4	16	87
85	4	4	4	4	4	3	4	27	4	3	5	3	4	3	22	4	4	4	3	4	3	22	3	5	5	3	16	87
86	4	4	4	4	3	4	4	27	5	5	4	4	3	4	25	3	3	3	4	3	4	20	4	3	4	4	15	87
87	3	4	3	3	4	3	4	24	4	3	3	3	4	3	20	4	5	4	3	4	3	23	3	4	4	3	14	81
88	4	4	4	4	3	4	5	28	5	4	4	4	3	5	25	3	4	3	5	3	5	23	4	3	3	4	14	90
89	3	3	4	3	4	3	4	24	4	3	3	3	4	4	21	3	4	3	4	4	4	22	3	4	4	3	14	81
90	4	4	4	4	3	4	5	28	4	4	4	4	3	3	22	5	4	4	3	3	5	24	4	3	3	4	14	88
91	3	4	4	4	3	4	3	25	4	3	3	3	4	4	21	4	4	4	5	4	4	25	5	4	4	4	17	88
92	4	3	3	5	4	3	4	26	3	5	4	4	3	3	22	4	4	3	5	3	4	23	4	3	3	5	15	86
93	3	4	4	4	3	4	3	25	4	4	4	3	3	4	22	4	4	4	4	4	3	23	4	4	5	3	16	86
94	4	3	5	3	4	3	4	26	4	3	3	4	4	3	21	4	3	4	3	3	4	21	3	5	4	4	16	84
95	3	4	4	4	3	4	3	25	4	4	4	3	3	5	23	5	4	4	4	4	5	26	4	3	3	4	14	88
96	4	3	3	3	4	5	4	26	3	4	3	4	4	4	22	4	4	4	3	3	3	21	3	4	4	5	16	85
97	3	4	4	4	3	4	3	25	4	4	4	3	3	3	21	4	4	4	4	4	4	24	4	3	3	4	14	84
98	3	3	4	3	4	3	4	24	4	4	3	4	4	4	23	5	4	5	4	4	4	26	3	4	4	3	14	87
99	4	4	4	4	3	4	5	28	4	4	4	4	3	3	22	5	4	4	4	4	4	25	4	4	3	4	15	90
100	3	4	4	4	3	4	3	25	4	4	4	4	4	4	24	3	4	3	3	4	3	20	3	5	4	4	16	85
101	4	3	3	5	4	3	4	26	3	4	3	5	3	3	21	5	4	4	5	4	4	26	4	3	3	5	15	88

102	4	3	5	4	4	4	4	28	4	4	5	5	4	4	26	5	4	4	4	3	4	24	3	4	4	4	15	93
103	4	4	3	4	3	3	3	24	3	4	4	4	3	3	21	5	4	5	3	4	4	25	4	3	4	3	14	84
104	4	4	4	3	4	4	4	27	3	3	5	3	4	4	22	5	4	4	4	4	4	25	4	4	3	3	14	88
105	3	4	3	4	3	5	3	25	4	4	4	4	3	4	23	5	4	4	4	4	4	25	4	3	4	4	15	88
106	4	4	4	5	4	3	4	28	4	3	3	4	4	3	21	5	4	4	3	4	4	24	3	4	5	5	17	90
107	3	4	3	5	3	4	3	25	4	4	4	4	3	4	23	3	5	4	4	4	3	23	5	3	4	3	15	86
108	3	5	4	5	4	3	4	28	3	3	3	3	4	3	19	4	3	3	5	3	3	21	4	4	3	4	15	83
109	3	4	3	5	3	4	3	25	4	5	4	4	3	4	24	3	5	4	4	4	4	24	3	5	4	3	15	88
110	5	5	5	4	4	3	4	30	3	4	4	3	4	4	22	4	4	4	4	4	4	24	4	3	4	4	15	91
111	5	4	3	3	3	4	3	25	3	5	3	4	3	3	21	4	4	3	4	3	4	22	3	4	4	3	14	82
112	5	5	4	4	4	3	5	30	4	4	4	5	4	4	25	3	3	4	3	4	3	20	4	3	3	4	14	89
113	4	4	4	4	3	4	3	26	4	5	3	5	3	3	23	4	4	4	4	4	4	24	5	4	4	4	17	90
114	3	3	3	3	4	3	4	23	4	4	4	5	4	4	25	3	3	4	3	3	3	19	4	3	3	4	14	81
115	4	4	5	4	3	4	3	27	4	4	3	5	3	3	22	4	4	3	4	4	4	23	4	4	5	3	16	88
116	3	3	4	3	5	3	5	26	4	4	5	4	4	4	25	3	3	4	3	3	4	20	3	3	4	5	15	86
117	4	3	5	4	4	4	4	28	5	4	3	3	3	4	22	4	4	3	4	4	5	24	4	4	4	3	15	89
118	3	3	4	5	3	3	3	24	3	3	4	4	4	4	22	3	3	4	4	3	4	21	3	3	3	4	13	80
119	4	4	3	4	4	4	4	27	3	3	3	3	3	4	19	4	4	3	5	4	4	24	5	4	4	3	16	86
120	3	4	3	3	3	3	3	22	5	4	4	4	4	4	25	3	3	4	4	5	3	22	4	5	3	4	16	85
121	4	3	3	4	4	4	4	26	3	4	3	3	3	4	20	4	4	3	5	4	4	24	3	4	4	5	16	86
122	4	3	5	3	3	3	3	24	4	3	5	4	4	4	24	3	4	4	4	4	4	23	4	3	3	4	14	85
123	4	3	3	3	4	4	4	25	3	4	4	3	3	4	21	4	3	3	4	4	3	21	3	4	4	3	14	81
124	4	4	4	4	3	3	3	25	4	5	3	4	3	5	24	4	3	3	3	4	5	22	4	3	3	4	14	85
125	3	3	3	3	4	4	4	24	3	5	4	3	5	3	23	3	4	4	4	3	4	22	4	3	4	4	15	84
126	4	4	4	4	4	3	3	26	4	5	3	4	4	3	23	3	3	4	3	4	3	20	4	4	3	4	15	84
127	3	4	3	3	5	4	4	26	3	5	4	3	4	5	24	4	4	4	4	3	4	23	3	3	5	5	16	89
128	4	3	4	4	5	3	3	26	5	4	4	4	4	3	24	3	4	4	4	3	4	22	5	4	4	3	16	88
129	3	4	3	3	5	4	4	26	4	3	5	3	4	3	22	4	3	3	5	4	3	22	4	3	4	4	15	85

130	5	3	4	4	5	4	3	28	3	4	4	4	3	4	22	4	3	3	3	4	4	21	4	4	3	3	14	85
131	4	4	3	3	3	4	4	25	4	3	3	3	4	5	22	3	4	4	4	3	3	21	3	3	4	4	14	82
132	3	3	4	4	4	3	3	24	3	4	4	4	3	4	22	4	3	3	3	4	4	21	4	4	3	3	14	81
133	4	4	3	4	4	4	4	27	3	3	4	3	4	3	20	3	4	4	4	3	3	21	3	5	4	4	16	84
134	3	4	3	3	3	3	3	22	4	4	4	4	3	4	23	4	3	3	3	5	4	22	4	3	3	5	15	82
135	4	3	3	4	4	4	4	26	3	4	4	4	3	4	22	3	4	4	4	4	5	24	3	4	4	3	14	86
136	4	3	5	3	3	3	3	24	4	3	3	5	4	3	22	4	3	3	3	3	4	20	4	3	3	4	14	80
137	4	3	3	3	4	4	4	25	4	3	5	4	4	4	24	3	4	4	4	4	3	22	3	4	4	3	14	85
138	4	4	4	4	3	3	3	25	4	4	3	4	3	3	21	4	3	4	3	3	4	21	4	4	3	4	15	82
139	1	2	1	2	1	2	1	10	1	4	3	4	3	4	19	5	4	4	4	4	3	24	3	5	4	4	16	69
140	4	4	4	4	4	3	3	26	4	3	3	5	3	3	21	3	4	4	3	4	3	21	5	4	4	5	18	86
141	3	4	4	5	4	4	3	27	3	4	4	5	4	4	24	3	4	4	4	3	4	22	4	3	3	3	13	86
142	4	3	3	4	3	3	4	24	3	3	4	4	5	4	23	3	3	4	3	3	4	20	3	4	5	4	16	83
143	4	4	4	3	4	4	3	26	4	4	3	3	4	3	21	4	4	3	4	4	3	22	4	3	4	3	14	83
144	3	4	3	4	3	4	4	25	4	4	4	4	4	3	23	4	3	4	3	4	4	22	3	4	3	4	14	84
145	4	4	4	4	4	3	4	27	4	4	4	4	3	4	23	4	4	4	4	3	4	23	5	4	4	4	17	90
146	4	4	4	4	3	4	4	27	3	4	3	3	4	3	20	4	4	4	3	4	4	23	4	5	3	5	17	87
147	3	4	3	3	4	3	4	24	4	4	4	4	3	4	23	4	3	3	4	3	4	21	4	3	4	3	14	82
148	4	4	4	4	4	4	5	29	3	3	4	3	4	3	20	4	4	4	4	4	5	25	4	4	3	4	15	89
149	4	4	3	4	3	4	4	26	4	4	4	3	4	3	22	4	3	4	3	4	4	22	4	3	4	3	14	84
150	3	3	4	3	4	3	3	23	3	3	3	4	3	4	20	3	4	3	4	3	3	20	4	3	4	4	15	78
151	4	4	4	4	4	4	4	28	4	4	4	4	4	3	23	4	3	4	4	4	3	22	5	4	3	3	15	88
152	3	3	4	3	3	3	4	23	3	3	3	3	3	4	19	3	4	3	3	3	4	20	4	3	4	4	15	77
153	4	4	3	4	4	4	5	28	4	4	4	4	4	3	23	4	3	4	4	4	3	22	4	4	4	3	15	88
154	3	3	4	3	3	4	4	24	3	3	3	3	3	4	19	4	4	3	4	3	4	22	3	3	3	4	13	78
155	4	4	3	4	4	5	4	28	5	4	4	4	4	3	24	3	3	5	3	4	3	21	4	4	4	3	15	88
156	3	3	4	4	3	4	3	24	4	3	3	4	4	4	22	4	4	4	4	4	4	24	5	3	3	4	15	85
157	4	4	3	5	4	4	4	28	3	4	4	3	3	5	22	3	3	3	3	3	3	18	4	4	4	3	15	83

158	3	3	4	4	5	3	3	25	4	3	3	4	4	4	22	4	4	4	4	4	4	24	3	5	5	4	17	88
159	4	4	3	5	4	4	4	28	3	4	4	4	3	3	21	5	4	3	3	3	4	22	4	3	4	4	15	86
160	3	4	4	4	4	4	3	26	4	4	3	3	4	4	22	4	5	4	4	4	3	24	4	4	3	4	15	87
161	4	3	3	4	4	3	4	25	3	3	4	4	3	4	21	4	3	3	4	3	4	21	3	3	4	3	13	80
162	3	4	4	3	3	4	3	24	4	4	4	3	4	3	22	3	4	4	3	4	3	21	4	4	3	4	15	82

Anexo 5. Evidencia digital de similitud

UNIVERSIDAD PERUANA DE CIENCIAS INFORMÁTICA
ESCUELA DE POSGRADO
MAESTRÍA EN INVESTIGACIÓN Y DOCENCIA UNIVERSITARIA



TESIS
Candidato: del servicio educativo y la satisfacción estudiantil de la Facultad de Farmacia y
Biotecnología de la Universidad Peruana Los Andes en el año 2021

AUTOR:
García Marino, Rubi Clara
Cabrera Córdova, Rand John

PARA OPTAR EL GRADO ACADÉMICO DE:
Máster en Investigación y Docencia Universitaria

ASESOR:
Mg. Zúñiga Romanos, Henry Alex
ORCID: 0000-0001-6418-0108

LIMA – PERÚ
2022

23

Alta resolución Activado

Versión solo texto del informe

Número de palabras: 21675

Página: 1 de 94

Anexo 6. Autorización de publicación en el repositorio



FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Huaney Tinoco Julio Cesar

DNI: 43716762 Correo electrónico: juce6485@gmail.com

Domicilio: Barrio de Nueva Florida, Av. Interoceánica media S/N.

Teléfono fijo: _____ Teléfono celular: 943954475

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: de Posgrado

Tipo: Trabajo de Investigación Bachiller () Tesis (X)

Título del Trabajo de Investigación / Tesis:

"Infraestructura de un Data Center Para la Seguridad de la
Información (ISO 27001) de la Municipalidad Provincial
de Huaraz 2021."

3.- OBTENER:

Bachiller () Título () Mg. (X) Dr. () PhD. ()

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (<http://repositorio.upci.edu.pe>), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art.23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):

() Sí, autorizo el depósito y publicación total.

() No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 16 días del mes de agosto de 2022.


Firma



Evidencias fotográficas





