UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

ESCUELA DE POSGRADO

TESIS

IMPLEMENTACIÓN DE LOS CONTROLES DE LA ISO/IEC 27002:2013 PARA LA GESTIÓN DE LA BASE DE DATOS DE LOS REGISTROS PÚBLICOS DE LA ZONA VII – SEDE HUARAZ, 2019

PRESENTADO POR

BERÚ APAMEL MEJIA CUENTAS

PARA OPTAR EL GRADO ACADÉMICO DE

MAESTRO EN GESTIÓN TECNOLOGICA DE LA INFORMACIÓN

ASESOR

Mg. SANDRA NASHELI LOZANO ARAGÓN

LÍNEA DE INVESTIGACIÓN

GESTIÓN DE SISTEMAS DE INFORMACIÓN

LIMA - PERÚ

2020

Dedicatoria

A mi querida familia

Agradecimiento

A los docentes de la Escuela de Posgrado de la Universidad Peruana de Ciencias e Informática.

Índice

Lista de tablas

Lista de figuras

Resumen

La investigación tiene por finalidad Demostrar el impacto de implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, mediante un enfoque cuantitativo, basado en resultados estadísticos, de diseño experimental – pre experimental, debido a que solo se manipula la variable dependiente y se realizan observaciones a través de instrumentos, por otro lado es de alcance temporal longitudinal, pues se aplicó el instrumento en dos momentos, esto es antes de la implementación de la red de datos (pretest) y otro después de la implementación de la red de datos (postest), así mismo se trabajó con una población censal conformada por 12 trabajadores, la técnica empleada fue la encuesta y el instrumento una cuestionario para la variable gestión de información, con opciones de respuesta politómicas, pasando por un proceso de validez y confiabilidad antes de ser aplicada, en donde se concluyó: Se demostró la afectividad de los controles de la ISO/IEC 27002:2013 sobre la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, obteniendo resultados que en el nivel deficiente se mejoró en 91.7 %, en el nivel regular se mantuvo su percepción y en el nivel eficiente se incrementó en un 71.7 %, con lo cual se comprueba la hipotesis afirmando que existe mejoras significativas de los resultados en la comparación del pre y post test.

Palabras claves: Controles de la ISO/IEC 27002:2013, gestión de la base de datos

Abstract

The purpose of the research is to demonstrate the impact of implementing the controls of ISO / IEC 27002: 2013, favoring the management of the database of Public Registries in Zone VII - Huaraz Headquarters, 2019, through a quantitative approach , based on statistical results, experimental design - pre experimental, because only the dependent variable is manipulated and observations are made through instruments, on the other hand it is of longitudinal temporal scope, because the instrument was applied in two moments, this it is before the implementation of the data network (pretest) and another one after the implementation of the data network (posttest), likewise, we worked with a census population made up of 12 workers, the technique used was the survey and the instrument a questionnaire for the variable information management, with polytomic response options, going through a process of validity and reliability before being applied, in where it was concluded: The affectivity of the controls of ISO / IEC 27002: 2013 on the management of the database of the Public Registries of Zone VII - Huaraz Headquarters, 2019, was demonstrated, obtaining results that at the deficient level was improved in 91.7%, at the regular level its perception was maintained and at the efficient level it was increased by 71.7%, with which the hypothesis is verified affirming that there are significant improvements of the results in the comparison of the pre and post test.

Keywords: ISO / IEC 27002: 2013 controls, database management

Introducción

El estudio se enmarca en desarrollar una estrategia que permita gestionar la base de datos de registros públicos de la zona VII- Sede Huaraz a través de la implementación de los controles de la ISO/IEC 27002:2013, para ello el investigador ha desarrollado un plan de mejora que fue implementado para determinar la efectividad en la gestión de la base de datos.

El desarrollo del estudio se basa en el enfoque cuantitativo, con diseño experimental – pre experimental, basándose en el análisis de la gestión de la base de datos y demostrando el efecto que tiene los controles de la ISO, el alcance temporal que presenta el estudio es longitudinal, basándose en l recolección de datos en dos momentos, antes y después de implementar los controles planificados por la norma ISO.

Para la selección de la población y muestra, se consideró una muestra censal, basándose en la cantidad de la población, como muestra, representada por 12 trabajadores, del área de informática, a quienes se les aplico la técnica de la encuesta y como instrumento se usó el cuestionario.

Para el desarrollo del estudio se basa en realizar el proceso de validez y confiabilidad del instrumentos antes de ser aplicado a los trabajadores dl área de informática, los cuales permitirá que los resaltados sean los más adecuados y cumplan con los requisitos de veracidad y claridad para el desarrollo del estudio, permitiendo arribar a las conclusiones previstas.

Capítulo I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática:

Mantener asegurada la red es muy importante para toda organización, porque es el punto céntrico, en donde, las empresas utilizan las tecnologías de la información para mantenerse conectados y permitir a sus trabajadores que cuenten con información que les permita realizar su trabajo de manera eficiente y oportuna, es importante mencionar el estudio realizado por Torres y Lavayen (2017), quien desarrolló un trabajo en Ecuador, mencionando que existe un manejo masivo de recursos y datos dentro de las empresas, sin estar integrados a un Sistema de Gestión de Seguridad de la información, lo cual atrae cada vez más a diferentes atacantes conllevando perjuicios y convirtiéndose en un riesgo eminente para el mejoramiento y la repotenciación de las instituciones, como para cada una de las áreas que la conforman. También resalta que información representa un pilar fundamental dentro de cada organización por lo cual surge la necesidad de protegerla, sin

importar el soporte en el que se encuentre, por lo tanto, es imprescindible que la Empresa Eléctrica Quito evalué los riesgos, estrategias y controles para salvaguardar de forma permanente la protección de los datos. Y en la Empresa Eléctrica Quito, la seguridad de la información busca establecer normas y políticas con la finalidad de mantener la confidencialidad, integridad y disponibilidad de la información, puesto que la falta del cumplimiento de estos objetivos pondría a la empresa en riesgo al punto de afectar la integridad de datos de la empresa referida.

En el caso de Perú, el estudio realizado por Gavidia y Torres (2018), en Lima, encontró que el área de TI de la UPN programa sus funciones de acuerdo al Plan Operativo Anual (POA), donde se percibía que carecían de una infraestructura apropiada para el desarrollo de sus actividades. Adicionalmente, se observaba que existía un mal manejo de las políticas de seguridad de la información, puesto que estas no se encontraban documentadas, ni estaban bien definidas, además de no ser revisadas constantemente, igualmente se distinguió que existía una ineficiente gestión de riesgos de la información, por lo que se llegó a percibir que dentro del área de TI de la UPN existió un bajo nivel de gestión de la seguridad física y lógica de la información. Entre los factores principales que intervinieron se halló que hubo medidas limitadas de seguridad de la información a nivel lógico y físico lo que conllevaba a darse posibles errores los cuales podrían ser: pérdida de información, fallas en los sistemas y aplicaciones, fallas internas en los activos de información, entre otros. Esta situación motivaba la vulnerabilidad de la información, lo que se agravaba por el desconocimiento de la norma ISO/IEC 27002 para la Gestión de la Seguridad de la Información por parte del personal del Área de TI.

En el contexto regional se evidencia que las empresas no se preocupan por asegurar su información y mantener políticas que le permitan que todos sus datos se encuentren disponibles para los trabajadores, es importante mencionar que las empresas de Huaraz, en

especial las entidades públicas presentan deficiencias en este aspecto, dejando de lado la seguridad de sus datos.

En los registros públicos de la Zona VII – Sede Huaraz se evidencia que existe un problema con la seguridad de la base de datos, dejando de lado la implementación de políticas, que garanticen la información y permitan a los trabajadores contar con la información segura y disponible. Dentro de este contexto por problemas principales por lo que afronta los registros públicos es la falta de equipos que le permitan asegurar la información, también la falta de protocolos que garanticen la disponibilidad de los datos.

Uno de los problemas resaltantes por los que afronta los registros públicos es la necesidad de mantener a su personal del área de informática capacitada y con los conocimientos necesarios para que puedan realizar su trabajo de manera eficiente, con los protocolos que se requieren para la gestión de la base de datos.

1.2 Definición del problema

1.2.1 Problema general

¿Cómo la implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, ¿2019?

1.2.2 Problemas específicos

¿Cómo se presenta la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013?

¿Cómo se presenta la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013?

¿Qué niveles se alcanzaron al comparar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013?

1.3. Objetivos de la investigación:

1.3.1. Objetivo general:

Demostrar el impacto de implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

1.3.2. Objetivos específicos

Diagnosticar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013.

Analizar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013.

Comparar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

1.4. Hipótesis de la investigación

1.4.1. Hipótesis general

Hi: La implementación de los controles de la ISO/IEC 27002:2013, favorece a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

H0: La implementación de los controles de la ISO/IEC 27002:2013, no favorece a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

1.4.2. Hipótesis específicas

H1i: La gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013, es deficiente.

H2i: La gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013, es eficiente.

H3i: La comparación la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013, resulta favorable.

1.5. Variables y dimensiones

Variable independiente: Controles de la ISO/IEC 27002:2013

Variable dependiente: Gestión de la base de datos

Definición conceptual de la variable independiente: Controles de la ISO/IEC 27002:2013

Según Parra (2017), La información es un recurso que, como el resto de los activos, tiene un valor importante para todas las empresas, por lo que debe protegerse adecuadamente. La seguridad de la información se protege de diversas amenazas, con el objetivo de garantizar la continuidad del conocimiento de la empresa, reducir el daño y reducir el retorno de oportunidades e inversiones.

Definición operacional de la variable independiente: Controles de la ISO/IEC 27002:2013

Es la aplicación de los conocimientos relacionados a la seguridad que se debe tener, relacionado a la información de la empresa, para el caso del estudio se plantea un plan de trabajo para aplicarlo a los registros públicos.

Definición conceptual de la variable dependiente: Gestión de la base de datos

Es un conjunto de programas que permiten el almacenamiento, modificación y extracción de información en una base de datos. Los usuarios pueden acceder a la información utilizando herramientas específicas para consultar y generar informes, o mediante aplicaciones para este propósito.

Definición operacional de la variable dependiente: Gestión de la base de datos

Es el gestión y protección de la base de datos de los registros públicos, realiza por el personal de sistemas y las políticas con la que cuenta la institución.

Operacionalización de variables

Al realizar la operacionalización de las variables se tiene en cuenta que la finalizar de realizar esta acción es obtener el instrumento que se utilizara para recolectar información y alcanzar los objetivos establecidos por el investigador:

Tabla 1.

Operacionalización de la variable Controles de la ISO/IEC 27002:2013.

Dimensiones	Indicadores	Ítems	Escala y valores	Niveles y rango
D1: Gestión de Activos	Inventario de Activos Directrices de Clasificación Gestión de Soporte Extraíble	No corresponde	No presenta, porque de esta variable se desarrolla las sesiones que comprende la capacitación relacionado a los controles de la ISO/IEC 27002:2013.	Por ser el desarrollo de la capacitación de los controles no presenta una escala, tampoco rangos para su evaluación.
D2: Control de Acceso	Política de control de accesos. Control de acceso a las redes y servicios asociados Gestión de altas/bajas en el registro de usuarios. Gestión de los derechos de acceso asignación a usuarios. Gestión de los derechos de acceso con privilegios especiales. Gestión de información confidencial de autenticación de Usuarios. Retirado o adaptación de los derechos de acceso			

	Uso de Información confidencial para la autenticación.	
D3: Seguridad Física y Ambiental	Política de uso del control de criptográficos.	
	Gestión de Claves.	
D4: Seguridad de las Operaciones	Gestión de Cambios	
	Gestión de capacidades	
D5: Aspectos de seguridad de la información para la gestión del a continuidad del negocio.	Planificación de la continuidad de la seguridad de la información	
	Implantación de la continuidad de la seguridad de la información	

Fuente: Gavidia y Torres (2018)

Tabla 2.

Operacionalización de la variable Gestión de la base de datos.

Dimensiones	Indicadores	Ítems	Escala y valores	Niveles y rango
D1: Disponibilidad de la Base de Datos	Horario de acceso de los usuarios	1	1. Nunca 2. Casi nunca 3. A veces 4. Casi siempre 5. Siempre	Deficiente Regular Eficiente
	Tipo de acceso de los usuarios	2		
	Permisos y pollitas de acceso a la base de datos	3,4		
D2: Escalabilidad de la base de datos	Crecimiento de la base de datos	5		
		6		
	Adaptación a otras tecnologías	7		
		8		
	Espacio del disco duro del servidor	9		
	Capacidad física del servidor			
D3: Accesibilidad de consulta y escritura	Acceso de consultas	10 - 11		
	Tiempo de respuesta de la base de datos	12 - 13		
D4: Respaldo y copias de seguridad	Copias de seguridad	14		
	Almacenamiento de las copias de seguridad.	15 16 17		
	Acceso a las copias de seguridad	18		
	Seguridad física de la base de datos			

Fuente: Elaboración propia

1.6. Justificación de la investigación

El estudio presenta la siguiente justificación que facilita resaltar la importancia que tiene para el desarrollo del trabajo, resaltando lo siguiente:

Relevancia social: Es importante mencionar que el estudio se considera relevante para los trabajadores y la gerencia de los registros públicos, resaltando la importancia que tiene el desarrollo de la investigación, para realizar el análisis de las fortalezas y debilidades que presenta la gestión de la base de datos.

Justificación practica: El estudio se centra en analizar de manera cuantitativa como se percibe la gestión de la base de datos, a partir de un análisis realizado al área de informática y a su personal con la finalidad de analizar cuáles son los puntos más alto y más bajos, con la finalidad de establecer estrategias que ayuden a mejorar esta percepción.

Justificación metodológica, el estudio al plantear y elaborar un instrumento para el desarrollo del estudio, se considera relevante porque permite a los futuros investigadores realizar estrategias que favorezcan a la gestión de base de datos y les permita analizar otras empresas a partir del instrumento diseñado por el investigador.

Respecto a la justificación teórica, se tiene que el estudio es importante porque a las conclusiones.

Capítulo II

2. MARCO TEÓRICO

2.1. Antecedentes de la investigación

Ámbito internacional

Aleman (2015), En Tunja Colombia, hizo una tesis titulada: Metodología para la implementación de un SGSI en la fundación universitaria juan de castellanos, bajo la norma ISO 27001:2005. Su objetivo de investigación fue Establecer una metodología para la implementación de un SGSI en la Fundación Universitaria Juan de Castellanos, teniendo como base el estándar ISO 27001. Se estudió a la fundación universitaria Juan de Castellanos para establecer los pasos a seguir para la implementación de un SGSI para gestionar la seguridad. Asimismo, La presente metodología basada en la Norma ISO 27001 y su guía de buenas prácticas ISO 27002, permitirán Determinar los parámetros y lineamientos que se deben tener en cuenta para la implementación de un SGSI, basado en la norma ISO 27001:2005 en una organización, Analizar la

estructura organización y características principales de la Fundación Universitaria Juan de Castellanos para posteriormente proponer una metodología que permita gestionar la seguridad informática, diseñar una metodología para la implementación y mantenimiento de un SGSI, norma ISO 27001, Recomendar algunas herramientas que faciliten la implementación del SGSI en cada una de las etapas propuestas por la norma ISO 27001:2005. Finalmente, los resultados obtenidos al medir las variables de estudios se concluye que la Fundación Universitaria Juan de Castellanos logro organizar, diseñar y administrar de manera sistemática su SGSI, La metodología propuesta y aplicación del SGSI le permitirá a su vez a las directivas de la Universidad mantener una visión general del estado de los sistemas informáticos, plantear estrategias de cambio y mejora de los mismos, verificar las medidas de seguridad aplicadas y los resultados obtenidos, valorar y asegurar sus activos de posibles riesgos y vulnerabilidades presentes, permitiendo la toma de decisiones de manera consecuente, argumentada y documentada, involucrando a todo el personal en un proceso global que le proporcionara la mejora continua.

Guevara (2017), desarrollo un estudio con la denominación: Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01 de educación, desarrollado en la Universidad Técnica De Ambato, Cuyo objetivo es Implementar un Sistema de Gestión de Seguridad de la Información bajo parámetros de las normas ISO/IEC 27001, para el mejoramiento de la seguridad de la información en el Distrito 18D01 de Educación, llego a concluir: El Distrito 18D01 de Educación no cuenta actualmente con procedimientos relacionados a la salvaguardia de la información. Los diferentes procesos que se llevan a cabo no se los realiza en base a políticas establecidas, únicamente se aplican ciertas normativas para gestionar la

información las cuales no son suficientes para garantizar que la información esté asegurada. Al no contar con un sistema preventivo para gestionar adecuadamente la información, todas las acciones que emprende la institución en lo referente a la seguridad de la misma son de carácter correctivo lo cual genera un desperdicio de recursos para el Distrito de Educación.

Moscoso (2017), en Cuenca Ecuador, hizo una tesis titulada: Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos. Se estudió al departamento de producción de una empresa industrial de Alimentos. Su objetivo de investigación fue el planteamiento de una metodología de manera clara y detallada con el fin de elaborar y difundir las políticas de seguridad de la información más adecuadas. Se estudió a las empresas de la industria de alimentos. Asimismo, se emplearon diferentes metodologías y estándares como la ISO/IEC 27002 de seguridad de la información. Finalmente, los resultados obtenidos es el planteamiento de un método apropiado, que consiste de 3 etapas y un total de 9 pasos propuestos para la identificación, análisis y evaluación de riesgos y la elaboración formal de las políticas de seguridad de la información que los mitiguen. El método está diseñado para ser aplicado en empresas industriales de alimentos, pero no se descarta que pueda ser aplicado también en otro tipo de empresas, con su respectiva validación La aplicación práctica de cada una de estas etapas, y su evaluación mediante el análisis de los resultados obtenidos en ellas, se realizó en una empresa industrial de alimentos aplicando la metodología planteada, donde se encontraron un total de 30 riesgos que fueron valorados en base a su probabilidad de ocurrencia y sus consecuencias que afectan a la disponibilidad, integridad o confidencialidad de la información. Además, aplicando la metodología planteada se obtuvieron 13 dominios, 30 categorías de control y 88 controles

seleccionados de la norma ISO/IEC 27002 en su versión 2013, para mitigar los riesgos identificados y se plasmaron estos controles formalmente en un documento en forma de políticas de seguridad de la información, siendo este el entregable final del presente trabajo de investigación para la empresa en la que se realizó el caso de estudio.

Ámbito nacional

Gavidia y Torres (2018), en Lima Perú, hizo una tesis titulada: Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte. Su objetivo de investigación fue Implementar los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte. Se estudió a nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte, por lo cual no se trabajó con muestra ya que utilizaron el 100 % del área. Asimismo, Durante la etapa de auditoria se realizaron dos evaluaciones para medir el nivel de la seguridad de la información en el área de TI de la Unión Peruana del Norte, donde se permite conocer al detalle cómo se cumplieron los criterios de evaluación del PAM de Cobit. Finalmente, los resultados obtenidos se midieron las variables de estudio donde se concluye que: La implementación de los controles de la ISO/IEC 27002:2013 mejoró significativamente el nivel de seguridad de la información, puesto que durante la primera evaluación se obtuvo un resultado inicial de 47% y en la segunda evaluación ya con los controles implementados se obtuvo un resultado de 84%. Donde concluyó que la diferencia encontrada entre ambos resultados, mejoró en un 37% de la seguridad física y lógica de la información.

Cortéz y Santiago (2018), en su estudio desarrollado: Plan de seguridad informática basado en la Norma ISO 27002 para mejorar la gestión tecnológica del Colegio

Carmelitas – Trujillo, desarrollado en la Universidad Nacional de Trujillo, quien llego a concluir: Se controló los accesos a los recursos informáticos de la institución para aumentar la disponibilidad de la información. Las políticas de cifrado se definieron para aumentar la integridad de la información. La seguridad física y ambiental se estableció en todo el departamento para aumentar la integridad de la información. La seguridad se estableció en las operaciones comerciales para aumentar la confidencialidad de la información. La seguridad de las telecomunicaciones se estableció para aumentar la confidencialidad de la información.

Mercado (2016), quien desarrollo un estudio denominado: Modelo de gestión de seguridad de la información para el E-Gobierno, desarrollado en la Universidad Nacional Mayor De San Marcos, quien llego a demostrar: Se elaboró un modelo de gestión de seguridad de la información para el gobierno electrónico resultado de la revisión y análisis de 11 modelos de seguridad de la información, en los que se identificaron los elementos más relevantes que forman parte del modelo propuesto. Se ha definido una estructura organizacional con funciones definidas que contempla los procesos estratégicos, fundamentales y de soporte, la cual permite gestionar la seguridad de la información y garantizar una mejor experiencia al cliente cuando requiera interactuar con los procesos o servicios de la organización. Se han identificado 05 niveles de madurez para la implementación y operación del modelo de seguridad de la información en los procesos que brindan servicio de gobierno electrónico, permitiendo la gestión de la seguridad en dichos procesos y conocer el nivel de seguridad con que se cuenta.

Ámbito local

Referente a los antecedentes locales no se registraron trabajos similares en los diferentes repositorios de las universidades locales.

2.2. Bases teóricas

Para deducir los problemas o riesgos ante la seguridad de la Información que tiene una institución se necesita tener la capacidad para determinar las acciones y procesos que realiza, es importante entender términos y definiciones que son fundamentales y que a lo largo de la investigación serán citados. Las definiciones serán el soporte de ayuda para otorgar un resultado viable a la problemática identificada. Los términos claves dentro del proyecto de investigación son:

- ✓ Controles de la Norma ISO/IEC 27002:2013.
- ✓ Mejora del nivel de seguridad física y lógica de la información.
- ✓ Base de datos de la SUNARP Zona Registral N° VII- Sede Huaraz.

A continuación, se detalla los términos o conceptos que están contenidos dentro de ellos, y que son importantes para el análisis y alcance del problema.

Controles de la Norma ISO/IEC 27002:2013.

A. Seguridad de la Información.

Según Parra (2017), la información es un medio o recurso que al igual que el resto de los activos, posee un valor importante para toda organización, por lo cual tendría que ser debidamente protegida.

La seguridad de la información la resguarda de diversas amenazas, con el propósito de asegurar la continuidad del negocio, reducir el daño al mismo y reducir el retorno sobre las oportunidades e inversiones.

Córdova J. (2012) menciona que la seguridad de la información cuenta con tres soportes importantes: la integridad, confidencialidad y disponibilidad de la información.

Confidencialidad: Según Caccuri (2012), “debe tener la capacidad de proteger la información ante el intento de acceso de divulgación a otros usuarios no

autorizados. Consiste en asegurar la privacidad de los datos. Solamente los individuos, procesos o dispositivos autorizados pueden acceder a ellos".

Integridad: Según Caccuri (2012), "la información debe estar completa y no ser alterada o modificada sin autorización. La integridad se refiere a la protección de la información de acciones tanto deliberadas como accidentales".

Disponibilidad: Según Pacheco & Jara (2010), "la disponibilidad garantiza que los recursos del sistema y la información estén disponibles solo para usuarios autorizados en el momento que los necesiten."

(***Fuente:*** infosegur)

Figura 1. Propiedades fundamentales de la seguridad

- Requerimientos de seguridad de la información.

  Según Project Management Consultores de Proyectos (2006), existen tres fuentes primordiales para los requerimientos en referencia a la seguridad de la información. La primera fuente deriva de hacer una evaluación de riesgo para la organización, al tener en cuenta los objetivos y estrategia de negocio. A través de esta evaluación de riesgos se identifican las amenazas pertenecientes a los activos, se evalúa su vulnerabilidad y su probabilidad de ocurrencia y se estima o calcula su impacto potencial. La segunda fuente son los requerimientos reguladores, requerimientos legales, requerimientos contractuales y requerimientos estatutarios que se ven en la necesidad de

complacer a una organización, a los contratistas, a sus socios comerciales y proveedores de servicio y su entorno socio-cultural.

La tercera fuente es con los objetivos, conjunto particular de principios y los requerimientos comerciales para el desarrollo de la información que una organización ha procesado para mantener sus operaciones.

- .Entidades implicadas en la seguridad de la información.

  Según Godoy (2011), las actividades de seguridad deben ser tomadas en cuenta por todo el personal relacionado con los sistemas de información, como son:

  - Desarrolladores de software y Fabricantes de productos.
  - Integradores de datos en el sistema.
  - Compradores, que pueden ser organizaciones o usuarios finales.
  - Organizaciones de evaluación de la seguridad, como certificadores de sistemas, evaluadores de productos o acreditadores de operación.
  - Administradores de sistemas y de seguridad.
  - Terceras partes confiables (TTP), como son las autoridades de certificación, fedatarios electrónicos con servicios de firma electrónica avanzada y sellado temporal.
  - Consultores u organizaciones de servicios, por ejemplo, servicios de externalización u outsourcing de la gestión de la seguridad.

B. Norma ISO/IEC 27002:2013.

La ISO 27002 es una guía de recomendaciones de buenas prácticas para la gestión de la información. Otorga directrices a las normas de seguridad de la información en las prácticas de seguridad de la información y en las organizaciones, abarcando la selección, implementación y la administración de controles considerando el contexto de seguridad de la información de la organización.

Para Perú se tiene la NTP-ISO/IEC 1799, y según ISOTools Excellence (2015), “Ofrece todas las recomendaciones para poder gestionar un Sistema de Seguridad de la información (SSI), al igual que la norma internacional ISO 27001, ofrece los requisitos necesarios para que los responsables del área en concreto puedan iniciar, implantar, mantener y mejorar la seguridad en las organizaciones.”. Aparte de ello se tiene NTP-ISO/IEC 27002:2017 para la seguridad de la información.

La ISO 27002 es de suma importancia para el desarrollo en la mejora del nivel de seguridad de la información, puesto que establece los controles a seguir para certificar la disponibilidad, confidencialidad e integridad de la información.

- Historia de la Norma ISO/IEC 27002.

  Prada (2009) menciona que esta norma nace como evolución histórica de la norma británica BS 7799, ya en el 2000 se le conoce como ISO/IEC 17999 y en el año 2005 pasa a llamarse ISO/27002 para formar parte de la familia de la ISO 27000.

- Contenido de la Norma ISO/IEC 27002:2013.

  Gutiérrez (2013) señala que en esta versión nueva de la norma se hallan los controles que intentan disminuir la posibilidad de ocurrencia y/o el impacto de los variados riesgos al cual se encuentra expuesta una organización.

  Manjón (2015) menciona que con el reajuste de En este estándar, las organizaciones pueden encontrar una guía útil para implementar controles de seguridad en una organización y sobre los métodos más efectivos para administrar la seguridad de la información.

  La norma ISO/IEC 27002:2013 contiene 15 dominios, 35 objetivos de control y 115 controles. La Tabla 1 muestra los dominios respectivos para ISO 27002: 2013 con objetivos de control respectivos y cantidades de control.

Tabla 3

Dominios – Objetivos de Control y Controles ISO 27002:2013

1	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	1.1 DIRECTRICES DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	2
2	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	2.1 ORGANIZACIÓN INTERNA. 2.2 DISPOSITIVOS PARA MOVILIDAD Y TELETRABAJO	5 2
3	SEGURIDAD RELATIVA A LOS RECURSOS RUMANOS	3.1 ANTES DEL EMPLEO 3.2 DURANTE EL EMPLEO 3.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO	2 3 1
4	GESTIÓN DE ACTIVOS	4.1 RESPONSABILIDAD SOBRE LOS ACTIVOS 4.2 CLASIFICACIÓN DE LA INFORMACIÓN 4.3 MANIPULACIÓN DE LOS SOPORTES	4 3 3
5	CONTROL DE ACCESO	5.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS 5.2 GESTIÓN DE ACCESO DE USUARIO 5.3 RESPONSABILIDADES DEL USUARIO 5.4 CONTROL DE ACCESO A SISTEMAS Y	2 6 1 5
6	CRIPTOGRAFÍA	6.1 CONTROLES CRIPTOGRÁFICOS	2
7	SEGURIDAD FÍSICA Y DEL ENTORNO	7.1 ÁREAS SEGURAS 7.2 SEGURIDAD DE LOS EQUIPOS	6 9
8	SEGURIDAD DE LAS OPERACIONES	8.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES 8.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE) 8.3 COPIAS DE SEGURIDAD 8.4 REGISTROS Y SUPERVISIÓN 8.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN 8.6 GESTIÓN DE LA VULNERABILIDAD	4 1 1 4 1 2 1
9	SEGURIDAD DE LAS COMUNICACIONES	9.1 GESTIÓN DE LA SEGURIDAD DE REDES 9.2 INTERCAMBIO DE INFORMACIÓN	3 4
10	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	10.1 REQUISITOS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN 10.2 SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE	3 9 1
11	RELACIÓN CON PROVEEDORES	11.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES 11.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR	3 2
12	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	12.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS	7
13	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	13.1 CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN 13.2 REDUNDANCIAS	3 1
14	CUMPLIMIENTO	14.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES 14.2 REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	5 3

Fuente: Enunciado adoptado de la Norma ISO 27002:2013 (AENOR, (2015))

- Dominios de control.

  En la Figura 2 se observa los dominios de control la Norma ISO 27002:2013 enmarcados dentro de 4 vertientes tales como: seguridad organizativa, seguridad física, seguridad lógica y seguridad legal; y bajo tres niveles: operacional, estratégico y táctico.

(Fuente: https://es.slideshare.net/Tensor/iso-27001-iso-27002)

Figura 2. Dominios de control de la ISO 27002.

- Selección de controles.

  Según AENOR (2015), la selección de controles a depender de las determinaciones de carácter organizativo basadas sobre los criterios de aceptación de riesgo, elecciones de tratamiento de riesgo y de los enfoques generales de gestión de riesgo adaptado en la organización. También tendría que depender, de toda la legislación internacional y nacional aplicable. La selección de controles dependerá igualmente del modo en que los controles interactúen para brindar una protección en profundidad.

  Dentro de esta norma algunos controles pueden considerarse como principios o normas que dirigen la gestión de la seguridad de la información, siendo así aplicables en la mayoría de las organizaciones.

- Seguridad física.

  La seguridad física es importante para toda organización, puesto que se necesita proteger el acceso físico a las áreas de información, esta deducción entiende que ante cualquier eventualidad que perjudique a la información, se tenga que prever un mejor análisis de seguridad. Ante ello, la falta de análisis en las áreas de información sobre seguridad física, algunas empresas pierden credibilidad y presupuesto que no se encontraba como inversión, por ello se recomienda concientizar a las empresas sobre la importancia de la seguridad física.

  Para cumplir con la necesidad que algunas empresas desconocen sobre la seguridad física, la norma ISO/IEC 27002:2013 establece controles de seguridad físicos, que indica que parámetros cumplir, para la protección segura sobre los equipos que se encuentran en el área de información, permitiendo restricciones sobre el acceso a ellos.

  A continuación, de la Tabla 2 a la Tabla 4, se muestran los controles de seguridad física seleccionados para la implementación. Los controles fueron seleccionados durante la elaboración del Plan de Tratamiento de Riesgo y mediante el proceso DSS05 – “Gestionar los servicios de Seguridad" de COBIT. A esto se les considero algunos de los controles de los dominios 5 y 8 tanto para la seguridad física como para la lógica.

- Seguridad lógica

  La seguridad lógica va de la mano con la seguridad física, porque es sumamente importante para la seguridad de la información. Ante ello, se requiere que la seguridad lógica, proteja a la información durante su tránsito

en la red de la organización. Algunas organizaciones no tienen segura a la información, porque no toman conciencia sobre los daños o pérdidas que podría ocasionar si se infecta o pierde la información, se debe tomar medidas que en conjunto con la seguridad física para que protejan la información de la organización.

La norma ISO/IEC 27002:2013 contiene controles que están asociados a la seguridad lógica, es por ello que te indica cuáles son los parámetros que requiere para que la información se encuentre confiable y segura cuando esta llegue a su destinatario.

- Norma ISO 27005

Concepto.

Según Baca (2016), “La ISO 27005 establece las directrices para la gestión del riesgo en la seguridad de la información, además de que también apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos”.

Hasta el momento, el marco que existe para la gestión de riesgos lo conforma el estándar ISO 27005. Se puede utilizar diferentes metodologías que existen bajo la estructura descrita. Este estándar para implementarlos requiere un sistema de gestión de seguridad de la información.

Esta regla es aplicable a todos los miembros de la junta y al personal relacionado con la gestión de riesgos en seguridad de la información dentro de una organización y, cuando corresponda, a las partes externas que respaldan tales operaciones.

Objeto y campo de aplicación.

- Esta norma proporciona criterios para la gestión en la seguridad de la información.
- Esta norma brinda soporte a los distintos conceptos que se especifican en la norma ISO 27001.
- Esta norma está diseñada para proporcionar la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión de riesgo.
- Todos los conceptos que se mencione en las normas ISO/IEC 27001 e ISO/IEC 27002 es importante para su comprensión de esta norma.
- Esta norma se puede emplear a diferentes tipos de organizaciones que exista en todo el mundo como (empresas pequeñas, agencias del gobierno, empresas sin ánimo de lucro).

- Análisis de riesgo.

Según Moreno (2008), el análisis de riesgo es la herramienta que ayuda a identificar a las amenazas y vulnerabilidades que se encuentran en los activos de información, teniendo una valoración por riesgo minimizando, el impacto que podría ocasionar en la organización. La Figura 8 se puede apreciar la secuencia de pasos para realizar el análisis de riesgo que describe la norma.

(Fuente: Samuel G y Luis T. (2018))

Figura 3. Análisis de riesgo

- Identificación de activos.

  Un activo es aquel que tiene un valor importante para la organización, por ello se necesita protegerlo ante cualquier amenaza que pueda surgir.

  La identificación del activo consta de un análisis detallado que permite tener la información exacta de cada activo encontrado en la organización, este análisis contiene el tipo de activo, el propietario que está a cargo del activo y la localización donde se encuentra el activo, logrando tener la responsabilidad necesaria para el desarrollo, mantenimiento, uso y seguridad según corresponda al análisis que se realice.

- Identificación de amenazas.

  - La amenaza tiene la capacidad de perjudicar y/o eliminar a los activos que se encuentran dentro de la organización. Las amenazas suelen ser de tipo natural o humano y podría ser accidental o deliberada.

- Identificación de vulnerabilidades.

- La vulnerabilidad que no tiene una amenaza, puede que no necesariamente tenga que recurrir a la implementación de los controles, pero se recomienda que se analice y se monitoree para ver los cambios que tuvo.
- Una vulnerabilidad también se relaciona con los activos de la organización para así determinar cuáles son los riesgos que necesita ser reducido. Se puede identificar vulnerabilidades en las siguientes áreas.

C. Plan de tratamiento de riesgo.

El plan de tratamiento de riesgo, es la parte más compleja, la cual la organización debe conocer, porque estipula el tiempo que se desarrollará, y que controles de la norma ISO/IEC 27002:2013 implementar, es importante tener conocimiento del plan porque permite controlar el cumplimiento de los controles.

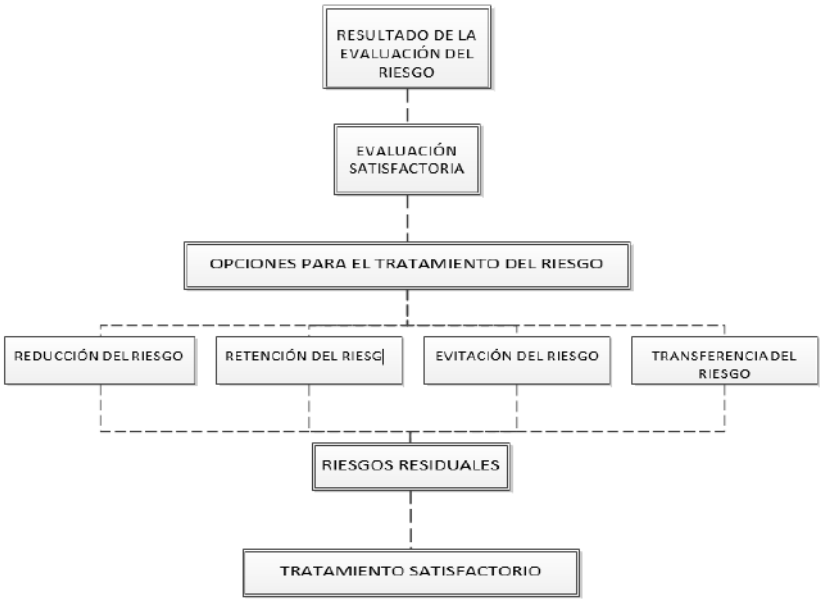
Las organizaciones deben estipular su plan de tratamiento de riesgo para conocer los factores principales que permitan minimizar los riesgos que se encuentran en cualquier entidad organizativa.

- Tratamiento del riesgo en la seguridad de la información.

Descripción del tratamiento de riesgo.

- Para el tratamiento del riesgo se necesita tener una lista de los riesgos priorizados para analizar su valor por cada riesgo (sea el impacto o el costo del riesgo), estableciendo un plan de tratamiento del riesgo para su reducción.
- Para el tratamiento de riesgo existen 4 opciones las cuales son: aceptación del riesgo, reducción del riesgo, transferencia del riesgo y evitación del riesgo.

- En algunos casos un tratamiento de riesgo puede tratar eficazmente más de un riesgo.
- En el caso de que en el análisis del tratamiento de riesgo se indica las opciones transferir, evadir y aceptar es recomendable no colocar los controles de la norma, solo en el caso que la opción sea reducir se implementa los controles que la norma menciona. En la Figura 4 se grafica las actividades que se deben optar para el tratamiento del riesgo, tal como lo describe la norma.



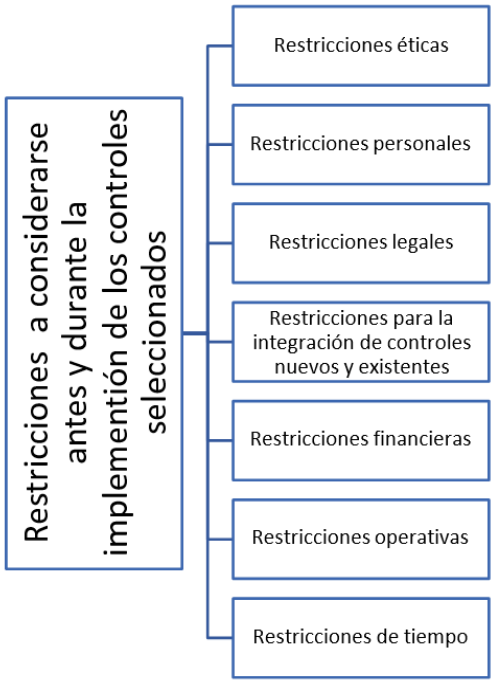
(Fuente: Moreno (2008))

Figura 4. Actividad para el tratamiento del riesgo

Reducción del riesgo.

- Es necesario seleccionar los controles justificados y adecuados, que cumplan con los requisitos identificados en el tratamiento del riesgo.
- También se debe considerar el marco temporal y el costo de ello para la implementación de los controles.

- Los controles pueden ofrecer uno o más tipos de protección: detección, prevención, minimizar el impacto, corrección, eliminación, concienciación y recuperación.
- Es necesario considerar varias restricciones cuando se selecciona los controles antes y durante la implementación.
- Por lo tanto, se consideran lo siguientes restricciones, tal como se muestra en la Figura 5.



(Fuente: Moreno (2008))

Figura 5. Restricciones a considerarse antes y durante la implementación de los controles seleccionados.

Aceptación del riesgo

- Se toma la decisión de aceptar el riesgo, dependiendo de la evaluación del riesgo.

- Cuando el nivel del riesgo satisface los criterios para su aceptación no se implementa los controles identificados y el riesgo se puede retener

Evitación del riesgo.

- Es cuando los riesgos son costosos y se consideran altos para la organización, se toma una decisión de evitar por completo el riesgo, mediante el retiro de una actividad.

Transferencia del riesgo.

- Se debe transferir a otra empresa que lo trabaje de manera eficaz y eficiente el riesgo que se encontró en la evaluación.
- La trasferencia del riesgo implica una decisión para compartirlo con las partes externas.
- La transferencia se realiza a través de un seguro que respaldará las consecuencias o mediante una subcontratación de una empresa asociada cuya función es monitorear el sistema de información y tomar medidas rápidas para detener el ataque.

2.3. Definición de términos básicos

En el desarrollo del estudio no se consideran la definición de términos básicos, debido a que toda la fundamentación teórica se encuentra en el desarrollo del marco teórico y los antecedentes tomados para el desarrollo del estudio.

Es importante mencionar que para el desarrollo se estudió se tomó en cuenta la fundamentación de las teorías que más se relacionan con las variables que se encuentran analizando, partiendo de un análisis preliminar para diagnosticas como se encuentra en la actualidad y plantear un plan de mejora que ayude a fortalecer los procedimientos establecidos.

Capítulo III:

3. DISEÑO METODOLÓGICO

3.1. Tipo de investigación

El estudio se considera de tipo aplicada, según Hernández, Fernández, y Baptista (2014), los estudio de tipo aplicada se basan en utilizar fuentes teóricas existentes para dar fundamento al estudio y proporcionar alternativas de solución que beneficie al desarrollo establecido.

Al mismo tiempo se considera cuantitativo, basado en utilizar resultados de tipo numérico o estadísticos para proporcionar resultados para los objetivos establecidos en el desarrollo del estudio.

3.2. Diseño de investigación

Se considera un diseño experimental – Pre experimental, según Valderrama (2012), los estudio pre experimental se basan en la intervención y manipulación de la variable

independiente para ver el efecto que tendrá en la variable dependiente, analizando este proceso en dos momentos antes y después d aplicar. También es Pre experimental porque se cuenta con un solo grupo de trabajadores que conforman el grupo experimental.

Según el alcance temporal que presenta se considera longitudinal, porque el análisis de la información se realiza en dos tiempos, antes de después de aplicar a la variable independiente, además de ello se tiene que el estudio es relevante porque permitió determinar el efecto que tendrá sobre la variable dependiente.

3.3. Población y muestra de la investigación

La población está representada por 12 trabajadores del área de informática, según Hernández, Fernández y Baptista (2014), la población es considerada como el total de sujetos que integran un estudio y cuentan con los conocimientos necesarios para conformar la muestra de estudio. También los autores mencionan que cuando la población es de una cantidad pequeña se puede tomar como muestra al total de la población, denominándoles población censal.

La muestra en el desarrollo del estudio se tomó al total de personas que integran la población, por ser un número manejable para el investigador, extrayéndola mediante el muestreo no probabilístico a criterio del investigador.

3.4. Técnicas para la recolección de datos

Para el desarrollo del estudio, se consideró la técnica de la encuesta, definida por Hernández, Fernández y Baptista (2014), como las acciones que se realizan en el proceso de investigación con la finalidad de obtener datos, que conlleven al análisis de información y que puedan ayudar a responder los objetivos de investigación.

3.4.1. Descripción de los instrumentos

El instrumento que se utilizó fue el cuestionario, considerada por Hernández, Fernández y Baptista (2014), como un medio físico, tangible con el que tienen contacto los trabajadores de la Sunarp y pueden brindar sus opiniones para ser utilizadas en la obtención de resultados que fundamenten a los objetivos establecidos en la investigación.

3.4.2 Validez y confiabilidad de los instrumentos

Validez, para el desarrollo de la validez del instrumento se tiene en cuenta al juicio de expertos, quienes determinan la consistencia interna del instrumento, evaluando la correcta redacción y los lineamientos que tenga con los indicadores, dimensiones y variables, además se tiene en consideración, que tienen que ser profesionales de la línea y que presenten experiencia en el tema de desarrollo.

Confiabilidad, para desarrollar este proceso se tiene en consideración, la realización de una prueba piloto conformada por 12 personas que no forman parte de la muestra, pero presentan características similares, también es importante mencionar que esta prueba sirve de fundamento para proporcionar la viabilidad del instrumento y certeza que el instrumento está bien realizado.

3.4.3. Técnicas para el procesamiento y análisis de los datos

La técnica que se aplicó en el desarrollo del estudio para procesar los datos es el método inductivo, partiendo de establecer objetivos y hipótesis, comprobada con el análisis de resultados, luego se tiene que diseñar la base de datos, ordenarlas por dimensiones y variable, para obtener las tablas de frecuencia y figuras de barra, que permitan responder a los objetivos establecidos para el desarrollo del estudio.

Capítulo IV

4. PRESENTACIÓN DE RESULTADOS

4.1. Presentación e interpretación de resultados en tablas y figuras

Por ser una investigación pre experimental, no presenta análisis de tablas cruzadas y de correlación, más bien se basa en el análisis de los resultados plasmados en tablas de frecuencia a través del análisis descriptivo para realizar la comparación del antes y después que se implemente el plan de mejora relacionado a los controles de la ISO/IEC 27002:2013, para el desarrollo de la prueba de normalidad si se realizó, puesto que los resultados tiene que determinar el método inferencia que se utilizó en el desarrollo del estudio con la finalidad de realizar la comprobación de la hipótesis del estudio.

Por otro lado, se realiza un análisis de cómo se implementó el plan de mejora y los efectos que presento en la gestión de la base de datos de la institución, además de ello se tiene considerado un tiempo que determino la efectividad de la implementación.

4.1.1. Resultados descriptivos por variable y dimensiones

Tabla 4.

Frecuencia el impacto de implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

Criterio	Gestión de la base de datos					
	PRE		POST		MEJORA	
	f_i	%	f_i	%	f_i	%
Deficiente	11	91.7%	0	0.0%	11	91.7%
Regular	1	8.3%	1	8.3%	0	0.0%
Eficiente	0	0.0%	11	91.7%	11	91.7%
Total	**12**	**100.0%**	**12**	**100.0%**		

Fuente: Base de datos de los encuestados

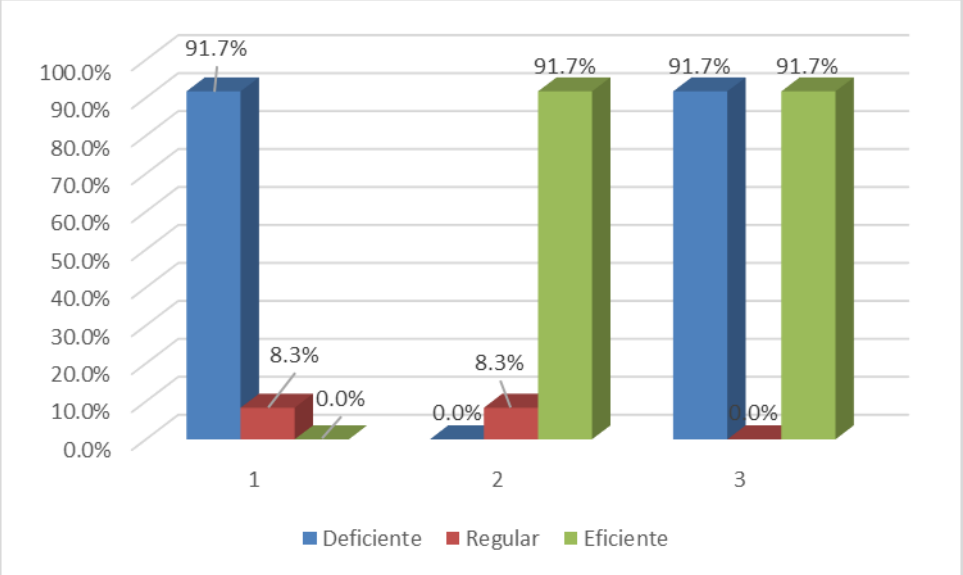


Figura 6. Barra del impacto de implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

Interpretación:

A partir de los resultados plasmados se puede mencionar que en el pre test se tiene que 11 trabajadores que conforman el 91.7% lo consideran como deficiente, mientras que en el pos test se tiene que ninguna persona lo considera como deficiente, obteniendo una mejora de 11 trabajadores que integran el 91.7 %. Por otro lado, se tiene que e1 trabajador que integra el 8.3 % lo considera como regular, mientras que e1 trabajador lo considera como regular, durante este proceso n ose relevo mejoras significativas. Para el desarrollo del estudio se tiene que en el desarrollo del pre test nadie considera que es eficiente, mientras que en el pos test pasa todo lo contrario que 11 trabajadores que conforman el 91.7 % lo considera como eficiente, teniendo una efectividad considerable del estudio con un valor de 91.7 %.

Tabla 5.

Frecuencia de la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013.

Criterio	PRE - TEST									
	DIMENSIONES								VARIABLE	
	Disponibilidad de la Base de Datos		Escalabilidad de la base de datos		Accesibilidad de consulta y escritura		Respaldo y copias de seguridad		Gestión de la base de datos	
	f_i	%	f_i	%	f_i	%	f_i	%	f_i	%
Deficiente	8	66.7%	10	83.3%	8	66.7%	8	66.7%	11	91.7%
Regular	4	33.3%	2	16.7%	4	33.3%	4	33.3%	1	8.3%
Eficiente	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
	12	**100.0%**	**12**	**100.0%**	**12**	**100.0%**	**12**	**100.0%**	**12**	**100.0%**

Fuente: Base de datos de los encuestados

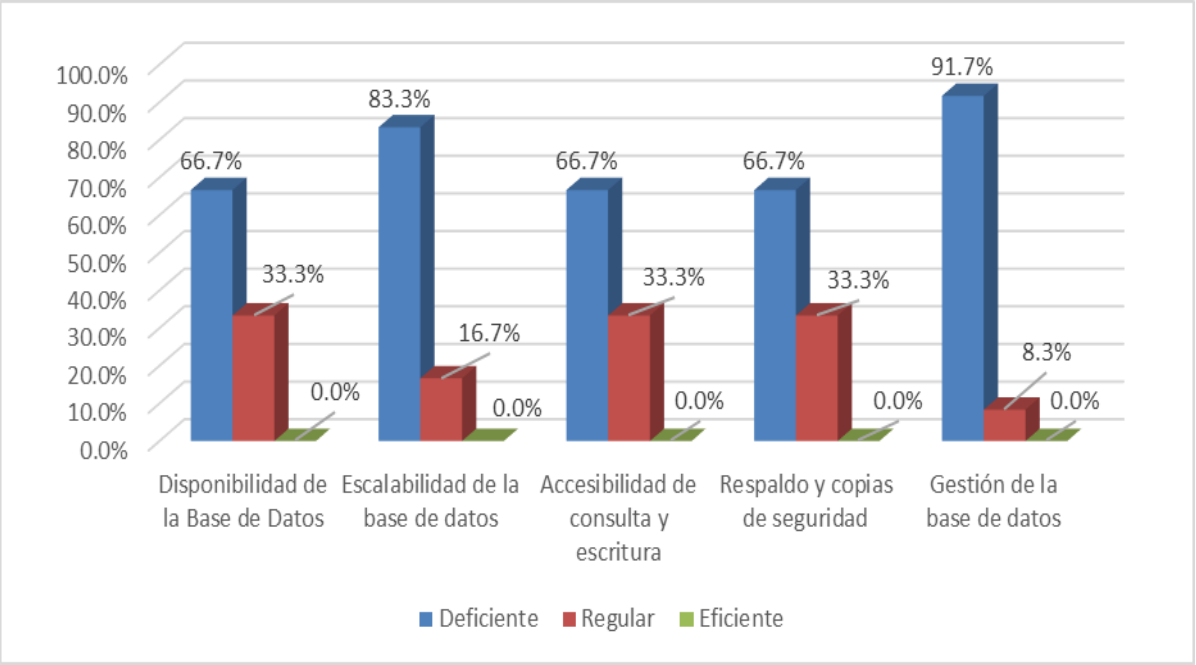


Figura 7. Barra de la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013.

Interpretación:

A partir de los resultados presentados en la tabla y la figura se puede mencionar que la dimensión disponibilidad de la base de datos se tiene que 8 trabajadores que integran el 66.7 % lo consideran como deficiente, seguido de 4 trabajadores que conforman el 33.3 % lo analizan como regular y finalmente se tiene que ningún trabajador lo considera como eficiente. Respecto a la dimensión escalabilidad de la base de datos se tiene que 10 trabajadores que conforman el 83.3 % lo analizan como deficiente, mientras que 2 trabajadores que conforman el 16.7 % lo interpretan como regular, finalmente se tiene que ningún trabajador lo considera como eficiente. Al mencionar a la dimensión accesibilidad de consulta y escritura se tiene que 8 trabajadores que conforman el 66.7 % lo analizan como deficiente, mientras que 4 trabajadores que integran el 33.3 % lo consideran como regular y ningún trabajador lo considera como eficiente. Por otro lado, se tiene que 8 trabajadores que

conforman el 66.7 % lo analizan como deficiente, mientras que 4 trabajadores que conforman el 33.3 5 lo consideran como regular, finalmente se tiene que ningún trabajador lo considera como eficiente. Por último respecto a la variable gestión de la base de datos, se tiene que 11 trabajadores que integran el 91.7 % lo consideran como deficiente, mientras que 1 trabajador que conforma el 8.3 % lo interpreta como regular y finalmente ningún trabajador lo considera como eficiente.

Respecto al objetivo diseñar los controles de la ISO/IEC 27002:2013 para la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

Figura 8. Ciclo de vida del diseño de los controles de la ISO/IEC 27002:2013 para la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.

Interpretación:

Referente a la proyección de la implementación se tiene que el diagnostico de los requerimientos y de la detección de la problemática se realizó durante el mes de julio, luego de eso se tiene que el diseño, desarrollo y la implementación, se desarrolló durante los meses de agosto y septiembre, que tuvo un tiempo de vida que demostró la efectividad, luego de ello se tiene la fase evaluativa que se desarrolló durante el mes de octubre, con la finalidad de analizar el grado de efectividad que demostró los controles de la ISO/IEC 27002:2013.

Tabla 6.

Frecuencia de la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013.

Criterio	PRE - TEST									
	DIMENSIONES								VARIABLE	
	Disponibilidad de la Base de Datos		Escalabilidad de la base de datos		Accesibilidad de consulta y escritura		Respaldo y copias de seguridad		Gestión de la base de datos	
	f_i	%	f_i	%	f_i	%	f_i	%	f_i	%
Deficiente	0	0.0%	0	0.0%	0	0.0%	0	0.0%	0	0.0%
Regular	1	8.3%	1	8.3%	4	33.3%	6	50.0%	1	8.3%
Eficiente	11	91.7%	11	91.7%	8	66.7%	6	50.0%	11	91.7%
	12	**100.0%**	**12**	**100.0%**	**12**	**100.0%**	**12**	**100.0%**	**12**	**100.0%**

Fuente: Base de datos de los encuestados

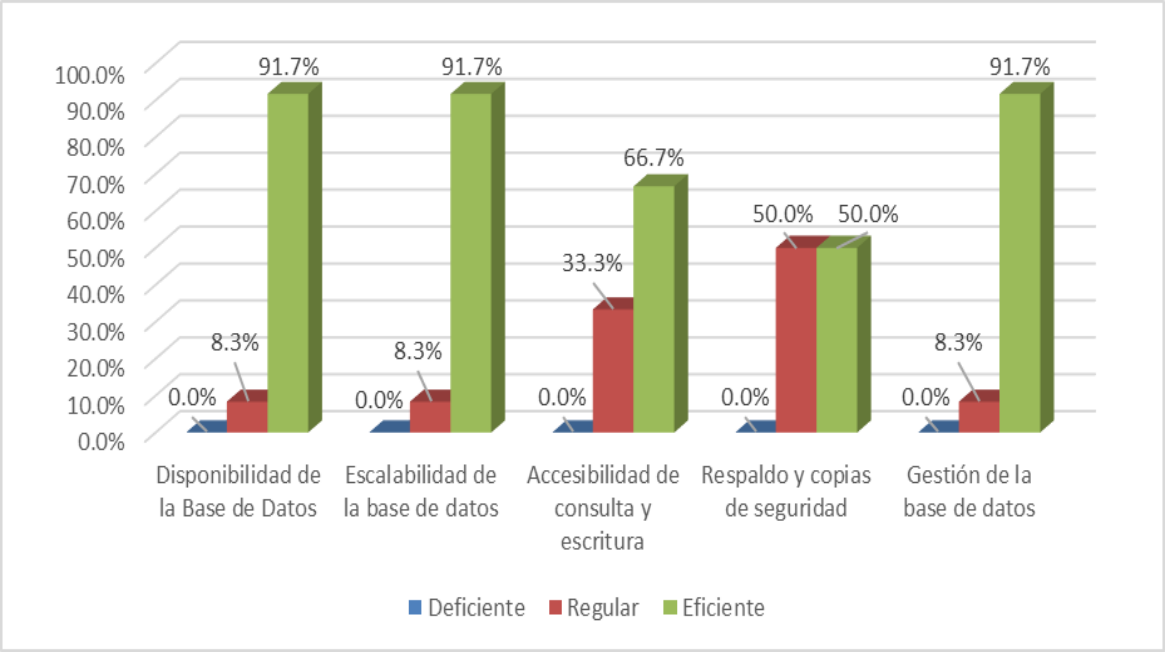


Figura 9. Frecuencia de la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013.

Interpretación:

Con los resultados presentados se tiene que la dimensión disponibilidad de la base de datos presenta que ningún trabajador lo considera como deficiente, mientras que 1 trabajador que conforma el 8.3 % lo considera como regular y 11 trabajadores que conforman el 91.7 % lo analizan como eficiente, mientras que respecto a la dimensión escalabilidad de la base de datos se tiene que ningún trabajador lo considera como deficiente, mientras que 1 trabajador que representa el 8.3 % lo considera como regular y finalmente se tiene que 11 trabajadores que conforman el 91.7 % lo analizan como eficiente, respecto a la dimensión accesibilidad de consulta y escritura se tiene que ningún trabajador lo considera deficiente, mientras que 4 trabajadores que conforman el 33.3 % lo interpretan como regular y 8 trabajadores que conforman el 66.7 % lo considera como eficiente. Respecto a la dimensión respaldo y copias de seguridad se tiene que ningún trabajador lo considera como deficiente, mientras que 6 trabajadores que conforman el 50.0 % lo analizan como regular y finalmente se tiene que 6 trabajadores que conforman el 50.0 % lo consideran como eficiente. Finalmente, cuando se menciona a la gestión de la base de datos se tiene que ningún trabajador lo considera como deficiente, mientras que 1 trabajador que conforma el 8.3 % lo considera como regular y 11 trabajadores que integran el 91.7 % lo consideran como eficiente. A partir de los datos presentados luego de haber aplicado los controles de la ISO/IEC 27002:2013, se demuestra la efectividad que presento en el desarrollo del estudio y lo favorable que puede ser aplicarlo a otras entidades públicas y privadas del país.

Respecto al objetivo: Comparar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Tabla 7.

Frecuencia de la disponibilidad de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Criterio	Disponibilidad de la Base de Datos					
	PRE		POST		MEJORA	
	f_i	%	f_i	%	f_i	%
Deficiente	8	66.7%	0	0.0%	8	66.7%
Regular	4	33.3%	1	8.3%	3	25.0%
Eficiente	0	0.0%	11	91.7%	11	91.7%
Total	**12**	**100.0%**	**12**	**100.0%**		

Fuente: Base de datos de los encuestados

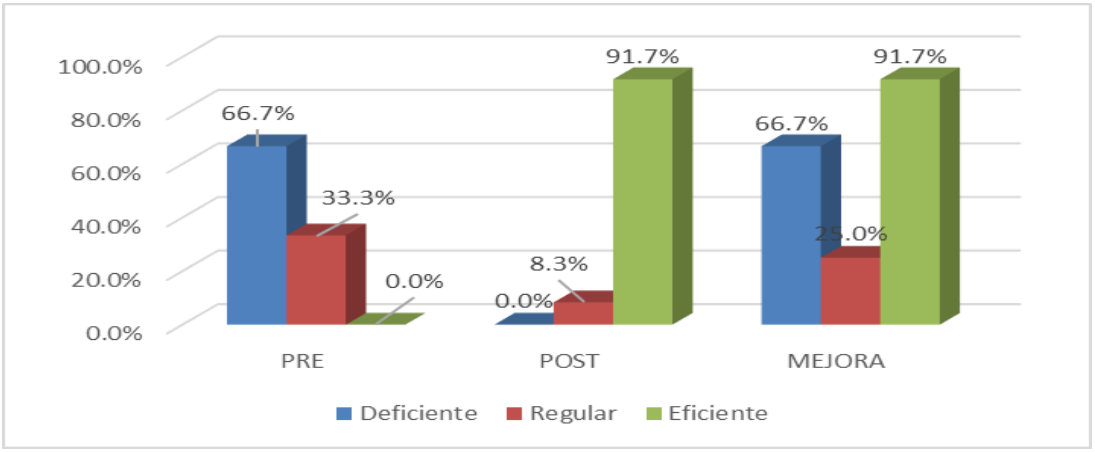


Figura 10. Barra de la disponibilidad de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Interpretación:

A partir de los datos mostrados en la tabla y la figura se puede encontrar que la dimensión de la base de datos, en el pre test se tiene que 8 trabajadores que conforman el 66.7 % lo interpretan como deficiente, mientras que en el pos test se tiene que ningún trabajador lo considera como deficiente, mostrando una mejora de 8 trabajadores, que representan el 66.7 %, respecto al nivel regular se presentó que en el pre test se tiene que 4 trabajadores que conforman el 33.3 % lo analizan como regular, por otro lado en el pos test se tiene que 1 trabajador que conforma el 8.3 % lo analiza como regular, mostrando una efectividad de 3 trabajadores que representan el 25.0 %, respecto al nivel eficiente se tiene que en el pre test se obtuvo que ningún trabajador lo considero como eficiente, mientras que en el desarrollo del pos test se tiene que 11 trabajadores que conforman el 91.7 % lo consideran como eficiente, mostrando una mejora de 11 trabajadores que conforman el 91.7 %. A partir de estos resultados se comprueba la efectividad que tuvo los controles de la ISO/IEC 27002:2013, en la gestión de la base de datos.

Tabla 8.

Frecuencia de la escalabilidad de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Criterio	**Escalabilidad de la base de datos**					
	PRE		**POST**		**MEJORA**	
	f_i	**%**	**f_i**	**%**	**f_i**	**%**
Deficiente	10	83.3%	0	0.0%	10	83.3%
Regular	2	16.7%	1	8.3%	1	8.3%
Eficiente	0	0.0%	11	91.7%	11	91.7%
Total	**12**	**100.0%**	**12**	**100.0%**		

Fuente: Base de datos de los encuestados

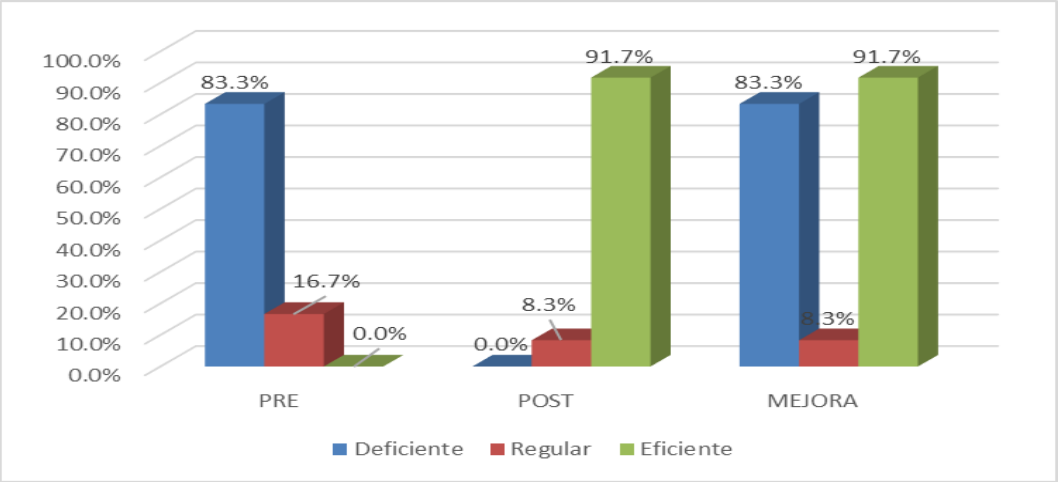


Figura 11. Barra de la escalabilidad de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Interpretación:

A partir de los datos mostrados en la tabla y la figura se puede decir la efectividad que se tuvo en la dimensión escalabilidad de la base de datos, presenta que en el pre test se tiene que 10 trabajadores que conforman el 83.3 % lo analizan como deficiente, mientras que en el pos test se tiene que ningún trabajador lo considera como deficiente, obteniendo una mejora de 10 trabajadores que conforman el 83.3 5, luego al analizar el nivel regular se tiene que 2 trabajadores que conforman el 16.7 % lo analizaron en el pre test, mientras que en el pos test alcanzo que 1 trabajador que representa el 8.3 % lo considera regular, obteniendo una mejora de 1 trabajador que representa el 8.3 %. Finalmente se tiene que ningún trabajador lo considera eficiente en el pre test, mientras que en el pos test se tiene que 11 trabajadores que conforman el 91.7 % lo interpretan como eficiente, obteniendo una mejora de 91.7 %.

Tabla 9.

Frecuencia de la accesibilidad de consulta y escritura de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Criterio	Accesibilidad de consulta y escritura					
	PRE		POST		MEJORA	
	f_i	%	f_i	%	f_i	%
Deficiente	8	66.7%	0	0.0%	8	66.7%
Regular	4	33.3%	4	33.3%	0	0.0%
Eficiente	0	0.0%	8	66.7%	8	66.7%
Total	**12**	**100.0%**	**12**	**100.0%**		

Fuente: Base de datos de los encuestados

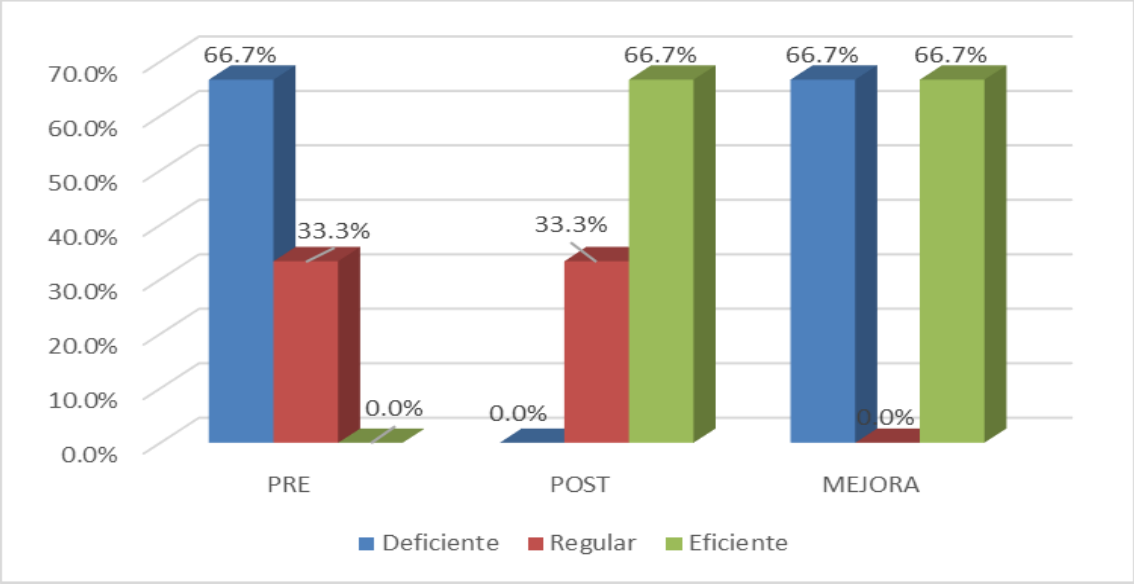


Figura 12. Barra de la accesibilidad de consulta y escritura de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Interpretación:

A partir de los datos mostrados en la tabla y la figura se puede decir que la dimensión accesibilidad de consulta y escritura se tiene que en el pre test presento que 8 trabajadores que conforman el 66.7 % lo consideran como deficiente, mientras que en el pos test no se alcanzó valores para este nivel, seguido de 4 trabajadores que conforman el 33.3 % lo consideran regular, por otro lado en el pos test se alcanzó que 4 trabajadores que conforman el 33.3 % lo consideran regular, manteniendo su nivel, además de ello se tiene que en el pre test no se encontró datos para el nivel eficiente, mientras que en el desarrollo del pos test se obtuvo que 8 trabajadores que conforman el 66.7 % lo analizan como eficiente, obteniendo una mejora de 8 trabajadores que conforman el 66.7 %. A partir de estos resultados se resalta la mejora obtenida por parte de los controles de la ISO/IEC 27002:2013 en la accesibilidad de consultas y escritura en la base de datos.

Tabla 10.

Frecuencia de respaldo y copias de seguridad de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Criterio	Respaldo y copias de seguridad					
	PRE		POST		MEJORA	
	f_i	%	f_i	%	f_i	%
Deficiente	8	66.7%	0	0.0%	8	66.7%
Regular	4	33.3%	6	50.0%	2	16.7%
Eficiente	0	0.0%	6	50.0%	6	50.0%
Total	**12**	**100.0%**	**12**	**100.0%**		

Fuente: Base de datos de los encuestados

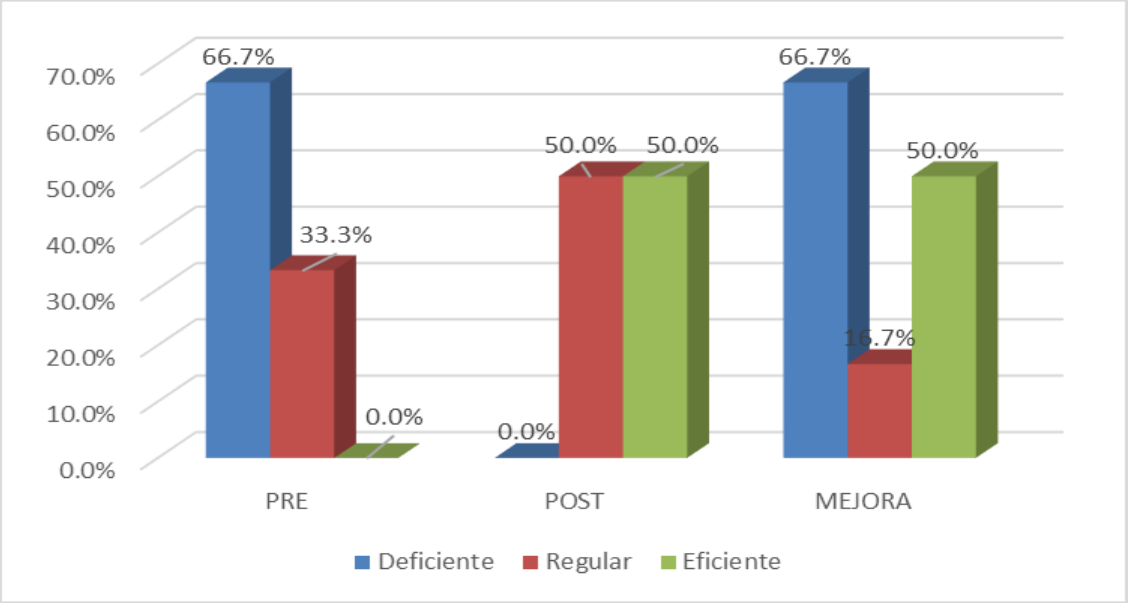


Figura 13. Barra de respaldo y copias de seguridad de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013.

Interpretación:

A partir de los datos mostrados en la tabla y la figura se puede decir que la dimensión respaldo y copias de seguridad de la base de datos, presenta que en el pre test registro que 8 trabajadores que conforman el 66.7 5 lo consideran como deficiente, mientras que en el pos test se registró que ningún trabajador lo considera como deficiente, seguido de 4 trabajadores que conforman el 33.3 % lo consideran de nivel regular, mientras que en el pos test se tiene que 6 trabajadores que conforman el 50.0 % lo analizan como regular, obteniendo una mejora de 2 trabajadores que conforman el 16.7 %, respecto al nivel eficiente se tiene que ningún trabajador lo considera eficiente, mientras que en el pos test se tiene que 6 trabajadores que conforman el 50.0 % lo consideran como eficiente, obteniendo una mejora del 50.0 %. A partir de lo descrito se puede mencionar la efectividad que tiene los controles de la ISO/IEC 27002:2013, para contar con estrategias que fortalezcan la gestión de la base de datos.

4.1.2. Tablas cruzadas por variables y dimensiones

Por el tipo de investigación se ha considerado no necesario implementar las tablas cruzadas.

4.1.3. Prueba de normalidad

Tabla 11.

Prueba de normalidad mediante el método de Shapiro-Wilk para determinar la prueba de hipotesis.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Disponibilidad de la Base de Datos Pre test	,846	12	,033
Escalabilidad de la base de datos Pre test	,704	12	,001
Accesibilidad de consulta y escritura Pre test	,944	12	,547
Respaldo y copias de seguridad Pre test	,955	12	,718
Gestión de la base de datos Pre test	,914	12	,242
Disponibilidad de la Base de Datos Pos test	,902	12	,170
Escalabilidad de la base de datos Pos test	,842	12	,030
Accesibilidad de consulta y escritura Pos test	,841	12	,028
Respaldo y copias de seguridad Pos test	,908	12	,200
Gestión de la base de datos Pos test	,932	12	,407

Fuente: Base de datos de las encuestas

Interpretación:

Demos datos presentados en la tabla se tiene la prueba de normalidad de datos mediante el método de Shapiro-Wilk, por ser una muestra inferior a 50, obteniendo un promedio de significancia que supera al 0.05, con lo cual se determina que la distribución de la muestra es paramétrica y por ser un estudio experimental, el método estadístico más adecuado para el desarrollo es el método de T de Student, con el cual se realizó la prueba de hipotesis.

4.1.4. Contrastación de las hipótesis de investigación

Tabla 12.

Prueba paramétrica de T de Student para realizar la comprobación de la hipotesis

Variable	Prueba T - Student			Nivel de significancia	Decisión
	Valor observado	Valor tabular	Probabilidad significancia		$t_o > t_c$ p <
Gestión de información	t_o= 17,629	t_c = 1,795	p = 0,0000	α = 0,05	Se rechaza

Fuente: Base de datos de las encuestas

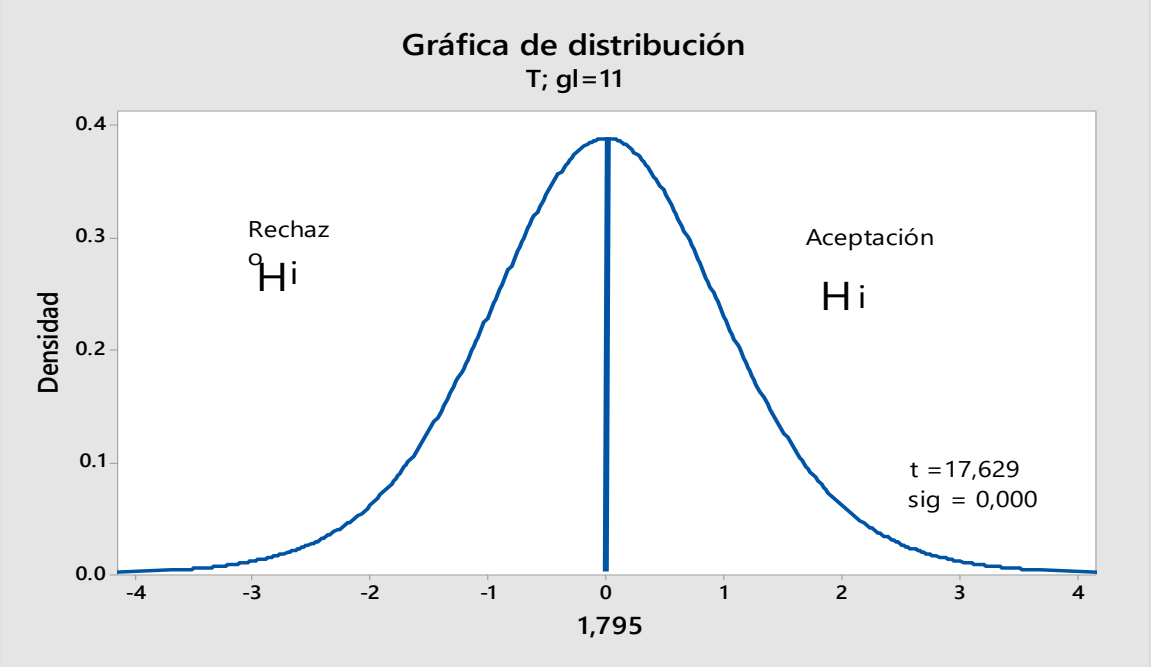


Figura 14. Campana de Gauss para realizar la prueba de hipotesis de investigación.

Interpretación:

A partir de los datos mostrados en la tabla y la campana de Gauss se tiene que el estudio presenta un valor T esperado de 1.795, el cual es el punto clave para determinar la efectividad de la variable independiente, por otro lado, el valor T observado es de 17.629, siendo superior al valor T esperado, con lo que se demuestra la efectividad que se tiene. Además, al analizar si es significativa se tiene que el valor de la significancia obtenida es de sig. = 0.000, ubicada por debajo del margen de error 0.05 con lo que se demuestra que la mejora que se alcanzó en el desarrollo del estudio es significativa.

Capítulo V

5. DISCUSIÓN

5.1. Discusión de resultados obtenidos

Para el desarrollo de este capítulo se tiene en cuenta el análisis de los resultados, en comparación con los antecedentes del estudio, realizando un comentario como investigador y aportando con fundamentación teórica del estudio, detallado en las siguientes líneas:

Respecto al objetivo: Demostrar el impacto de implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, los los resultados plasmados se puede mencionar que en el pre test se tiene que 11 trabajadores que conforman el 91.7% lo consideran como deficiente, mientras que en el pos test se tiene que ninguna persona lo considera como deficiente, obteniendo una mejora de 11 trabajadores que integran el 91.7 %. Por otro lado,

se tiene que e1 trabajador que integra el 8.3 % lo considera como regular, mientras que e1 trabajador lo considera como regular, durante este proceso n ose relevo mejoras significativas. Para el desarrollo del estudio se tiene que en el desarrollo del pre test nadie considera que es eficiente, mientras que en el pos test pasa todo lo contrario que 11 trabajadores que conforman el 91.7 % lo considera como eficiente, teniendo una efectividad considerable del estudio con un valor de 91.7 %, resultados que al ser comparado con lo hallado por Isabel (2015). Se estudió a la fundación universitaria Juan de Castellanos para establecer los pasos a seguir para la implementación de un SGSI para gestionar la seguridad. Asimismo, La presente metodología basada en la Norma ISO 27001 y su guía de buenas prácticas ISO 27002, permitirán Determinar los parámetros y lineamientos que se deben tener en cuenta para la implementación de un SGSI, basado en la norma ISO 27001:2005 en una organización, Analizar la estructura organización y características principales de la Fundación Universitaria Juan de Castellanos para posteriormente proponer una metodología que permita gestionar la seguridad informática, diseñar una metodología para la implementación y mantenimiento de un SGSI, norma ISO 27001, Recomendar algunas herramientas que faciliten la implementación del SGSI en cada una de las etapas propuestas por la norma ISO 27001:2005. Finalmente, los resultados obtenidos al medir las variables de estudios se concluye que la Fundación Universitaria Juan de Castellanos logro organizar, diseñar y administrar de manera sistemática su SGSI, La metodología propuesta y aplicación del SGSI le permitirá a su vez a las directivas de la Universidad mantener una visión general del estado de los sistemas informáticos, plantear estrategias de cambio y mejora de los mismos, verificar las medidas de seguridad aplicadas y los resultados obtenidos, valorar y asegurar sus activos de posibles riesgos y vulnerabilidades presentes, permitiendo la toma de decisiones de manera consecuente, argumentada y documentada, involucrando a todo el personal en un proceso global que le proporcionara la mejora continua, fundamentado por

Parra (2017) la información es un medio o recurso que al igual que el resto de los activos, posee un valor importante para toda organización, por lo cual tendría que ser debidamente protegida. La seguridad de la información la resguarda de diversas amenazas, con el propósito de asegurar la continuidad del negocio, reducir el daño al mismo y reducir el retorno sobre las oportunidades e inversiones.

Respecto al objetivo: Diagnosticar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013, los resultados obtenidos en la tabla y la figura se puede mencionar que la dimensión disponibilidad de la base de datos se tiene que 8 trabajadores que integran el 66.7 % lo consideran como deficiente, seguido de 4 trabajadores que conforman el 33.3 % lo analizan como regular y finalmente se tiene que ningún trabajador lo considera como eficiente. Respecto a la dimensión escalabilidad de la base de datos se tiene que 10 trabajadores que conforman el 83.3 % lo analizan como deficiente, mientras que 2 trabajadores que conforman el 16.7 % lo interpretan como regular, finalmente se tiene que ningún trabajador lo considera como eficiente. Al mencionar a la dimensión accesibilidad de consulta y escritura se tiene que 8 trabajadores que conforman el 66.7 % lo analizan como deficiente, mientras que 4 trabajadores que integran el 33.3 % lo consideran como regular y ningún trabajador lo considera como eficiente. Por otro lado, se tiene que 8 trabajadores que conforman el 66.7 % lo analizan como deficiente, mientras que 4 trabajadores que conforman el 33.3 5 lo consideran como regular, finalmente se tiene que ningún trabajador lo considera como eficiente. Por último respecto a la variable gestión de la base de datos, se tiene que 11 trabajadores que integran el 91.7 % lo consideran como deficiente, mientras que 1 trabajador que conforma el 8.3 % lo interpreta como regular y finalmente ningún trabajador lo considera como eficiente, resultados que guardan similitud con lo hallado por Moscoso (2017), Asimismo, se emplearon diferentes metodologías y

estándares como la ISO/IEC 27002 de seguridad de la información. Finalmente, los resultados obtenidos es el enfoque de un método apropiado, compuesto por 3 pasos y un total de 9 pasos propuestos para la identificación, análisis y evaluación de riesgos y la elaboración formal de políticas de seguridad de la información que los mitiguen. El método fue desarrollado para ser aplicado en empresas alimentarias industriales, pero no se excluye que también se puede aplicar en otros tipos de empresas, con sus respectivas validaciones. La aplicación práctica de cada uno de estos pasos y su evaluación a través del análisis de los resultados obtenidos en ellos se llevaron a cabo en una empresa alimentaria industrial, aplicando la metodología propuesta, donde se encontraron un total de 30 riesgos basados en la probabilidad de ocurrencia y en las consecuencias que afectan la disponibilidad, integridad o confidencialidad del producto. información Además, aplicando la metodología propuesta, se obtuvieron 13 dominios, 30 categorías de control y 88 controles seleccionados de ISO / IEC 27002 en su versión 2013 para mitigar los riesgos identificados y estos controles se reflejaron formalmente en un documento en forma de políticas seguridad de la información, siendo este el resultado final del trabajo de investigación actual para la compañía donde se realizó el estudio de caso, resultados que son fundamentados por lo expuesto por Según Caccuri (2012), “debe tener la capacidad de proteger la información ante el intento de acceso de divulgación a otros usuarios no autorizados. Consiste en asegurar la privacidad de los datos. Solamente los individuos, procesos o dispositivos autorizados pueden acceder a ellos”. Integridad: Según Caccuri (2012), “la información debe estar completa y no ser alterada o modificada sin autorización. La integridad se refiere a la protección de la información de acciones tanto deliberadas como accidentales”.

Respecto al objetivo: Analizar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013, los resultados presentados se tiene que la dimensión disponibilidad

de la base de datos presenta que ningún trabajador lo considera como deficiente, mientras que 1 trabajador que conforma el 8.3 % lo considera como regular y 11 trabajadores que conforman el 91.7 % lo analizan como eficiente, mientras que respecto a la dimensión escalabilidad de la base de datos se tiene que ningún trabajador lo considera como deficiente, mientras que 1 trabajador que representa el 8.3 % lo considera como regular y finalmente se tiene que 11 trabajadores que conforman el 91.7 % lo analizan como eficiente, respecto a la dimensión accesibilidad de consulta y escritura se tiene que ningún trabajador lo considera deficiente, mientras que 4 trabajadores que conforman el 33.3 % lo interpretan como regular y 8 trabajadores que conforman el 66.7 % lo considera como eficiente. Respecto a la dimensión respaldo y copias de seguridad se tiene que ningún trabajador lo considera como deficiente, mientras que 6 trabajadores que conforman el 50.0 % lo analizan como regular y finalmente se tiene que 6 trabajadores que conforman el 50.0 % lo consideran como eficiente. Finalmente, cuando se menciona a la gestión de la base de datos se tiene que ningún trabajador lo considera como deficiente, mientras que 1 trabajador que conforma el 8.3 % lo considera como regular y 11 trabajadores que integran el 91.7 % lo consideran como eficiente. A partir de los datos presentados luego de haber aplicado los controles de la ISO/IEC 27002:2013, se demuestra la efectividad que presento en el desarrollo del estudio y lo favorable que puede ser aplicarlo a otras entidades públicas y privadas del país, resultados que son parecidos a lo hallado por Gavidia y Torres (2018), Su objetivo de investigación fue Implementar los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte. Se estudió a nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte, por lo cual no se trabajó con muestra ya que utilizaron el 100 % del área. Asimismo, Durante la etapa de auditoria se realizaron dos evaluaciones para medir el nivel de la seguridad de la información en el área de TI de la Unión Peruana del

Norte, donde se permite conocer al detalle cómo se cumplieron los criterios de evaluación del PAM de Cobit. Finalmente, los resultados obtenidos se midieron las variables de estudio donde se concluye que: La implementación de los controles de la ISO/IEC 27002:2013 mejoró significativamente el nivel de seguridad de la información, puesto que durante la primera evaluación se obtuvo un resultado inicial de 47% y en la segunda evaluación ya con los controles implementados se obtuvo un resultado de 84%. Donde concluyó que la diferencia encontrada entre ambos resultados, mejoró en un 37% de la seguridad física y lógica de la información, respaldo por Project Management Consultores de Proyectos (2006), existen tres fuentes primordiales para los requerimientos en referencia a la seguridad de la información. La primera fuente deriva de hacer una evaluación de riesgo para la organización, al tener en cuenta los objetivos y estrategia de negocio. A través de esta evaluación de riesgos se identifican las amenazas pertenecientes a los activos, se evalúa su vulnerabilidad y su probabilidad de ocurrencia y se estima o calcula su impacto potencial. La segunda fuente son los requerimientos reguladores, requerimientos legales, requerimientos contractuales y requerimientos estatutarios que se ven en la necesidad de complacer a una organización, a los contratistas, a sus socios comerciales y proveedores de servicio y su entorno socio-cultural.

Respecto al objetivo: Comparar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013, los datos mostrados en la tabla y la figura se puede encontrar que la dimensión de la base de datos, en el pre test se tiene que 8 trabajadores que conforman el 66.7 % lo interpretan como deficiente, mientras que en el pos test se tiene que ningún trabajador lo considera como deficiente, mostrando una mejora de 8 trabajadores, que representan el 66.7 %, respecto al nivel regular se presentó que en el pre test se tiene que 4 trabajadores que conforman el 33.3 % lo analizan como regular, por otro lado en el

pos test se tiene que 1 trabajador que conforma el 8.3 % lo analiza como regular, mostrando una efectividad de 3 trabajadores que representan el 25.0 %, respecto al nivel eficiente se tiene que en el pre test se obtuvo que ningún trabajador lo considero como eficiente, mientras que en el desarrollo del pos test se tiene que 11 trabajadores que conforman el 91.7 % lo consideran como eficiente, mostrando una mejora de 11 trabajadores que conforman el 91.7 %. A partir de estos resultados se comprueba la efectividad que tuvo los controles de la ISO/IEC 27002:2013, en la gestión de la base de datos. A partir de los datos mostrados en la tabla y la figura se puede decir la efectividad que se tuvo en la dimensión escalabilidad de la base de datos, presenta que en el pre test se tiene que 10 trabajadores que conforman el 83.3 % lo analizan como deficiente, mientras que en el pos test se tiene que ningún trabajador lo considera como deficiente, obteniendo una mejora de 10 trabajadores que conforman el 83.3 5, luego al analizar el nivel regular se tiene que 2 trabajadores que conforman el 16.7 % lo analizaron en el pre test, mientras que en el pos test alcanzo que 1 trabajador que representa el 8.3 % lo considera regular, obteniendo una mejora de 1 trabajador que representa el 8.3 %. Finalmente se tiene que ningún trabajador lo considera eficiente en el pre test, mientras que en el pos test se tiene que 11 trabajadores que conforman el 91.7 % lo interpretan como eficiente, obteniendo una mejora de 91.7 %. A partir de los datos mostrados en la tabla y la figura se puede decir que la dimensión accesibilidad de consulta y escritura se tiene que en el pre test presento que 8 trabajadores que conforman el 66.7 % lo consideran como deficiente, mientras que en el pos test no se alcanzó valores para este nivel, seguido de 4 trabajadores que conforman el 33.3 % lo consideran regular, por otro lado en el pos test se alcanzó que 4 trabajadores que conforman el 33.3 % lo consideran regular, manteniendo su nivel, además de ello se tiene que en el pre test no se encontró datos para el nivel eficiente, mientras que en el desarrollo del pos test se obtuvo que 8 trabajadores que conforman el 66.7 % lo analizan como eficiente, obteniendo una mejora de 8

trabajadores que conforman el 66.7 %. A partir de estos resultados se resalta la mejora obtenida por parte de los controles de la ISO/IEC 27002:2013 en la accesibilidad de consultas y escritura en la base de datos. A partir de los datos mostrados en la tabla y la figura se puede decir que la dimensión respaldo y copias de seguridad de la base de datos, presenta que en el pre test registro que 8 trabajadores que conforman el 66.7 5 lo consideran como deficiente, mientras que en el pos test se registró que ningún trabajador lo considera como deficiente, seguido de 4 trabajadores que conforman el 33.3 % lo consideran de nivel regular, mientras que en el pos test se tiene que 6 trabajadores que conforman el 50.0 % lo analizan como regular, obteniendo una mejora de 2 trabajadores que conforman el 16.7 %, respecto al nivel eficiente se tiene que ningún trabajador lo considera eficiente, mientras que en el pos test se tiene que 6 trabajadores que conforman el 50.0 % lo consideran como eficiente, obteniendo una mejora del 50.0 %. A partir de lo descrito se puede mencionar la efectividad que tiene los controles de la ISO/IEC 27002:2013, para contar con estrategias que fortalezcan la gestión de la base de datos. Fundamentado por ISO 27002 es una guía de recomendaciones de optimas prácticas para la gestión de la información. Otorga directrices a las normas de seguridad de la información en las prácticas de seguridad de los datos y en las organizaciones, abarcando la selección, implementación y la administración de controles considerando el contexto de seguridad de la información de la empresa.

5.2. Conclusiones

General

Se demostró la afectividad de los controles de la ISO/IEC 27002:2013 sobre la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, obteniendo resultados que en el nivel deficiente se mejoró en 91.7 %, en el nivel regular se mantuvo su percepción y en el nivel eficiente se incrementó en un 71.7 %, con lo cual se comprueba la hipótesis afirmando que existe mejoras significativas de los resultados en la comparación del pre y post test.

Específicas

Se encontró lo problemas por lo que afronta la gestión de la base de datos, se centran en la disponibilidad de la base de datos el puntaje más alto se encontró en el nivel deficiente, mientras que la dimensión escalabilidad de la base de datos se tiene el puntaje más alto para el nivel deficiente con un valor de 83.3 %, respecto a la dimensión accesibilidad de consultas y escritura se tiene el puntaje más alto para el nivel deficiente, respecto a la dimensión respaldo de copias de seguridad se tiene el puntaje más alto para el nivel deficiente con valores de 66.7 % y la gestión de la base de datos en general presenta el valor más alto para el nivel deficiente con una valor de 91.7 %.

Se encontró que las mejoras alcanzada por lo que afronta la administración de la base de datos se encuentra que en la dimensión disponibilidad de la base de datos se alcanzó que el punto más alto para el nivel eficiente con un valor de 91.7 %, seguido de la dimensión escalabilidad de la base de datos alcanzo el puntaje más alto para el nivel eficiente con un valor de 91.7 %, respecto a la dimensión accesibilidad de consulta y escritura se tiene que el puntaje más alto se ubica en el nivel eficiente con un valor de 66.7 %, respecto a la dimensión respaldo de copias de seguridad se tiene el valor más alto para el nivel regular y

eficiente con 50.0 % para cada uno de ellos, finalmente para la gestión de la base de datos se tiene que el puntaje más alto se tiene para el nivel eficiente con un valor de 91.7 %.

Al realizar la comparación del antes y después de las dimensiones se alcanzó mejoras que fortalecen el estudio, respecto a la dimensión disponibilidad de la base de datos se obtuvo una reducción del nivel deficiente del 66.7 %, en el nivel regular se mejoró en 25.0 % y en el nivel eficiente se mejoró en un 91.7 %. Respecto a la dimensión escalabilidad de la base de datos en el nivel deficiente se mejoró en 83.3 %, respecto al nivel regular se mejoró en 8.3 %, por último, se tiene que el nivel eficiente se mejoró en 91.7 %. Respecto a la dimensión accesibilidad de consulta y escritura de la base de datos, en el nivel deficiente se optimizo en 66.7 %, referente al nivel regular no se presentó mejoras y respecto al nivel eficiente se mejoró en 66.7 %.

5.3. Recomendaciones

Con el desarrollo del estudio se plantea las siguientes recomendaciones que pueden ayudar a fortalecer las deficiencias presentadas en el trabajo de la base de datos.

Primero: A la gerencia de la empresa establecer capacitaciones al personal de sistemas relacionados al manejo de controles de la ISO/IEC 27002:2013 para que puedan contar con los conocimientos necesarios para la administración de la base de datos de manera oportuna.

Segundo: Al personal de sistemas realizar siempre inspecciones y monitoreo del óptimo funcionamiento de la base de datos y realizar los mantenimientos preventivos físicos de manera oportuna para evitar daños y perdida de información.

Tercero: A la entidad invertir en la adquisición de nuevos equipos de infraestructura física cada 3 años con la finalidad de contar con los equipos necesarios para que la conectividad sea más rápida, además de ellos establecer supervisiones periódicas.

Cuarta: Realizar las copias de seguridad de la base de datos y programarla para que se almacene en un lugar donde se encuentre segura y no pueda ser afectada o dañada por otras personas.

Quinta: Desarrollar formatos para registrar cada cambio que se realice en el desarrollo laboral y la administración de la base de datos.

FUENTES DE INFORMACIÓN

Aliaga, L. (2013). *Diseño de un sistema de Gestión de Seguridad de información para un instituto educativo.* Lima, Perú: Pontificia Universidad Católica del Perú.

Aleman, H. (2015). *Metodología para la implementación de un SGSI en la fundación universitaria Juan de Castellanos, Bajo la norma ISO 27001: 2005.* (Tesis de maestría). Recuperado de https://reunir.unir.net/bitstream/handle/123456789/3129/HelenaClaraIsabel_Aleman_Novoa.pdf?sequence=1&isAllowed=y

AENOR. (2015). Norma española UNE-ISO/IEC 27002. Madrid: AENOR

Aguirre, J. D., & Aristizabal, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda.* Recuperado de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf?sequence=1

Alegre, M., & Garcia, A. (2011). SEGURIDAD INFORMATICA ED.11 Paraninfo. Madrid: Paraninfo.

Baca, G. (2016). *Introducción a la Seguridad Informática.* México: Grupo Editorial Patria.

Godoy, C.(2011). Historia de la seguridad de la información. Recuperado de http://es.scribd.com/doc/59484913/Historia-de-La-Seguridad-a

Caccuri, G. (2012). *Salvaguardando la privacidad.* Recuperado de https://www.cookiebot.com/es/

Cortéz, A. y Santiago, W. (2018). Plan de seguridad informática basado en la Norma ISO 27002 para mejorar la gestión tecnológica del Colegio Carmelitas – Trujillo (Tesis de maestría). Recuperado de http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/11066/CORT%c3%89Z%20R

ODR%c3%8dGUEZ%2c%20AMELIA%20IVON%2c%20SANTIAGO%20CUEVA%2c%20WILFREDO%20JHONATAN.pdf?sequence=1&isAllowed=y

Fernández, G., (2018). El concepto de riesgo, probabilidad e impacto a la hora de realizar la evaluación de impacto de protección de datos. [en línea]. Disponible en: https://www.iberley.es/revista/concepto-riesgo-probabilidad-impacto-evaluacion-impactoproteccion-datos-219.

Gavidia, S. y Torres, L. (2018). *Implementación de los controles de la ISO/IEC 27002:2013 para la mejora del nivel de seguridad física y lógica de la información en el área de TI de la Unión Peruana del Norte* (Tesis de maestría). Recuperado de https://gestion.pe/tendencias/management-empleo/upn-40-adultos-estudian-universidad-estudios-tecnicos-buscan-142021-noticia/

Gómez, A., (2011). Enciclopedia de la seguridad informática. Vol. 6. S.l.: s.n.

Gómez, S., (2007). Seguridad De La Información. Universidad Nacional de Ingeniería [en línea], pp. 500. ISSN 1815-0268. DOI 10.13128/ijae-9077. Disponible en: http://cybertesis.uni.edu.pe/handle/uni/9764%0Ahttp://cybertesis.uni.edu.pe/bitstream/uni/9 764/1/gomez_fs.pdf.

Hallberg, J. y Hunstad, A., (2005*). A frmewor for system security assessment. Information Assurance Workshop,* vol. Six annual, pp. 25. INFOBAE, 2011. No Title [en línea]. 2011. S.l.: 2011-08-09. Recuperado en: http://www.seguridadydefensa.com.ec/noticias/anonymus-revelo-datos-de-45-mil-policias24513.html.

Hernandez Sampieri, R. (2017). Fundamentos de Investigación. Ciudad de México: McGRAW - HILL/INTERAMERICANA EDITORES, S.A.

Hernández, R., Fernández, C. & Baptista, P. (2014). Metodología de la investigación (6a ed.). México: Mc Graw – Hill.

Hernández, M. (12 de Diciembre de 2012). *Tipos y Niveles de investigación. Recuperado de Metodología de la investigación:* http://metodologiadeinvestigacionmarisol.blogspot.pe/2012/12/tipos-y-niveles-deinvestigacion.html

ISOTools Excellence (2015). *Sistemas de Gestión de Riesgos y Seguridad.* Recuperado de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Lahuara, E. (2007). *Metodología para desarrollar un plan de Seguridad de Información. Lima, Perú: Universidad San Martin de Porres.* Tesis para obtener el título de ingeniero de computación y sistemas.

Lahuara, E. (2007). *Metodología para desarrollar un plan de Seguridad de Información. Lima, Perú: Universidad San Martin de Porres.* Tesis para obtener el título de ingeniero de computación y sistemas.

Montenegro, L. (2014). *Seguridad de la Información: Más que una actitud, un estilo de vida.* Recuperado de http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/ Muñoz, C. (1998). Como Elaborar y Asesorar una Investigación de Tesis. México: Prentice Hall.

Mendez, A., Mesa, J., Zapico, F. y Guerreo, V., (2003). *Techno-Legal Aspects of Information Society and New Economy: an Overview. [en línea]*, pp. 187. Disponible en: http://mario.elinos.org.mx/publication/papers/2003/002.pdf.

Mentor, (2016). *Normas ISO sobre gestión de seguridad de la información | Seguridad Informática.* [en línea]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_ sobre_ gestin_de_seguridad_de_la_informacin.html.

Mercado, J. (2016). Modelo de gestión de seguridad de la información para el E-Gobierno. (Tesis de maestría). Recuperado de

https://cybertesis.unmsm.edu.pe/bitstream/handle/cybertesis/6414/Mercado_rj.pdf?sequence=1&isAllowed=y

Moscoso, F. (2017). *Elaboración y plan de implementación de políticas de seguridad de la información aplicadas a una empresa industrial de alimentos.* (Tesis de maestría). Recuperado de http://dspace.ucuenca.edu.ec/handle/123456789/28655

Moreno, F. (2008). Proyecto de norma técnica colombiana NTC-ISO 27005. Colombia.

Parra, L. (2017). *Importancia de la planificación de recursos humanos en la empresa perspectivas* (Tesis de maestría). Recuperado de https://www.redalyc.org/pdf/4259/425942331002.pdf

Project Management Consultores de Proyectos (2006). *Herramientas y técnicas para la gestión de proyectos de desarrollo PM4R.* Recuperado de https://indesvirtual.iadb.org/file.php/1/PM4R/Guia%20de%20Aprendizaje%20PMA%20SPA.pdf?fbclid=IwAR0_17MRzWGU-xgLTa1HregQQYcDu4V8vVnAga7GbhPdR2dJ0QbezaNZ-ig

Ramírez, R. (2010). Proyecto de investigación. Lima-Perú: Universidad Mayor de San Marcos. Sánchez, A. (2010). Normativa e inducción en seguridad de información para el grupo telefónica. Lima: Universidad San Martin de Porres. Tesis para obtener el título de ingeniero de computación y sistemas.

Swanson, Marine y Guttman, Barbara. Generally Accepted Principles and Practices for Securing Information Technology Systems. Washington DC: s.n., 1996. NIST SP 800-14.

Torres, A. y Lavayen, M. (2017). *Diseño de un sistema de gestión de calidad según las normas ISO 9001:2015 para una empresa textil de la ciudad de Guayaquil.* (Tesis de maestría). Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/14220/1/UPS-GT001890.pdf

Tokeshi, A. (2008). Planifique, desarrolle y apruebe su tesis: Guía para mejores resultados. Lima-Perú: Universidad de Lima.

Téllez, J., (2014). Contratos, riesgos y seguros informáticos. México DF: Universidad Autónoma de México.

Valderrama, S. (2012). Pasos para Elaborar Proyectos de Investigación Científica. (2a ed.). Perú: San Marcos.

ANEXOS

Anexo 1. Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES Y DIMENSIONES	METODOLOGÍA
Problema principal: ¿Cómo la implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019?	**Objetivo general:** Demostrar el impacto de implementación de los controles de la ISO/IEC 27002:2013, favorecen a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.	**Hipótesis general:** La implementación de los controles de la ISO/IEC 27002:2013, favorece a la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019.	**Variable I:** Controles de la ISO/IEC 27002:2013 **D1:** Gestión de Activos **D2:** Control de Acceso **D3:** Seguridad Física y Ambiental **D4:** Seguridad de las Operaciones **D5:** Aspectos de seguridad de la información para la gestión del a continuidad del negocio. **Variable D:** Gestión de la base de datos **D1:** Disponibilidad de la Base de Datos **D2:** Escalabilidad de la base de datos **D3:** Accesibilidad de	**Tipo de investigación** Aplicada **DISEÑO** Experimental – Pre experimental **POBLACIÓN** 12 trabajadores **MUESTRA** 12 trabajadores **TÉCNICA** Encuesta **INSTRUMENTOS** Cuestionarios
Problemas secundarios: ¿Cómo se presenta la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013? ¿Cómo se presenta la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013? ¿Qué niveles se alcanzaron al comparar la gestión de la base	**Objetivos específicos:** Diagnosticar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013. Analizar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013. Comparar la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la	**Hipótesis específicas:** La gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes de la implementación de los controles de la ISO/IEC 27002:2013, es deficiente. La gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, después de la implementación de los controles de la ISO/IEC 27002:2013, es eficiente. La comparación la gestión de la base de datos de los Registros Públicos de la Zona VII – Sede Huaraz,		

de datos de los Registros Públicos de la Zona VII – Sede Huaraz, 2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013?	ISO/IEC 27002:2013.	2019, antes y después de la implementación de los controles de la ISO/IEC 27002:2013, resulta favorable.	consulta y escritura **D4:** Respaldo y copias de seguridad	

Anexo 2. Instrumentos para la recolección de datos

"IMPLEMENTACIÓN DE LOS CONTROLES DE LA ISO/IEC 27002:2013, PARA LA GESTIÓN DE LA BASE DE DATOS DE LOS REGISTROS PUBLICOS DE LA ZONA VII – SEDE HUARAZ, 2019"

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: Disponibilidad de la Base de Datos					
1	¿La institución cuenta con horarios para el ingreso de usuario a la base de datos, resguardando la seguridad de la misma?					
2	¿Se cuenta con tipo de accesos para los usuarios (Permisos de ingreso a la base de datos)?					
3	¿Existen políticas de acceso a la base de datos?					
4	¿Todos los usuarios cuentan con los mismos permisos para acceder a la base de datos?					
	DIMENSION: Escalabilidad de la base de datos					
5	¿Considera que la base de datos es escalable y nuevas tecnologías?					
6	¿Es necesario mejorar la escalabilidad de la base de datos?					
7	¿Considera suficiente el espacio con el que cuenta el disco dura del servidor?					
8	¿Se cuenta con disco dura de almacenamiento de respaldo?					
9	¿Es necesario mejoras en la capacidad física del servidor?					
	DIMENSION: Accesibilidad de consulta y escritura					
10	¿Cualquier usuario puede realizar sus consultas a la base de datos?					
11	¿Se cuenta con controles para el acceso a la base de datos?					
12	¿El tiempo de respuesta de la base de datos es oportuno?					
13	¿Se debería mejorar el tiempo de respuesta de la base de datos?					
	DIMENSION: Respaldo y copias de seguridad					
14	¿Se realizan copias de seguridad de la base de datos?					
15	¿Es necesario realizar copias de seguridad de manera periódica?					
16	¿Se cuenta con un espacio para almacenar las copias de seguridad de manera que aseguren la información?					
17	¿Se cuenta con protocolos para el acceso a las copias de seguridad de la base de datos?					
18	¿Se cuenta con seguridad física de la base de datos?					

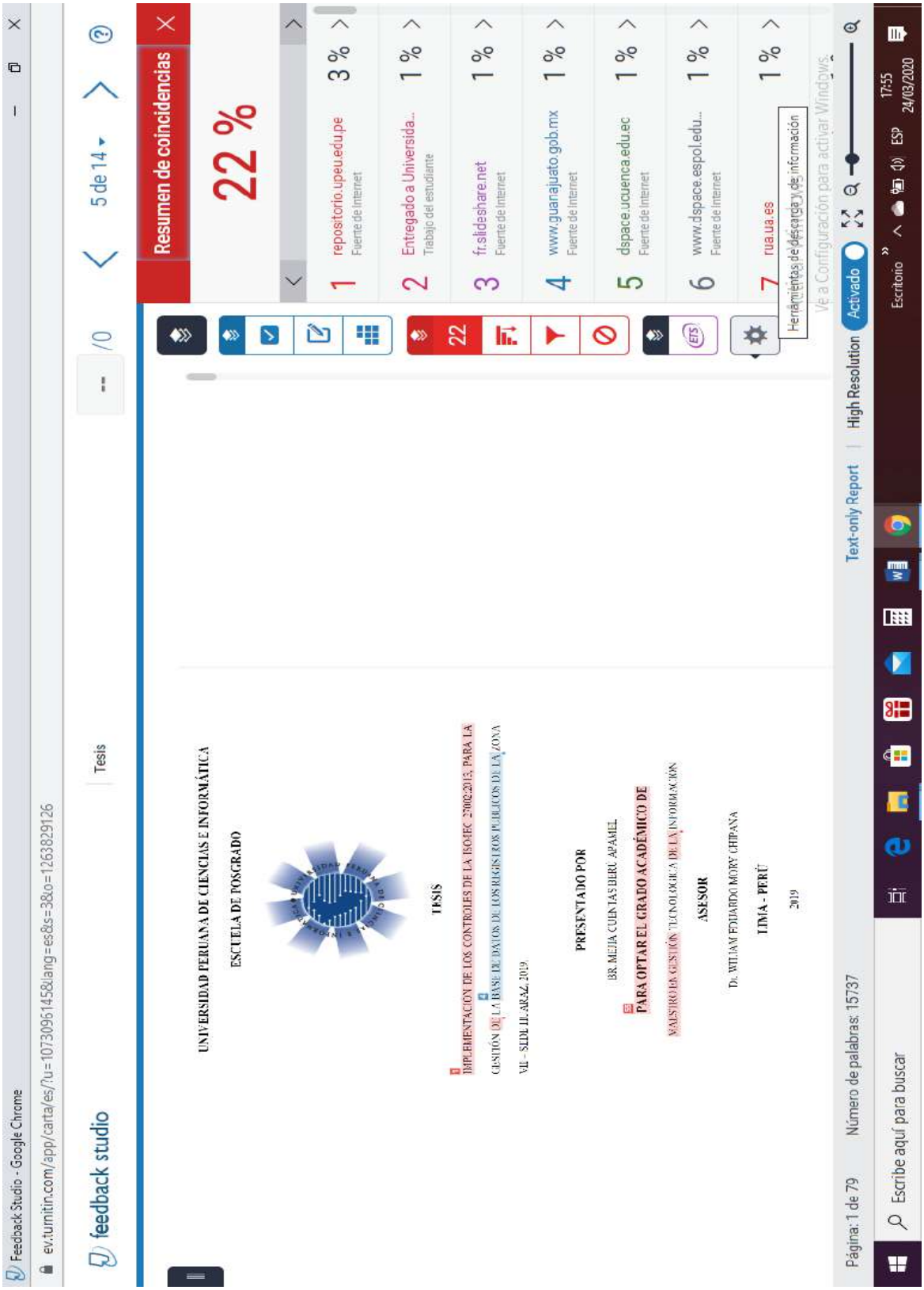
Gracias por tu aportación

Anexo 3. Base de datos

PRE-TEST VARIABLE: GESTIÓN DE LA BASE DE DATOS DE LOS REGISTROS PUBLICOS DE LA ZONA VII – SEDE HUARAZ, 2019																						TOTAL
N°	D1: Disponibilidad de la Base de Datos				SUB	D2:Escalabilidad de la base de datos					SUB	D3: Accesibilidad de consulta y escritura				SUB	D4: Respaldo y copias de seguridad					SUB	
	1	2	3	4		5	6	7	8	9		10	11	12	13		14	15	16	17	18		
1	3	3	2	2	10	1	2	1	3	2	9	1	3	2	2	8	2	2	2	2	2	10	37
2	2	2	3	2	9	1	1	2	2	3	9	1	2	3	2	8	2	3	1	1	2	9	35
3	2	2	2	2	8	1	2	1	2	2	8	1	2	2	2	7	2	3	4	3	3	15	38
4	2	2	2	2	8	1	2	2	2	2	9	2	2	2	2	8	2	3	3	4	3	15	40
5	2	2	1	2	7	1	4	3	2	1	11	1	2	1	2	6	2	2	2	2	2	10	34
6	2	2	2	1	7	1	2	2	2	2	9	1	2	2	1	6	2	1	1	1	1	6	28
7	3	3	2	2	10	1	2	2	3	2	10	2	3	2	2	9	2	2	3	2	2	11	40
8	2	2	2	1	7	1	4	1	2	2	10	1	2	2	1	6	2	1	3	3	2	11	34
9	3	2	2	3	10	1	4	2	2	2	11	2	2	2	3	9	2	3	3	2	2	12	42
10	3	2	2	2	9	1	2	2	2	2	9	2	2	2	2	8	2	3	2	3	3	13	39
11	1	2	2	2	7	1	2	2	2	2	9	1	2	2	2	7	3	2	2	2	1	10	33
12	2	3	2	1	8	3	5	2	4	3	17	3	2	1	2	8	2	2	2	2	1	9	42

POS-TEST VARIABLE: GESTIÓN DE LA BASE DE DATOS DE LOS REGISTROS PUBLICOS DE LA ZONA VII – SEDE HUARAZ, 2019																							TOTAL
N°	D1: Disponibilidad de la Base de Datos				SUB	D2:Escalabilidad de la base de datos					SUB	D3: Accesibilidad de consulta y escritura				SUB	D4: Respaldo y copias de seguridad					SUB	
	1	2	3	4		5	6	7	8	9		10	11	12	13		14	15	16	17	18		
1	3	4	5	5	17	5	4	4	5	5	23	4	3	2	2	11	3	4	4	4	3	18	69
2	4	3	3	4	14	5	5	5	4	4	23	4	3	5	2	14	3	4	4	5	3	19	70
3	4	4	3	4	15	4	4	5	5	5	23	4	3	5	2	14	3	4	4	5	3	19	71
4	5	3	5	5	18	4	4	4	4	5	21	5	4	2	2	13	3	4	4	5	3	19	71
5	3	5	4	5	17	5	5	3	5	4	22	1	5	4	2	12	3	4	5	5	3	20	71
6	4	4	3	5	16	3	5	5	3	4	20	3	5	4	1	13	3	4	4	4	3	18	67
7	5	4	4	4	17	3	4	4	5	5	21	3	5	4	2	14	3	4	3	4	4	18	70
8	5	4	5	5	19	4	4	4	4	5	21	3	4	4	1	12	4	4	3	4	4	19	71
9	5	4	4	5	18	4	3	5	4	5	21	4	4	4	3	15	4	4	3	4	4	19	73
10	5	4	5	4	18	5	4	4	4	5	22	4	4	4	2	14	4	4	3	4	4	19	73
11	5	4	4	5	18	5	5	5	5	4	24	4	4	4	2	14	5	4	3	4	4	20	76
12	5	4	4	4	17	3	4	2	4	3	16	3	4	4	2	13	4	4	4	4	3	19	65

Anexo 4. Evidencia digital de similitud



Anexo 5. Autorización de publicación en el repositorio

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

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

1.- DATOS DEL AUTOR

Apellidos y Nombres: Mejia Cuentas Beru Apamel

DNI: 45438278 Correo electrónico: beru_amc@hotmail.com

Domicilio: Jr. Candelaria Villar # 452 - Independencia

Teléfono fijo: _____ Teléfono celular: 956099245

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: Posgrado

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

Título del Trabajo de Investigación / Tesis:

Implementación de los Controles de la ISO/IEC 27002:2013 para la gestión de la base de datos de los registros públicos de la Zona VII – Sede Huaraz

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, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
(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 23 días del mes de junio de 2020.

Firma