UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

ISO 27001:2013 para la gestión del manejo de información en la UGEL Bolognesi, Ancash 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Ibarra Caqui, Lucio (orcid.org/0000-0002-2425-4668)

ASESOR:

Dr. Acuña Benites, Marlon Frank (orcid.org/0000-0001-5207-9353)

CO-ASESOR:

Dr. Flores Zafra, David (orcid.org/0000-0001-5846-325X)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2023

Dedicatoria

A mi esposa, por su gran amor, dedicación, su apoyo constante, a mis hermanos y manera especial a mi Madre por su constante consejo, apoyo y confianza.

Gracias a ustedes que sumaron esfuerzo para cumplir con mis objetivos personales y profesionales.

Agradecimiento

Expresar mi sincera gratitud a las personas y profesionales que me brindaron su apoyo para el desarrollo de mi investigación, resaltando lo siguiente:

A los trabajadores de la UGEL Bolognesi por la disponibilidad a brindarme la información necesaria para culminar con éxito el trabajo.

A la Universidad Cesar Vallejo, a los docentes por brindarnos conocimientos que hoy en día hacen posible la conclusión de la investigación.

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

El estudio presenta por objetivo general determinar la influencia de la implementación ISO 27001:2013 en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, referente a la metodología que se adoptó en el estudio se considera de tipo aplicada, el diseño fue experimental, con sub categoría pre experimental, el alcance temporal que presento fue longitudinal. La población se confirmó por 42 trabajadores, la muestra se conformó por la misma cantidad y el muestreo aplicado fue el no probabilístico, dentro de ello, se aplicó como técnica a la encuesta y el instrumento fue el cuestionario, para la aplicación se realizó el proceso de validación y confiabilidad, alcanzando un valor de 0.859. Logrando concluir: Se ha mejorado significativamente (sig. = 0.000 < 0.05) la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 52.4% en el post-test, luego para el nivel regular se mejoró en 19.0% y el nivel eficiente se incrementó en 71.4%.

Palabras clave: Implementación ISO 27001:2013, gestión del manejo de información, seguridad.

Abstract

The study has as a general objective to determine the influence of the implementation of ISO 27001: 2013 in the management of information management in the UGEL Bolognesi Ancash 2023, referring to the methodology that was adopted in the study is considered applied type, the design was experimental , with a pre-experimental subcategory, the temporal scope that I present was longitudinal. The population was confirmed by 42 workers, the sample was made up of the same amount and the applied sampling was non-probabilistic, within it, the technique was applied to the survey and the instrument was the questionnaire, for the application the process was carried out. validation and reliability, reaching a value of 0.859. Managing to conclude: It has been significantly improved (sig. = 0.000 < 0.05) the management of information management in the UGEL Bolognesi Ancash 2023, through the implementation of ISO 27001: 2013, at the deficient level it was reduced by 52.4% in the post test, then for the regular level it was improved by 19.0% and the efficient level increased by 71.4%.

Keywords: ISO 27001:2013 implementation, information management, security.

I. INTRODUCCIÓN

Con el inicio de la pandemia, las entidades públicas han comenzado a darle la importancia respectiva sobre el manejo de información, para lo cual, se requiere que se apliquen estrategias de seguridad de la información para salvaguardar los datos de las empresas (Estrada et al., 2021).

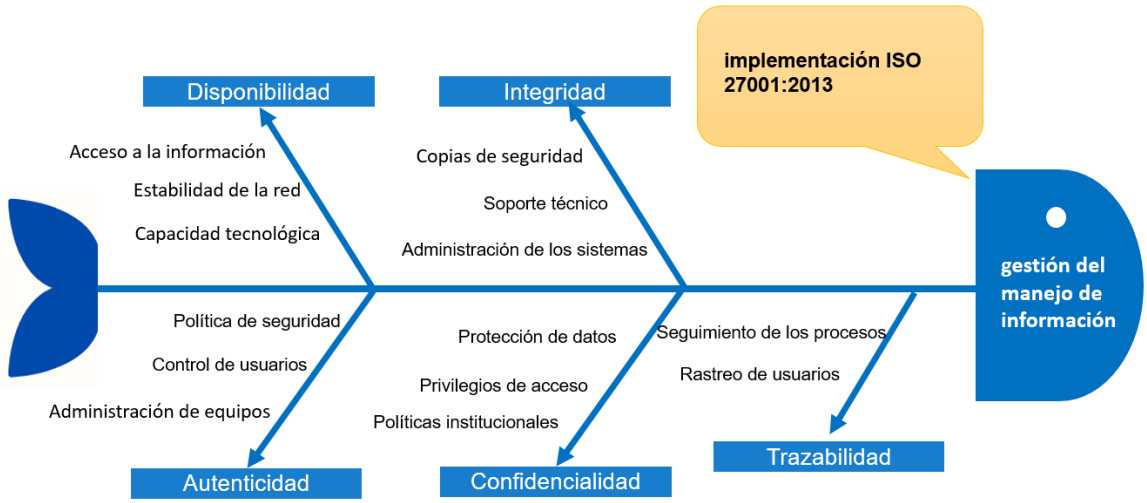
En México, durante los años 2020 y 2021 se ha iniciado una transformación del manejo de la información y las modalidades de trabajo ocasionados por la pandemia, lo cual ha generado que las instituciones que pertenecen al sector público y privado cambien la forma de trabajar a raíz del aislamiento social generado, adoptando medidas que permitan continuar brindando el servicio esperado y aplicar medidas de protección en la información que se transmite (Nieves y Ponjuan, 2021). Es así como, en Colombia los problemas tecnológicos generados con el origen de la pandemia han reflejado el descuido por parte de las autoridades de las diferentes organizaciones por incorporar medios tecnológicos en la automatización de los servicios que se brinda. Por ello, se ha reflejado vulneración de la información en el trabajo remoto desarrollado por diferentes entidades (Osorio, 2021). De la misma manera, en Ecuador, es evidente que las entidades públicas no se preocupan por mejorar su capacidad tecnológica y automatizar sus servicios por medio de aplicaciones web que permitan a los usuarios realizar sus trámites sin necesidad de recurrir a la entidad (Zuña et al., 2019).

Dentro del contexto nacional se tiene que la pandemia ha obligado a cambiar la modalidad de trabajar y ha puesto en evidencia la vulneración de la información y la falta de capacidad tecnológica para desarrollarlo, con entidades públicas que no cuentan con un firewall que proteja la información (Rodríguez et al., 2020). Es evidente que la tecnológica en la gestión pública peruana no ha sido tomada con la relevancia respectiva, evidenciada en las deficiencias tecnológicas que ha presentado el servicio a través del trabajo remoto presentada durante el tiempo de aislamiento que presentó el país, careciendo de infraestructura, equipamiento y en ocasiones el área de informática respectiva (Bustamante et al., 2021).

Es así como, en el contexto regional y local la UGEL Bolognesi, no es ajena a la realidad que ocurre en los diferentes sectores públicos del país, donde la capacidad tecnológica no tiene la relevancia respectiva y no es considerada como relevante en la gestión que se realiza de los trámites administrativos. Dentro de los principales inconvenientes que se ha registrado en la entidad se encuentra la conexión a internet que no tiene un firewall que brinde la seguridad respectiva a la red, luego la ausencia de procedimientos de seguridad de la información, por otro lado, no se desarrollan las copias de seguridad respectivas, quedando vulnerables ante cualquier inconveniente que se presente de virus o alteración de información. Otro aspecto considerado es que, algunos usuarios se conectan desde fuera de la entidad por Anydesk sin tener los procedimientos necesarios para resguardar la información de la entidad. Estos acontecimientos han llevado a que existe la necesidad de incorporar mecanismos que ayuden a resguardar la información y proteger con políticas necesarias para contar con la integridad de datos, además de evitar que se vulnera la confidencialidad de los usuarios o de la misma entidad.

Figura 1

Diagrama de Ishikawa



A través de los descrito se presenta como problema general: ¿De qué manera la implementación ISO 27001:2013 incide en la gestión del manejo de información en la Ugel Bolognesi Ancash 2023?; de ello se tiene como problemas específicos, primero ¿De qué manera la implementación ISO 27001:2013 incide la disponibilidad en la Ugel Bolognesi?; segundo ¿De qué manera la implementación

ISO 27001:2013 incide la autenticidad en la Ugel Bolognesi?; tercero ¿De qué manera la implementación ISO 27001:2013 incide la integridad en la Ugel Bolognesi?; cuarto ¿De qué manera la implementación ISO 27001:2013 incide la confidencialidad en la Ugel Bolognesi?; quinto ¿De qué manera la implementación ISO 27001:2013 incide en la trazabilidad en la Ugel Bolognesi?

Al hacer referencia a la justificación que refleja la investigación se tiene a la relevancia social, que a partir del análisis de la entidad y detallar la problemática que presenta referente al manejo de la información se dieron a conocer las medidas correctivas que se aplicarán para mejorar esta gestión por medio de la implementación de la seguridad de la información ISO 27001:2013.

Del mismo modo, en el aspecto practico se registrarán resultados estadísticos que ayuden a demostrar el efecto generado con la implementación de la ISO y las mejoras alcanzadas en el post-test, considerado como relevante en la gestión de la entidad.

Desde el campo metodológico el estudio elabora y adapta instrumentos que ayudaron a determinar cómo se presenta el manejo de la información, el cual al ser validado y obtener la confiabilidad respectiva puede ser aplicado a futuros estudios para un análisis de otro contexto.

Desde el punto de vista teórico se ha utilizado a la teoría de las TIC, además de la teoría de la Globalización y se ajusta a la teoría de las brechas digitales (Aguinaga et al., 2014), que se basa en los cambios de mercados y la incorporación de la tecnología como soporte, luego al obtener las conclusiones respectivas en el estudio podrán ser de gran aporte para la comunidad científica y continuar analizado otros contextos y evidenciar como se presenta la gestión del manejo de información.

Finalmente, desde el punto de vista tecnológico, el estudio favorece al investigador porque utiliza los conocimientos técnicos de ingeniería para desarrollar

la propuesta tecnológica, analizar la problemática y establecer las soluciones respectivas.

De lo detallado se propone como objetivo general: determinar la influencia de la implementación ISO 27001:2013 en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023. Con ello se menciona a los objetivos específicos: Primero, determinar la influencia de la implementación ISO 27001:2013 en la disponibilidad de la UGEL Bolognesi; segundo: determinar la influencia de la implementación ISO 27001:2013 en la autenticidad de la UGEL Bolognesi; tercero: Determinar la influencia de la implementación ISO 27001:2013 en la integridad de la UGEL Bolognesi; cuarto: Determinar la influencia de la implementación ISO 27001:2013 en la confidencialidad de la UGEL Bolognesi; quinto: determinar la influencia de la implementación ISO 27001:2013 en la trazabilidad de la UGEL Bolognesi.

Por último, la hipótesis del estudio, como general: La implementación ISO 27001:2013 incide significativamente en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023. De ahí se desprenden las especificas: Primero, la implementación ISO 27001:2013 incide significativamente en la disponibilidad de la entidad. Segundo: la implementación ISO 27001:2013 incide significativamente en la autenticidad de la UGEL Bolognesi. Tercero: la implementación ISO 27001:2013 incide significativamente en la integridad de la UGEL Bolognesi. Cuarta: la implementación ISO 27001:2013 incide significativamente en la confidencialidad de la UGEL Bolognesi. Quinta: la implementación ISO 27001:2013 incide significativamente en la trazabilidad de la UGEL Bolognesi.

II. MARCO TEÓRICO

Córdoba (2021), desarrollo su investigación de posgrado con el propósito de demostrar como la implementación de la ISO 27001:2013 brinda la protección necesaria de una entidad de Colombia, a partir de ello metodológicamente se alinea como experimental porque aplico y evaluó el efecto generado por la ISO en la protección de datos de la entidad, se ha trabajado con una población de 48 trabajadores, para ello se ha llegado a concluir: Los resultados han demostrado que en el pre test se ha tenido una vulnerabilidad de datos del 68.0% y en el post-test se ha reducido a 21.0%, presentando una efectividad del 47.0%, con ello los procesos que presenta la ISO son favorables para que la entidad pueda alcanzar la seguridad requerida y que se garantice el servicio con la protección de información de los usuarios y la entidad, de la misma manera se estableció los lineamientos a seguir en todo el proceso de seguimiento de la información que se accede por los usuarios.

Contero (2019), ejecutó una investigación de nivel de posgrado con la finalidad de implementar políticas de seguridad bajo los lineamientos de la ISO 27001:2013 con el propósito de optimizar el control de la información de una empresa en Quito, para ello se consideró de diseño experimental, presentando un alcance longitudinal, procediendo con la aplicación de técnicas e instrumentos necesarios que le permitieron recopilar la información necesaria, utilizó como población a 67 trabajadores, los resultados han determinado un nivel de vulneración de la información del 56.0%, lo cual se ha reducido en el post-test a 29.0%, presentando un nivel de eficiencia del 47.0%, que le permitió concluir: Según los lineamientos que se establecen en la ISO se ha podido desarrollar las políticas internas necesarias para proteger la intromisión de los sistemas informáticos y el control de los accesos, para ello el personal de informática debe monitorear de manera secuencial como se desarrolla cada uno de estos elementos.

Bornas (2019), exteriorizó su estudio de posgrado con la finalidad de proteger la información de una empresa de Arequipa a través de la implementación de la ISO 27001:2013, durante esa fase del estudio se consideró de diseño experimental, presentando una subcategoría de pre experimental, por contarse con

un solo grupo como muestra, donde participaron 83 trabajadores, dentro de los resultados que se alcanzaron se registró que la información se encontraba expuesta en 64.0%, luego al aplicar la seguridad de la información se ha reducido a 18.0%, alcanzando a mejorar en 46.0%, con ello se ha demostrado la efectividad que se presentó en el estudio, alcanzando a concluir: Se ha mejorado los procesos de la empresa instaurando los protocolos y las directivas necesarias que permitan resguardar la información de la empresa, además se ha implementado algunos mecanismos de control por medio de software como firewall y proxy que ayuden a la protección de información, finalmente se ha concientizado al personal para que adopten las medidas necesarias que resguarden la integridad de datos de la empresa.

Arias (2020), con su estudio de posgrado que se enfocó en implementar la ISO 27001:2013 en una empresa del Callao, para optimizar el manejo de su información, durante la fase metodológica se consideró de diseño experimental, aplicando estrategias que le permitan establecer las directivas de seguridad necesaria que resguarde la información y proteja los datos de la empresa, desarrollada con un alcance longitudinal, la muestra utilizada en el proyecto fue de 38 trabajadores de la empresa, para ello se registró como resultados que antes de aplicar la norma ISO se ha presentado una vulnerabilidad de información de 49.0% y en el post-test se ha reducido en 18.0%, con ello se ha demostrado una afectividad del 31.0%, logrando concluir: Los procesos de proteger a la información de la empresa se basa en la ISO que establece las directrices necesarias que permitan contar con los lineamientos de protección de datos y le brinde las garantías necesarias de confidencialidad de datos, quedando demostrado que la implementación de la ISO y su monitoreo respectivo garantiza la seguridad de la información.

Huerta (2020), desarrolló su estudio de posgrado con la finalidad de implementar políticas de seguridad de la información para resguardar los datos de una empresa de Lima, durante el proceso se consideró de diseño experimental, basado en dos momentos para el análisis de información y demostrando el efecto generado con la implementación, la muestra seleccionada estuvo conformada por

53 trabajadores, mostrando como resultados que la información presentó una vulneración del 43.0%, mientras que los hallazgos del post-test han revelado una vulneración de información del 21.0%, mejorando en 22..0%, logrando concluir: Definir los protocolos de seguridad y transmitirlas al personal es relevante para que se alcance la seguridad necesaria de la integridad de datos, estableciendo las fases necesarias y los controles pertinentes en cada uno de los procesos. Se ha demostrado que la ISO es una herramienta que permite a toda empresa proteger su información con los procedimientos necesarios.

Calderón (2019), presentó su estudio de posgrado con el objetivo de implementar la seguridad de la información por medio de la ISO 27001:2013 y resguardar los datos de una entidad de Lima, durante esta fase del estudio se consideró utilizar el diseño experimental, bajo una categoría pre experimental, la muestra seleccionada en el estudio fue de 41 trabajadores, los resultados han arrojado que durante la etapa evaluativa del estudio se ha registrado una vulneración de la información del 62.0%, luego con la aplicación de la norma ISO se ha reducido en 24.0% en el post-test, alcanzando una mejora del 38.0%, concluyendo que las buenas prácticas de las fases de la ISO favorecen para fortalecer la información de la entidad y brinda los lineamientos para proteger la transmisión de datos internos, además establece la estructura de la red necesaria para garantizar la protección de datos.

Jara (2018), con su estudio de maestría relacionado con la seguridad de la información y la gestión de los procesos de riesgos de una entidad de Perú, donde consideró un diseño experimental, presentando un alcance longitudinal, procediendo con la aplicación de técnicas e instrumentos necesarios que le permitieron recopilar la información necesaria, con una muestra de 55 trabajadores, obtuvo resultados del estudio que fue de 52.0% para el pre test, datos que fueron reducidos en el post-test alcanzando un valor de 27.0%, permitiendo obtener una mejora del 25.0%, que le permitió concluir: Se logro mejorar la seguridad de datos de la entidad a través de la implementación de las directivas que se establecen en la ISO, para ello se ha tenido que realizar las modificaciones necesarias en la

infraestructura de la red y creación de políticas de seguridad que permitan resguardar la información.

Bajo lo mencionado se tiene el fundamento teórico de la variable independiente implementación ISO 27001:2013, es el mundialmente conocido que brinda un marco para los sistemas de control de seguridad de registros (SGSI) para que usted brinde confidencialidad, integridad y disponibilidad persistente de los datos, además del cumplimiento legal. La certificación ISO 27001 es esencial para proteger su propiedad más importante, la información del comprador y del empleado, la foto de la empresa y otra información personal. La norma ISO incluye un método totalmente basado en formas para publicar, implementar, ejecutar y mantener un SGSI (Azán et al., 2017).

Según ISO/IEC, la seguridad de la información se describe como aquellas tácticas, prácticas exactas y metodologías que se buscan para proteger los datos y los sistemas de registros de la entrada, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados. Esta definición esencialmente significa que tenemos que proteger nuestras estadísticas y fuentes de infraestructura de generación de personas que intentarían hacer un mal uso de ellas (Guerra et al., 2021).

ISO 27001 consigue implementarse en diversas formas dentro de la organización, tanto privada o pública, de gran tamaño o pequeñas organizaciones. Está escrito con la ayuda de los mejores profesionales del mundo en el tema y suministra una metodología para efectuar el control estadístico de la seguridad en un empleador. También permite certificar una organización; lo que significa que un marco de certificación independiente confirma que las estadísticas de seguridad se han aplicado en esa empresa de conformidad con la norma ISO 27001 de actualidad (Parada et al., 2018).

El eje significativo de la ISO 27001 es defender la confidencialidad, integridad y disponibilidad de los datos en un empleador. Hace esto con la ayuda de investigar qué problemas de capacidad pueden querer afectar los hechos (es

decir, evaluación de peligros) y luego definir qué se quiere lograr para evitar que ocurran estos inconvenientes (Castillejos et al., 2016).

Las características (o controles) de seguridad que se aplicarán generalmente tienen la forma de políticas, procesos e implementación técnica (como una instancia, un programa de software y un equipo). Bajo la misma línea, en gran parte de los casos, las corporaciones ya se cuentan con todo el programa de hardware y software, pero lo usan de manera insegura; en otras palabras, la mayoría que desarrolla la implementación de ISO 27001 puede estar asociada con la determinación de las reglas organizativas (por ejemplo, la escritura de registros) importantes para evitar infracciones de seguridad (Aguilera et al., 2017).

Con ello se describe que el ciclo de Deming, reconocido también como círculo PDCA o ciclo de desarrollo continuo, se enfoca principalmente en cuatro pasos: la primera es la planificación, luego sigue hacer, además de la tercera fase de verificar y la última etapa es actuar (Plan, Do, Check y Act) (Carvajal et al., 2019). Este modelo adoptado es favorable para que la ISO 27001 se pueda incorporar en una empresa porque brinda los lineamientos necesarios para aplicar las propuestas necesarias.

Planificar (Plan), es considerada como la primera fase donde se montan las tareas esenciales del método para conseguir el efecto final previsto. Al enfocar los movimientos en el resultado final anhelado, la precisión y el acatamiento de las enumeraciones que se deben completar también se convierten en un detalle a mejorar (Lizárraga et al., 2022). Es fundamental: Recolectar datos para profundizar en la pericia del método. Detallar las enumeraciones de los resultados previstos. Conceptualizar las tareas vitales para la consecución de los productos o servicios, verificando las necesidades especificadas. Establecer los objetivos y estrategias vitales para cosechar los efectos importantes de acuerdo con las necesidades del cliente y lineamientos organizacionales (De La Rosa, 2021).

Hacer (Do), con base en los resultados logrados en la fase anterior, lo aprendido se recopila y se pone en funcionamiento. También hay pautas e investigaciones que normalmente sirven para retornar al paso inicial de

Planificación y, por lo tanto, el círculo nunca dejará de fluir. Algunos especialistas ahora eligen llamar a este paso "Ajustar". Esto brinda soporte a los sujetos que son nuevas en el ciclo PDCA a recordar el hecho de que el cuarto paso tiene que ver con el concepto de final del ciclo con comentarios para transmitir las consecuencias hacia los objetivos. Además, este paso "A" no debe ser cuidado con el conjunto de movimientos (implementación) como secuela de la expansión de los planes (que se desenvuelve dentro del 2d paso, "D", de "hacer" o "jugar fuera las acciones") (Martelo et al., 2018).

Controlar o verificar (Check), tras un tiempo premeditado, se recopila y analiza la información de gestión, comparándola con los requisitos exactos de partida, para saber si se han considerado y, en su caso, evaluar si se ha originado o no la mejora prevista. Si la mejora ya no cumple con las expectativas iniciales, deberá modificarse para concordar a los objetivos previstos (Vite et al., 2018).

Actuar (Act), por último, una vez que finaliza el período de verificación, los efectos deben estudiarse y compararse con el rendimiento general de los deportes antes de que se implemente el desarrollo. Si los resultados son los mejores, el desarrollo podría llevarse a cabo definitivamente, y si ya no lo es, será importante determinar si se deben hacer cambios para modificar los resultados o si se debe descartar. Una vez que se completa el paso 4, el paso uno debe retroceder periódicamente para ver las nuevas mejoras que se aplicarán (Valencia, 2018).

Un sistema de gestión de la seguridad de la Información (SGSI) consiste en el diseño, implementación y renovación de un sólido y rápido proceso para administrar de manera correcta y eficaz el acceso a los registros, investigando conservar estadísticas de primer nivel que incluyan confidencialidad, integridad y seguridad. Luego se presenta a la disponibilidad de propiedad de los hechos, buscando continuamente para disminuir los peligros de seguridad (Torres, 2020).

La optima gestión de la protección de la información indaga el establecimiento y preservación de aplicaciones, controles y lineamientos, los cuales pueden estar destinados a mantener la confidencialidad, integridad y disponibilidad

de los datos, si alguna de esas particularidades falla no es nada positivo (Sánchez y Ledesma, 2021).

Confidencialidad: Imposibilita la propaganda de estadísticas a personas, entidades o enfoques no acreditados. En otras palabras, afirma el acceso a la información solo a aquellos individuos que tienen el permiso adecuado (Saltos et al., 2020).esto implica que la información está disponible mejor a través de los mecanismos de transmisión, los cuales son lo que utilizan la información con la que se encuentra almacenada en la entidad. Esto es lo que se llama necesidad de protección de datos. Con este plazo, se hace referencia de que los hechos han de ser más efectivos respecto de las personas, entidades o estructuras jurídicas a las que se les otorga derecho de entrada. Ejemplos de violaciones de la confidencialidad son el robo de registros privados por parte de un atacante por medio de Internet, la divulgación no autorizada de registros personales por medio de las redes sociales o el acceso por parte de un trabajador a datos esenciales de la organización ubicados en carpetas sin permisos asignados, que debe ya no tiene derecho de entrada (Peñafiel, 2021).

Integridad: indaga mantener los datos libres de transformaciones no autorizadas, integridad es preservar correctamente la información tal como se genera, sin que sea maniobrada o sobresaltada por personas o medios no acreditados (Moreira, 2017). El aporte que se proporciona es que se mantiene la integridad de datos de la empresa, estableciendo las políticas necesarias que garanticen la protección y se cuente con el respaldo necesario de los datos.

La integridad de los registros se refiere a la verdad de que los hechos son correctos y libres de transformaciones y errores. Además, la información puede ser trastornada deliberadamente o errónea y también conseguimos basar nuestras disposiciones en ella. Modelos de vulneración contra la integridad de los datos son, la alteración malintencionada de archivos de dispositivos informáticos mediante la explotación de una debilidad o la transformación de un imperfecto de ventas por parte de un empleado que pretende dañar la información de la empresa o por un error humano (Montenegro et al., 2017).

Disponibilidad: La disponibilidad es el camino a la información y los sistemas a través de personas jurídicas en el momento en que lo requieran (Machicao, 2018). Frente a eso, considero importante que la data que maneja la UGEL Bolognesi se encuentre disponible las 24 horas del día para que se garantice y se confié en la gestión de datos presenta la disponibilidad requerida por los usuarios.

La disponibilidad de la información se refiere a que los registros estén disponibles mientras los necesitemos. Algunos ejemplos de indisponibilidad de datos son: cuando no nos es posible consentir al correo electrónico de la empresa debido a errores de distribución, o cuando se soporta un ataque de denegación de operador, en el que el dispositivo se "cuelga" impidiendo el acceso válido. Ambos tienen implicaciones graves para la seguridad de la información (Llanos, 2018).

La seguridad influye en todos los factores de una agencia. Lograr una seguridad integral para una máquina o conjunto de estructuras requiere: seguridad física, seguridad tecnológica y pautas y tácticas precisas. Tener dos de estas 3 variedades de seguridad no es suficiente para garantizar un grado suficiente de seguridad (Iturralde y Duque, 2021).

Seguridad de aplicaciones: Un servidor de Internet es un ejemplo de un software que puede verse afectado por problemas de protección. El servidor de Internet es un excelente ejemplo cuando se trata de instalar un escenario para revelar posibles vulnerabilidades en el nivel del software. Supongamos, por ejemplo, que un servidor se ha configurado para permitir el acceso a archivos cruciales solo para ciertos usuarios. En este escenario, si puede haber un programa malicioso dentro de la forma en que se determina la identificación de una persona, un atacante debería acceder a esos archivos (Guevara, 2017).

Seguridad del Sistema Operativo: son considerados como firewall, encargados de proporcionar al sistema todas las condiciones requeridas para que no sea vulnerada. Los fabricantes arrojan habitualmente parches y modernización para restaurar los inconvenientes detectados. Si un dispositivo operativo no está

bien parcheado, un atacante debería aprovechar una vulnerabilidad a pesar de un servidor web relajado, ya que un servidor delega en el sistema operativo varias funciones (Cueva y Alvarado, 2017).

Seguridad de la red: La capa de red es igualmente crítica. Debe asegurarse de que los paquetes legítimos más efectivos puedan enviarse en sus programas o estructuras en ejecución. Los visitantes maliciosos generalmente consisten en paquetes de datos que contienen secuencias que, interpretadas mediante el uso de software propenso, producen efectos repentinos para la persona y pueden razonar todo, desde un bloqueo de la máquina para obtener acceso a información privilegiada. Los cortafuegos y los IDS son dos estilos de herramientas que se pueden utilizar para hacer frente a este tráfico indudablemente malicioso (Carrasco, 2021).

La seguridad de la información es un tema importante para la era en la que los registros de innumerables personas y grupos se guardan en una variedad de sistemas informáticos, por lo general fuera de nuestro control directo. Cuando se habla de la seguridad de los datos de forma generalizada, es muy importante comprender que la seguridad y la productividad suelen ser ideas diametralmente adversas, y ser capaz de señalar exactamente cuándo nos sentimos cómodos es una tarea difícil (Castillo y Pérez, 2017). Luego se tiene el fundamento de la variable dependiente gestión del manejo de información, El conjunto de actividades que se realizan con el motivo de obtener, procesar, almacenar y, tarde o temprano, mejorar, de manera adecuada, la información que ésta produce o adquiere en una empresa y que permite el desarrollo de su interés (Benussi, 2020).

La información es un duro y rápido de las estadísticas convertidas de manera que contribuye a reducir la incertidumbre del futuro y, en consecuencia, permite la toma de decisiones. Los hechos representan las estadísticas convertidas de manera significativa para el individuo que lo recibe, es decir, tiene una tarifa real o percibida por sus selecciones y por sus movimientos. Así, los registros son información que ha sido interpretada y comprendida por el destinatario del mensaje. La datación entre estadísticas y hechos es igual a la que existe entre materia prima

y producto terminado (Abrego et al., 2020). La información es la pericia y el conocimiento de los hechos por parte del receptor. La información reduce la incertidumbre y proporciona al receptor algo que ya no reconoce (Florencia, 2012). Al mencionar a la información se debe tener claro que se requiere todas las medidas de seguridad para contar con los respaldos necesarios que garantice el respaldo de la información. Vela et al. (2019), menciona que aplicar seguridad a los servidores es una labor informática que resguarda la información de toda entidad y garantiza que no se vulneren los accesos.

Para seleccionar las dimensiones que corresponden a la variable gestión de datos se detalla lo expresado por el Instituto Nacional de Ciberseguridad de España (2020), detallando lo siguiente:

La primera dimensión se denomina disponibilidad: Se refiere a asegurarse de que el usuario pueda conceder acceso a las fuentes cuando lo requiera. La segunda dimensión se denomina autenticidad: Se especializa en presentar las garantías de las tácticas de autenticación y permite tener acceso a controlar para que el personal legal más cercano pueda tener acceso a los hechos. La tercera dimensión se denomina integridad: Se basa principalmente en salvaguardar la exactitud y exhaustividad de la información, detectando cualquier variación intencionada o no intencionada en el transporte de datos. La cuarta dimensión se denomina confidencialidad: Garantiza que las estadísticas guardadas por la persona o en tránsito en el transporte de datos no puedan ser leídas por personas no autorizadas. La quinta dimensión se denomina trazabilidad: Se montan los métodos y componentes para suministrar los registros vitales que faciliten realizar un análisis de seguridad (Instituto Nacional de Ciberseguridad de España, 2020).

La información es un factor crítico para la organización en la medida en que la propiedad o no de los datos correctos va a ser un componente determinante en el placer de las elecciones que se puedan adoptar y, por tanto, dentro del método que se pueda diseñar en un momento dado y luego puesto en práctica (Flores et al., 2007).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Según las particularidades que presentó el estudio se consideró de tipo aplicada, conceptualizada por Hernández y Mendoza (2018), como estudios que recopilan información de diversas fuentes para sustentar a las variables y por medio de los autores desarrollar el fundamento necesario del estudio y brindar la solución necesaria a la problemática presentada.

Bajo ello se tiene el enfoque que presentó es cuantitativo descrito por Baena (2017), como estudio que se enfocan en dar a conocer resultados por medio de datos estadísticos que permitan interpretar la percepción de la variable dependiente en el pre y post-test.

Según el diseño es preexperimental, desarrollada por Salgado (2018), como estudio que se basan en la manipulación de la variable independientes desarrollando estrategias y actividades que permitan ver el efecto que genera en la variable dependiente en dos momentos. Dentro de ello, se consideró como pre experimental, basada en Concepción et al. (2019), como estudios que presentan una muestra de estudio, el cual se evalúa en dos momentos, considerados como longitudinal, analizada antes y después de la aplicación del estímulo que es la variable independiente.

El esquema es:

$$G: \quad O_{Y_1} \longrightarrow X \longrightarrow O_{Y_2}$$

Dónde:

G : Grupo de estudio

O_{Y_1} : Observación de la gestión del manejo de información (Fase de diagnóstico)

O_{Y_2} : Observación de la gestión del manejo de información (Fase evaluativa)

X : Aplicación de la seguridad de la información (ISO 27001)

3.2. Variables y operacionalización

Variable independiente: Seguridad de la información (ISO27001)

De manera conceptual: Según ISO/IEC, la seguridad de la información se describe como aquellas tácticas, prácticas exactas y metodologías que se buscan para proteger los datos y los sistemas de registros de la entrada, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados. Esta definición esencialmente significa que tenemos que proteger nuestras estadísticas y fuentes de infraestructura de generación de personas que intentarían hacer un mal uso de ellas (Guerra et al., 2021).

De manera operacional: Es la aplicación de la norma ISO27001, en sus diversas etapas y ver el efecto que genera en la gestión de la información de la Ugel Bolognesi, para ello se detallan los parámetros necesarios para aplicación (Ver anexo 01).

Variable dependiente: Gestión del manejo de información

De manera conceptual: El conjunto de actividades que se realizan con el motivo de obtener, procesar, almacenar y, tarde o temprano, mejorar, de manera adecuada, la información que ésta produce o adquiere en una empresa y que permite el desarrollo de su interés.

De manera operacional: Es el análisis de la percepción de los trabajadores de la Ugel Bolognesi sobre la gestión de la información por medio de un instrumento elaborado en base a las dimensiones detalladas en el marco teórico, presentando opciones de respuestas de tipo Likert y analizada por medio de una escala ordinal (Ver Anexo 01).

Indicadores: La dimensión disponibilidad**,** presentó como indicadores al acceso a la información durante las 24 horas del día, la estabilidad de la red, luego a la capacidad tecnológica y al ancho de banda. Referente a la dimensión autenticidad presentó como indicadores a la política de seguridad, luego al control de los usuarios, además a la administración de los equipos y a la vulneración de

información. Respecto a la dimensión integridad ha presentado como indicadores a las copias de seguridad, luego a la asistencia técnica y la forma de administrar los sistemas. Al detallar a la dimensión confidencialidad se ha mostrado como indicadores a la protección de datos, luego a los privilegios de acceso y a las políticas institucionales. Finalmente, respecto a la dimensión trazabilidad se ha reflejado como indicadores al seguimiento de los procesos y el rastreo de los usuarios.

Escala de medición: Según las particularidades que presenta el estudio se ha considerado una escala ordinal de tipo deficiente, regular y eficiente para poder realizar el análisis descriptivo del estudio.

3.3. Población, muestra y muestreo

La población en el estudio la conforman 47 trabajadores de la institución. La definición que se presenta es que la población es considerada como el total de sujetos que se ubican bajo un contexto de problemática y a través de las experiencias de contienen, responden a instrumentos que ayudan a explicar los sucesos presentados (Carhuancho et al., 2019).

Criterios de inclusión: Durante esta etapa del estudio se ha considerado a todo personal que presenta una permanencia superior a 6 meses en la entidad.
Criterios de exclusión: Se ha tomado en cuenta a todo el personal que labore menos de 6 meses en la entidad.

De ello se tiene como muestra A 42 trabajadores por presentar una proporción con marco muestral, donde se tuvo que emplear métodos estadísticos para definir el tamaño de la muestra (Cabezas et al., 2018). Finalmente, el muestreo aplicado en el desarrollo del estudio es el probabilístico, aleatorio simple, llevado a cabo con el cálculo del tamaño de la muestra a través de una fórmula estadística y colocada como anexo (Cohen y Gómez, 2019).

3.4. Técnicas e instrumentos de recolección de datos

Técnica, en el estudio se consideró como técnica a la encuesta, con el cual se logró recoger la información requerida a través de su instrumento el cuestionario. Jiménez (2020), define a la encuesta como una manera de recoger información por medio de opiniones, realizadas de manera física o digital, a través de las experiencias que presenten los sujetos que conforman la muestra.

Instrumento, en el estudio se utilizó el cuestionario estructurado, presentando opciones politómicas, de tipo Likert, permitiendo categorizar las opiniones y cuantificar, logrando ser representadas en tablas estadísticas (Montalván et al., 2019).

Durante el análisis del pre y del post-test se ha utilizado el cuestionario de gestión del manejo de la información el cual se detalla en el siguiente texto.

El instrumento presenta 24 ítems, el cual se encuentra segmentado en 5 dimensiones, la primera dimensión se denomina disponibilidad, que conforma a los ítem del 1 al 5, luego se encuentra la dimensión autenticidad que se integra por los ítems del 6 al 10, además de ello se incorpora a la dimensión integridad que se conforma por los ítems del 11 al 15, luego se presenta a la dimensión confidencialidad que se conforma por los ítem del 16 al 20 y finalmente se tiene a la dimensión trazabilidad que corresponde a los ítems del 21 al 24. Todas las interrogantes presentan 5 alternativas de respuestas estructuradas bajo una escala Likert que va desde nunca con una puntuación de 1, luego se encuentra a veces con una puntuación de 2, continua con a veces con una puntuación de 3, luego se presenta a casi siempre con una puntuación de 4 y finalmente se ubica a siempre con una puntuación de 5. Todo el análisis se desarrolla bajo una escala ordinal que es deficiente con un intervalo de 24 s 56, luego se encuentra a regular con un intervalo que va desde 57 a 88 y de eficiente que va con una puntuación de 89 a 120.

Validez, en el estudio se va a seleccionar a 3 ingenieros con maestría o doctorado para que evalúen el instrumento y puedan certificar a través de la matriz

de validación si el instrumento cumple con las condiciones necesarias para ser aplicado a los trabajadores de la entidad que conforman la muestra.

Confiabilidad, se desarrolló a través de la selección de una muestra piloto, luego se les aplicó el instrumento para ser analizados por medio del alfa de Cronbach y determinar si es confiable, para ello la muestra piloto se conforma por 15 trabajadores que no pertenezcan al estudio, pero deben cumplir el requisito de presentar similares características. De acuerdo a los resultados alcanzados en el estudio se ha logrado obtener una confiabilidad de 0.859, lo cual indica que el instrumento es confiabilidad y se puede aplicar al estudio.

3.5. Procedimiento

Dentro de los procesos que involucran al estudio se tiene a la selección de la institución donde aplicar el estudio, luego realizar el análisis de la existencia de una determinada problemática para determinar y seleccionar a las variables a desarrollar; con ello se presentó una carta, solicitando el acceso a la información y el contacto con los trabajadores para recoger las opiniones. Con la aceptación del estudio se procederá a coordinar las reuniones requeridas para el recojo de datos, luego se procesarán con técnicas estadísticas, permitiendo obtener conclusiones que faciliten el análisis del estudio.

3.6. Método de análisis de datos

Durante esta etapa del estudio se utilizaron los programas de Excel 2021 y el SPSS 26.0, para organizar las opiniones recogidas por medio de los instrumentos y realizar el procesamiento necesario para responder a los objetivos del estudio.

La primera fase se fundamenta en el análisis descriptivo, que se presenta por medio de la presentación de tablas y figuras de frecuencia.

La segunda etapa del estudio presentó su fundamento con el análisis inferencial, iniciando con una prueba de normalidad para conocer la distribución que presenta la muestra por medio del método de Shapiro-Wilk por ser una muestra menor a 50, luego de conocer la distribución se utilizó el método inferencia según

la distribución presentada, T de Student si es paramétrico y Wilcoxon si es no paramétricos, métodos utilizados para determinar el efecto que presentó una variable sobre la otra.

3.7. Aspectos éticos

Para analizar el desarrollo del estudio se ha considerado la autenticad como principal aspecto ético, porque el estudio basa en recoger información que permita sustentar a las variables y dar a conocer las fuentes pertinentes que favorezcan al desarrollo del estudio, por otro lado, se tiene que, al consentimiento informado, desarrollado como una inducción a los trabajadores para darles a conocer la importancia de sus opiniones y que respondan con la serenidad del caso, de la misma manera se consideró al respeto, puesto que no se interviene ni manipula las opiniones.

IV. RESULTADOS

Para poder desarrollar el análisis de los resultados se ha tenido que aplicar el instrumento de la gestión del manejo de la información en dos etapas, la primera se basa en el pre test y la segunda en el post-test, desarrollado en el tiempo que duran la aplicación de la ISO 27001:2013.

Como soporte se ha utilizado los programas del Excel 2021, donde se ha desarrollado la organización de las opiniones del instrumento por medio de una escala Likert, presentando 5 alternativas como respuesta, además se ha realizado la sumatoria de los ítems por dimensiones para poder realizar el análisis por dimensión y variable.

La escala que se ajustado a la finalidad que presentó el estudio es la ordinal de tipo deficiente, regular y eficiente, en conjunto a los intervalos calculados. La primera etapa del estudio consiste en mostrar los niveles alcanzados por medio de la estadística descriptiva.

En el caso de la comprobación de la hipótesis se ha desarrollado una prueba de normalidad por medio del método de Shapiro-Wilk, considerado para muestras que presenten un tamaño menor a 50, ello se refuerza con lo demostrado por Galindo (2020), en conjunto de Flores et al. (2021), han detallado lo mencionado. Con la prueba realizada se conoció la distribución que presenta la muestra y se seleccionó los métodos paramétricos y no paramétricos más adecuados para el estudio.

4.1. Análisis descriptivo

Variable dependiente: Gestión del manejo de información

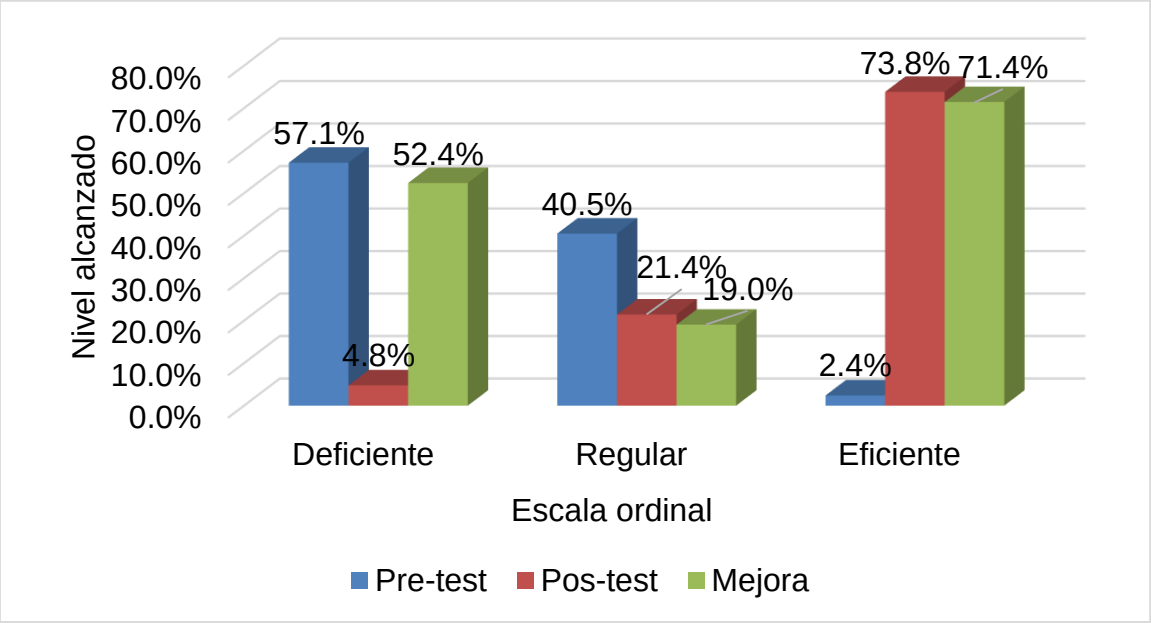
Tabla 1

Niveles de la gestión del manejo de información en la UGEL Bolognesi durante el pre-test y post-test.

Nivel	Pre-test		Post-test		Mejora	
	fi	%	fi	%	fi	%
Deficiente	24	57.1%	2	4.8%	22	52.4%
Regular	17	40.5%	9	21.4%	8	19.0%
Eficiente	1	2.4%	31	73.8%	30	71.4%
Total	42	100.0%	42	100.0%		

Figura 2

Barra de la gestión del manejo de información en la UGEL Bolognesi durante el pre-test y post-test.



Por medio de las valoraciones registradas en la tabla, se ha dado a conocer las medidas estadísticas presentadas en el desarrollo del estudio, encontrando que el nivel deficiente de la gestión del manejo de la información se ha percibido con una variación del 52.4%, quedando demostrado que la implementación de la ISO 27001:2013 ha presentado una mejora, ello se sustenta con la comparación realizada del valor registrado en el pre-test con 57.1% y siendo comparado con lo evidenciado en el post-test con 4.8%. Respecto al valor alcanzado para el nivel regular sobre el manejo de la información se ha reflejado una variación registrada del 19.0%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 40.5% y siendo comparado con lo evidenciado en el post-test con 21.4%. Por último, al analizar las valoraciones registradas para el nivel eficiente se ha dado a conocer que el manejo de la información ha reflejado una variación del 71.4%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 2.4% y siendo comparado con lo evidenciado en el post-test con 73.8%.

Dimensión 1: Disponibilidad

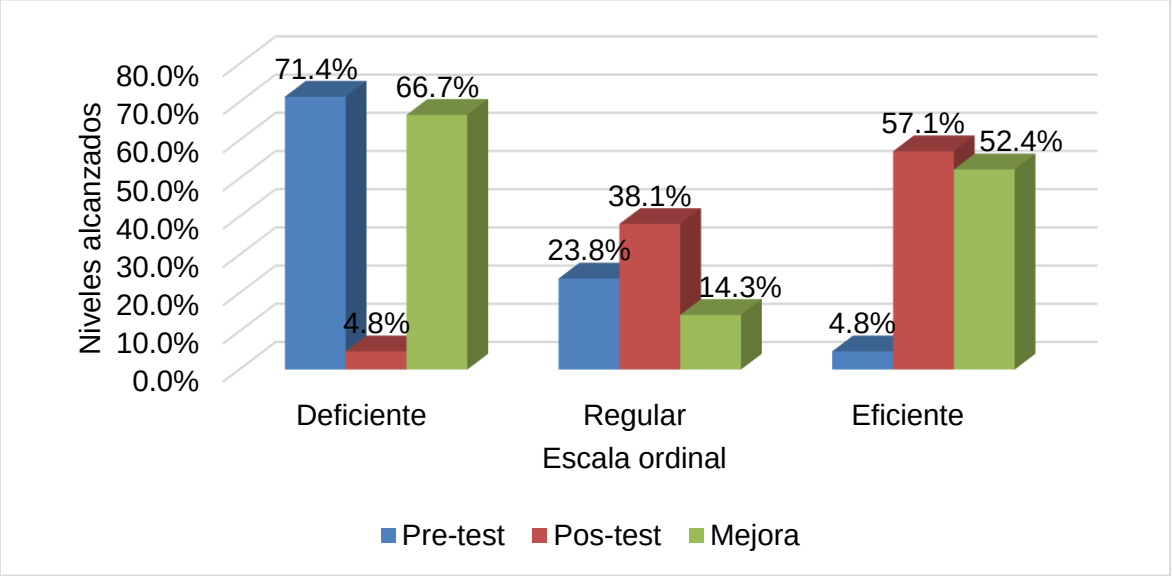
Tabla 2

Niveles de la disponibilidad en la UGEL Bolognesi durante el pre-test y post-test.

Nivel	Pre-test		Post-test		Mejora	
	fi	%	fi	%	fi	%
Deficiente	30	71.4%	2	4.8%	28	66.7%
Regular	10	23.8%	16	38.1%	6	14.3%
Eficiente	2	4.8%	24	57.1%	22	52.4%
Total	42	100.0%	42	100.0%		

Figura 3

Barra de la disponibilidad en la UGEL Bolognesi durante el pre-test y post-test.



Por medio de las valoraciones registradas en la tabla se ha dado a conocer las medidas estadísticas presentadas en el desarrollo del estudio, encontrando que el nivel deficiente de la disponibilidad se ha percibido con una variación del 66.7%, quedando demostrado que la implementación de la ISO 27001:2013 ha presentado una mejora, sustentada con la comparación realizada del valor registrado en el pre-test con 71.4% y siendo comparado con lo evidenciado en el post-test con 4.8%. Respecto al valor alcanzado para el nivel regular sobre la disponibilidad se ha reflejado una variación registrada del 14.3%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 23.8% y siendo comparado con lo evidenciado en el post-test con 38.1%. Por último, al analizar las valoraciones registradas para el nivel eficiente se ha dado a conocer que la disponibilidad, ha reflejado una variación del 52.4%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 4.8% y siendo comparado con lo evidenciado en el post-test con 57.1%.

Dimensión 2: Autenticidad

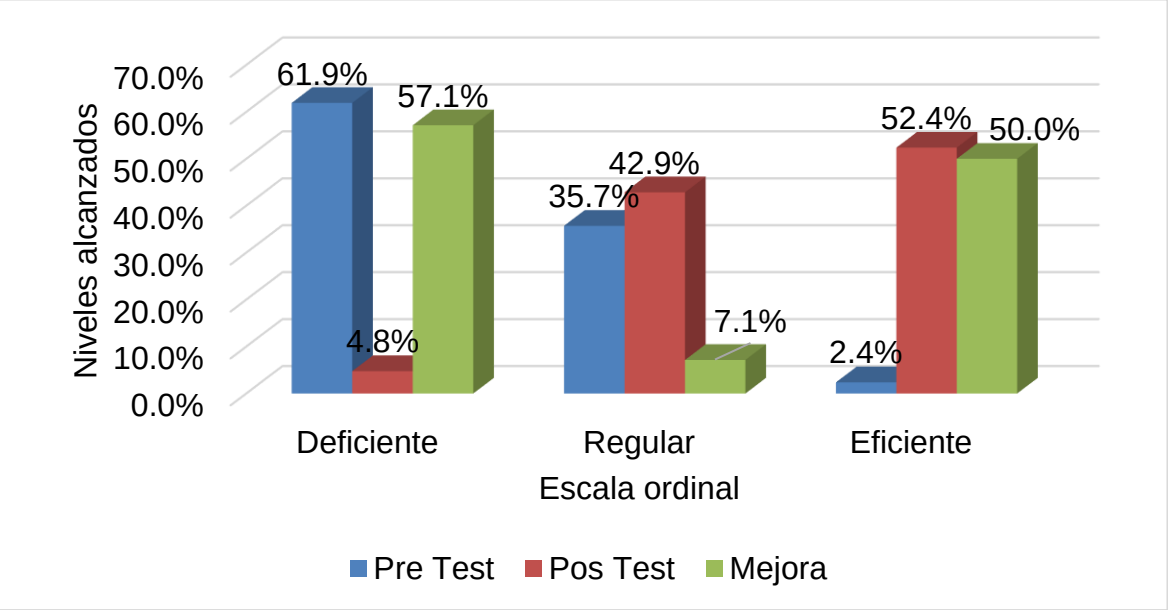
Tabla 3

Niveles de la autenticidad en la UGEL Bolognesi durante el pre-test y post-test.

Nivel	Pre-test		Post-test		Mejora	
	fi	%	fi	%	fi	%
Deficiente	26	61.9%	2	4.8%	24	57.1%
Regular	15	35.7%	18	42.9%	3	7.1%
Eficiente	1	2.4%	22	52.4%	21	50.0%
Total	42	100.0%	42	100.0%		

Figura 4

Barra de la autenticidad en la UGEL Bolognesi durante el pre-test y post-test.



Por medio de las valoraciones registradas en la tabla se ha dado a conocer las medidas estadísticas presentadas en el desarrollo del estudio, encontrando que el nivel deficiente de la autenticidad se ha percibido con una variación del 57.1%, quedando demostrado que la implementación de la ISO 27001:2013 ha presentado una mejora, sustentada con la comparación realizada del valor registrado en el pre-test con 61.9% y siendo comparado con lo evidenciado en el post-test con 4.8%. Respecto al valor alcanzado para el nivel regular sobre la disponibilidad se ha reflejado una variación registrada del 7.1%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 35.7% y siendo comparado con lo evidenciado en el post-test con 42.9%. Por último, al analizar las valoraciones registradas para el nivel eficiente se ha dado a conocer que la disponibilidad, ha reflejado una variación del 50.0%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 2.4% y siendo comparado con lo evidenciado en el post-test con 52.4%.

Dimensión 3: Integridad

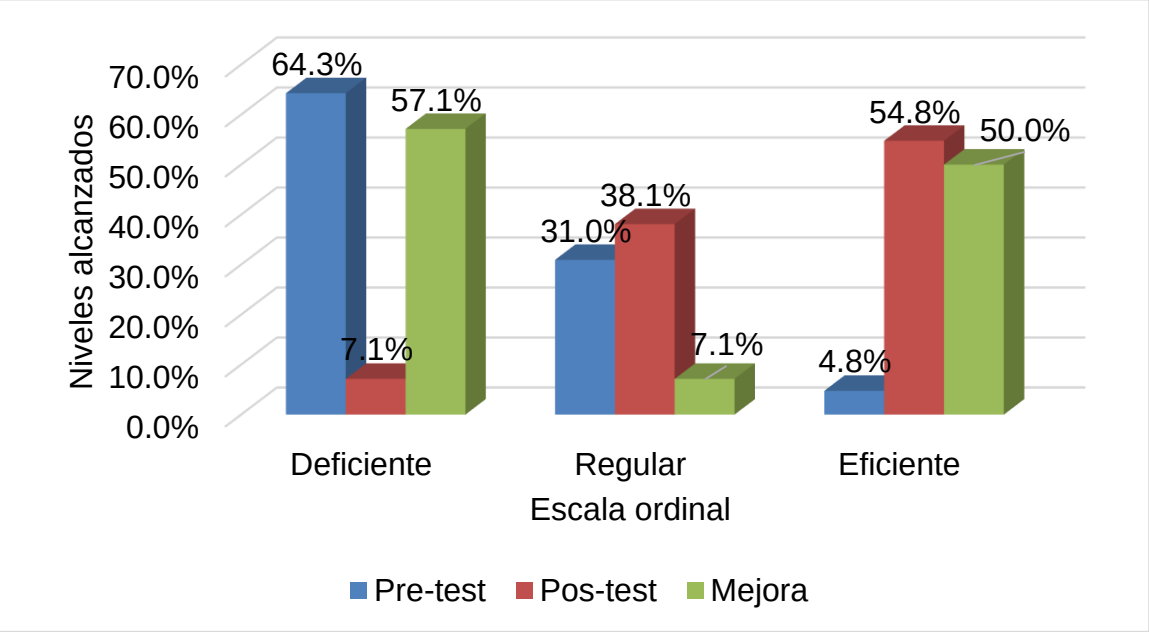
Tabla 4

Niveles de la integridad en la UGEL Bolognesi durante el pre-test y post-test.

Nivel	Pre-test		Post-test		Mejora	
	fi	%	fi	%	fi	%
Deficiente	27	64.3%	3	7.1%	24	57.1%
Regular	13	31.0%	16	38.1%	3	7.1%
Eficiente	2	4.8%	23	54.8%	21	50.0%
Total	42	100.0%	42	100.0%		

Figura 5

Barra de la integridad en la UGEL Bolognesi durante el pre-test y post-test.



Por medio de las valoraciones registradas en la tabla se ha dado a conocer las medidas estadísticas presentadas en el desarrollo del estudio, encontrando que el nivel deficiente de la integridad se ha percibido con una variación del 57.1%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 64.3% y siendo comparado con lo evidenciado en el post-test con 7.1%. Respecto al valor alcanzado para el nivel regular sobre la integridad se ha reflejado una variación registrada del 7.1%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 31.0% y siendo comparado con lo evidenciado en el post-test con 38.1%. Por último, al analizar las valoraciones registradas para el nivel eficiente se ha dado a conocer que la integridad, ha reflejado una variación del 50.0%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 4.8% y siendo comparado con lo evidenciado en el post-test con 54.8%.

Dimensión 4: Confidencialidad

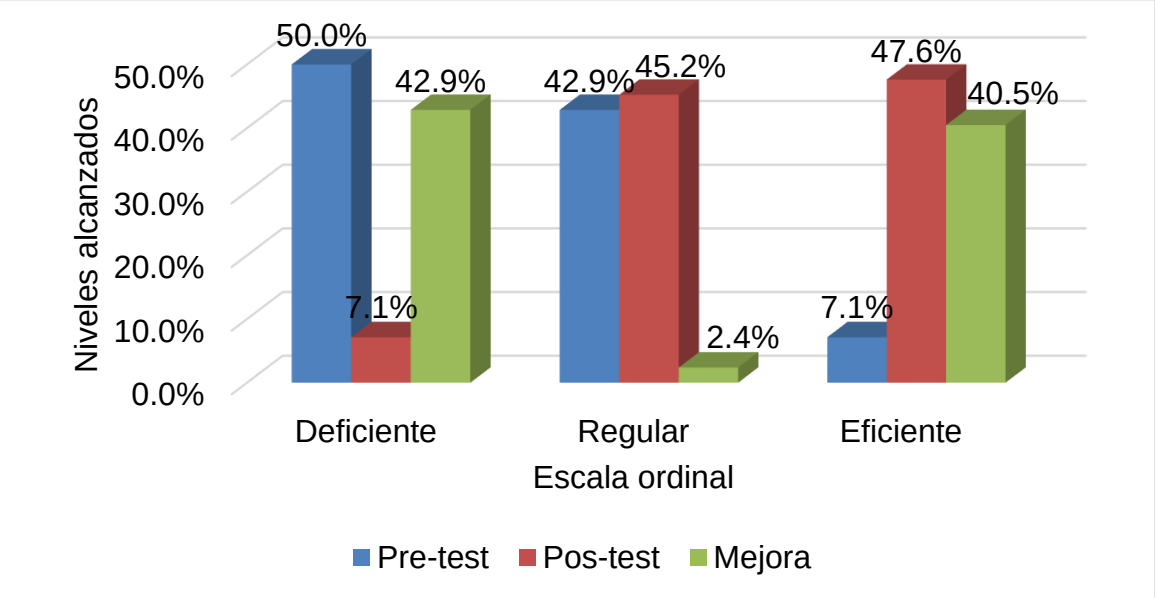
Tabla 5

Niveles de la confidencialidad en la UGEL Bolognesi durante el pre-test y post-test.

Nivel	Pre-test		Post-test		Mejora	
	fi	%	fi	%	fi	%
Deficiente	21	50.0%	3	7.1%	18	42.9%
Regular	18	42.9%	19	45.2%	1	2.4%
Eficiente	3	7.1%	20	47.6%	17	40.5%
Total	42	100.0%	42	100.0%		

Figura 6

Barra de la confidencialidad en la UGEL Bolognesi durante el pre-test y post-test.



Por medio de las valoraciones registradas en la tabla se ha dado a conocer las medidas estadísticas presentadas en el desarrollo del estudio, encontrando que el nivel deficiente de la confidencialidad se ha percibido con una variación del 42.9%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 50.0% y siendo comparado con lo evidenciado en el post-test con 7.1%. Respecto al valor alcanzado para el nivel regular sobre la confidencialidad se ha reflejado una variación registrada del 2.4%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 42.9% y siendo comparado con lo evidenciado en el post-test con 45.2%. Por último, al analizar las valoraciones registradas para el nivel eficiente se ha dado a conocer que la confidencialidad, ha reflejado una variación del 40.5%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 7.1% y siendo comparado con lo evidenciado en el post-test con 47.6%.

Dimensión 5: Trazabilidad

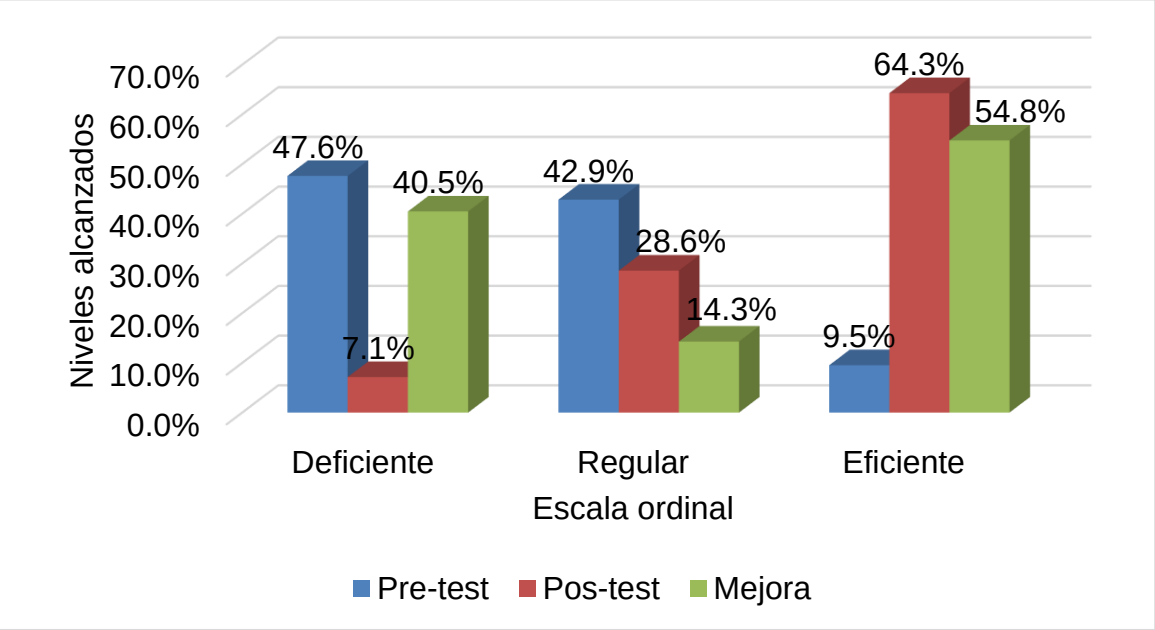
Tabla 6

Niveles de la trazabilidad en la UGEL Bolognesi durante el pre-test y post-test.

Nivel	Pre-test		Post-test		Mejora	
	fi	%	fi	%	fi	%
Deficiente	20	47.6%	3	7.1%	17	40.5%
Regular	18	42.9%	12	28.6%	6	14.3%
Eficiente	4	9.5%	27	64.3%	23	54.8%
Total	42	100.0%	42	100.0%		

Figura 7

Barra de la trazabilidad en la UGEL Bolognesi durante el pre-test y post-test.



Por medio de las valoraciones registradas en la tabla se ha dado a conocer las medidas estadísticas presentadas en el desarrollo del estudio, encontrando que el nivel deficiente de la trazabilidad se ha percibido con una variación del 40.5%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 47.6% y siendo comparado con lo evidenciado en el post-test con 7.1%. Respecto al valor alcanzado para el nivel regular sobre la trazabilidad se ha reflejado una variación registrada del 14.3%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 42.9% y siendo comparado con lo evidenciado en el post-test con 28.6%. Por último, al analizar las valoraciones registradas para el nivel eficiente se ha dado a conocer que la trazabilidad, ha reflejado una variación del 54.8%, quedando demostrado que la implementación de la ISO 27001:2013 ha mejorado, sustentada con la comparación realizada del valor registrado en el pre-test con 9.5% y siendo comparado con lo evidenciado en el post-test con 64.3%.

4.2. Análisis inferencial y comprobación de la hipótesis propuesta

Normalidad: Durante esta etapa del estudio se ha dado a conocer los resultados presentado del método de Shapiro-Wilk, con la finalidad de demostrar la distribución que presenta la muestra, mencionando a lo siguiente:

Tabla 7

Distribución de la muestra

Dimensión / Variable	Análisis	Shapiro-Wilk				
		Estadístico	gl	Sig.	Prom. Sig.	Distribución
VD: Gestión del manejo de información	Pre Test	,779	42	,000	0.000	No paramétrica
	Post-Test	,817	42	,000		
D1: Disponibilidad	Pre Test	,802	42	,000	0.000	No paramétrica
	Post-Test	,828	42	,000		
D2: Autenticidad	Pre Test	,875	42	,000	0.075	Paramétrica
	Post-Test	,960	42	,149		
D3: Integridad	Pre Test	,869	42	,000	,000	No paramétrica
	Post-Test	,862	42	,000		
D4: Confidencialidad	Pre Test	,913	42	,004	0.025	No paramétrica
	Post-Test	,892	42	,001		
D5: Trazabilidad	Pre Test	,816	42	,000	0.005	No paramétrica
	Post-Test	,927	42	,010		
Paramétrica	Sig. >0.05		No paramétrica			Sig. <=0.05

De acuerdo a las valorizaciones alcanzadas en el estudio se ha demostrado la distribución que presentan las dimensiones y la variable, detallando lo siguiente:

Para la variable gestión del manejo de la información se ha registrado un promedio de sig. = 0.000, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Al mencionar a la dimensión disponibilidad se ha registrado un promedio de sig. = 0.000, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Respecto a la dimensión autenticidad se ha registrado un promedio de sig. = 0.075, que al ser contrastados con el margen del 0.05, se afirma que es superior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es T de Student.

Referente a la dimensión integridad se ha registrado un promedio de sig. = 0.000, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Respecto a la dimensión confidencialidad se ha registrado un promedio de sig. = 0.025, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Al mencionar a la dimensión trazabilidad se ha registrado un promedio de sig. = 0.005, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Prueba de hipótesis

Resultado para la hipótesis general:

Hi: La implementación ISO 27001:2013 incide significativamente en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023.

Ho: La implementación ISO 27001:2013 no incide significativamente en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023.

Para la variable gestión del manejo de la información se ha registrado un promedio de sig. = 0.000, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Tabla 8

Prueba de Wilcoxon – indicador de nivel de confiabilidad

		N	Rango promedio	Suma de rangos
Post-Test de teletrabajo - Pre Test de teletrabajo	Rangos negativos	3[a]	13,50	40,50
	Rangos positivos	39[b]	22,12	862,50
	Empates	0[c]		
	Total	42		

a. Post-test de teletrabajo < Pre-Test de gestión del manejo de información

b. Post-test de teletrabajo > Pre-Test de gestión del manejo de información

c. Post-test de teletrabajo = Pre-Test de gestión del manejo de información

A través del análisis reflejado en la tabla se ha podido dar a conocer los valores de rango y sumatoria son significativos, al presentar un rango de 22.12 y suma de 862.50, con un rango positivo 4[b] que presenta b. Post-test de teletrabajo > Pre-test de gestión del manejo de información.

Tabla 9

Prueba de hipótesis para la implementación ISO 27001:2013 en la gestión del manejo de información

	Post-test de gestión del manejo de información – Pre-Test de gestión del manejo de información
Z	-5,140[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido de la prueba de rango de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023.

Resultado para la hipótesis específica 1:

Hi: La implementación ISO 27001:2013 incide significativamente en la disponibilidad de la entidad.

Ho: La implementación ISO 27001:2013 no incide significativamente en la disponibilidad de la entidad.

Al mencionar a la dimensión disponibilidad se ha registrado un promedio de sig. = 0.000, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Tabla 10

Prueba de Wilcoxon – indicador de nivel de confiabilidad

		N	Rango promedio	Suma de rangos
Post-Test de disponibilidad - Pre Test de disponibilidad	Rangos negativos	4[a]	5,63	22,50
	Rangos positivos	38[b]	23,17	880,50
	Empates	0[c]		
	Total	42		

a. Post-test de disponibilidad < Pre-Test de disponibilidad

b. Post-test de disponibilidad > Pre-Test de disponibilidad

c. Post-test de disponibilidad = Pre-Test de disponibilidad

A través del análisis reflejado en la tabla se ha podido dar a conocer los valores de rango y sumatoria son significativos, al presentar un rango de 23.17 y suma de 880.50, con un rango positivo 4[b] que presenta b. Post-test de disponibilidad > Pre-test de disponibilidad.

Tabla 11

Prueba de hipótesis para la implementación ISO 27001:2013 en la disponibilidad

	Post-test de disponibilidad – Pre-Test de disponibilidad
Z	-5,372[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido de la prueba de rango de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la

implementación ISO 27001:2013 incide significativamente en la disponibilidad en la UGEL Bolognesi Ancash 2023.

Resultado para la hipótesis específica 2:

Hi: La implementación ISO 27001:2013 incide significativamente en la autenticidad de la UGEL Bolognesi.

Ho: La implementación ISO 27001:2013 no incide significativamente en la autenticidad de la UGEL Bolognesi.

Respecto a la dimensión autenticidad se ha registrado un promedio de sig. = 0.075, que al ser contrastados con el margen del 0.05, se afirma que es superior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es T de Student.

Tabla 12

Prueba de hipótesis para la implementación ISO 27001:2013 en la autenticidad

Dimensión	Prueba T - Student			Nivel de significancia	Decisión $t_o > t_c$ $p < \alpha$
	Valor observado	Valor tabular	Probabilidad significancia		
Autenticidad	t_o= 9,342	tc = 1,680	p = 0,000	α =0,05	Se rechaza H_0

Con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido del método de T de Student, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la autenticidad en la UGEL Bolognesi Ancash 2023.

Resultado para la hipótesis específica 3:

Hi: La implementación ISO 27001:2013 incide significativamente en la integridad de la UGEL Bolognesi.

Ho: La implementación ISO 27001:2013 no incide significativamente en la integridad de la UGEL Bolognesi.

Referente a la dimensión integridad se ha registrado un promedio de sig. = 0.000, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Tabla 13

Prueba de Wilcoxon – indicador de nivel de confiabilidad

		N	Rango promedio	Suma de rangos
Post-Test de Integridad - Pre Test de Integridad	Rangos negativos	5[a]	12,60	63,00
	Rangos positivos	37[b]	22,70	840,00
	Empates	0[c]		
	Total	42		

a. Post-test de Integridad < Pre-Test de Integridad

b. Post-test de Integridad > Pre-Test de Integridad

c. Post-test de Integridad = Pre-Test de Integridad

A través del análisis reflejado en la tabla se ha podido dar a conocer los valores de rango y sumatoria son significativos, al presentar un rango de 22.7 y suma de 840.00, con un rango positivo 4[b] que presenta b. Post-test de integridad > Pre-test de integridad.

Tabla 14

Prueba de hipótesis para la implementación ISO 27001:2013 en la integridad

	Post-test de integridad – Pre-Test de integridad
Z	-4,865[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido de la prueba de rango de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la disponibilidad en la UGEL Bolognesi Ancash 2023.

Resultado para la hipótesis específica 4:

Hi: La implementación ISO 27001:2013 incide significativamente en la confidencialidad de la UGEL Bolognesi.

Ho: La implementación ISO 27001:2013 no incide significativamente en la confidencialidad de la UGEL Bolognesi.

Respecto a la dimensión confidencialidad se ha registrado un promedio de sig. = 0.025, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Tabla 15

Prueba de Wilcoxon – indicador de nivel de confiabilidad

		N	Rango promedio	Suma de rangos
Post-Test de Confidencialidad - Pre Test de Confidencialidad	Rangos negativos	5[a]	16,50	82,50
	Rangos positivos	37[b]	22,18	820,50
	Empates	0[c]		
	Total	42		

a. Post-test de Confidencialidad < Pre Test de Confidencialidad

b. Post-test de Confidencialidad > Pre Test de Confidencialidad

c. Post-test de Confidencialidad = Pre Test de Confidencialidad

A través del análisis reflejado en la tabla se ha podido dar a conocer los valores de rango y sumatoria son significativos, al presentar un rango de 22.18 y suma de 820.50, con un rango positivo 4[b] que presenta b. Post-test de confidencialidad > Pre-test de confidencialidad.

Tabla 16

Prueba de hipótesis para la implementación ISO 27001:2013 en la confidencialidad

	Post-test de confidencialidad – Pre-Test de confidencialidad
Z	-4,618[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido de la prueba de rango de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la

implementación ISO 27001:2013 incide significativamente en la confidencialidad en la UGEL Bolognesi Ancash 2023.

Resultado para la hipótesis específica 5:

Hi: La implementación ISO 27001:2013 incide significativamente en la trazabilidad de la UGEL Bolognesi.

Ho: La implementación ISO 27001:2013 no incide significativamente en la trazabilidad de la UGEL Bolognesi.

Al mencionar a la dimensión trazabilidad se ha registrado un promedio de sig. = 0.005, que al ser contrastados con el margen del 0.05, se afirma que es inferior, por lo tanto, se da a conocer que la distribución que se presenta en el pre y post-test es no paramétrica, bajo lo expuesto se menciona que el método utilizado para comprobar la hipótesis es Wilcoxon.

Tabla 17

Prueba de Wilcoxon – indicador de nivel de confiabilidad

		N	Rango promedio	Suma de rangos
Post-Test de Trazabilidad - Pre Test de Trazabilidad	Rangos negativos	4[a]	13,00	52,00
	Rangos positivos	37[b]	21,86	809,00
	Empates	1[c]		
	Total	42		

a. Post-test de Trazabilidad < Pre-Test de Trazabilidad

b. Post-test de Trazabilidad > Pre-Test de Trazabilidad

c. Post-test de Trazabilidad = Pre-Test de Trazabilidad

A través del análisis reflejado en la tabla se ha podido dar a conocer los valores de rango y sumatoria son significativos, al presentar un rango de 21.86 y suma de 809.00, con un rango positivo 4[b] que presenta b. Post-test de trazabilidad > Pre-test de trazabilidad.

Tabla 18

Prueba de hipótesis para la implementación ISO 27001:2013 en la trazabilidad

	Post-test de confidencialidad – Pre-Test de confidencialidad
Z	-4,914[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido de la prueba de rango de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la trazabilidad en la UGEL Bolognesi Ancash 2023.

V. DISCUSIÓN

A través de los hallazgos obtenidos para el objetivo general que se basa en determinar la influencia de la implementación ISO 27001:2013 en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, de acuerdo a la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido de la prueba de rango de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, dentro de la mejora registrada en el estudio se obtuvo que el nivel deficiente se redujo en 52.4% en el Post-test, luego para el nivel regular se mejoró en 19.0% y el nivel eficiente se incrementó en 71.4%.

Estos resultados presentan una concordancia con lo evidenciado por Córdoba (2021), quien desarrolló su investigación de posgrado con el propósito de demostrar como la implementación de la ISO 27001:2013 brinda la protección necesaria de una entidad de Colombia, a partir de ello metodológicamente se alinea como experimental porque aplico y evaluó el efecto generado por la ISO en la protección de datos de la entidad, se ha trabajado con una población de 48 trabajadores, para ello se ha llegado a concluir: Los resultados han demostrado que en el pre test sea tenido una vulnerabilidad de datos del 68.0% y en el post-test se ha reducido a 21.0%, presentando una efectividad del 47.0%, con ello los procesos que presenta la ISO son favorables para que la entidad pueda alcanzar la seguridad respectiva y se garantice el servicio con protección de información de los usuarios y la entidad, de la misma manera se estableció los lineamientos a seguir en todo el proceso de seguimiento de la información que se accede por los usuarios.

Con la afirmación realizada se tiene que un Sistema de Gestión de la Seguridad de la Información (SGSI) consiste en el diseño, implementación, renovación de un sólido y rápido proceso para administrar de manera correcta y eficaz el acceso a los registros, investigando conservar estadísticas de primer nivel que incluyan confidencialidad, integridad y seguridad. Disponibilidad de propiedad

de los hechos, buscando continuamente para disminuir los peligros de seguridad (Torres, 2020).

A través de los hallazgos obtenidos para el objetivo específico que se basa en determinar la influencia de la implementación ISO 27001:2013 en la disponibilidad de la UGEL Bolognesi, con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido del método de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la disponibilidad en la UGEL Bolognesi Ancash 2023. Dentro de la mejora registrada en el estudio se obtuvo que el nivel deficiente se redujo en 66.7% en el post-test, luego para el nivel regular se mejoró en 14.3% y el nivel eficiente se incrementó en 52.4%.

Estos resultados presentan una concordancia con lo evidenciado por Contero (2019), ejecutó una investigación de nivel de posgrado con la finalidad de implementar policitas de seguridad bajo los lineamientos de la ISO 27001:2013 con el propósito de optimizar el control de la información de una empresa en Quito, para ello se consideró de diseño experimental, presentando un alcance longitudinal, procediendo con la aplicación de técnicas e instrumentos necesarios que le permitieron recopilar la información necesaria, utilizó como población a 67 trabajadores, los resultados han determinado un nivel de vulneración de la información del 56.0%, lo cual se ha reducido en el post-test a 29.0%, presentando un nivel de eficiencia del 47.0%, que le permitió concluir: Según los lineamientos que se establecen en la ISO se ha podido desarrollar las políticas internas necesarias para proteger la intromisión de los sistemas informáticos y el control de los accesos, para ello el personal de informática debe monitorear de manera secuencial como se desarrolla cada uno de estos elementos.

Con la afirmación realizada se tiene que según ISO/IEC, la seguridad de la información se describe como aquellas tácticas, prácticas exactas y metodologías que se buscan para proteger los datos y los sistemas de registros de la entrada, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados. Esta definición esencialmente significa que tenemos que proteger nuestras

estadísticas y fuentes de infraestructura de generación de personas que intentarían hacer un mal uso de ellas (Guerra et al., 2021).

ISO 27001 consigue implementarse en diversas formas dentro de la organización, tanto privada o pública, de gran tamaño o pequeñas organizaciones. Está escrito con la ayuda de los mejores profesionales del mundo en el tema y suministra una metodología para efectuar el control estadístico de la seguridad en un empleador. También permite certificar una organización; lo que significa que un marco de certificación independiente confirma que las estadísticas de seguridad se han aplicado en esa empresa de conformidad con la norma ISO 27001 de moda (Parada et al., 2018).

A través de los hallazgos obtenidos para el objetivo específico que se basa en determinar la influencia de la implementación ISO 27001:2013 en la autenticidad de la UGEL Bolognesi, con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido del método de T de Student, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la autenticidad en la UGEL Bolognesi Ancash 2023. Dentro de la mejora registrada en el estudio se obtuvo que el nivel deficiente se redujo en 57.1% en el post-test, luego para el nivel regular se mejoró en 7.1% y el nivel eficiente se incrementó en 50.0%.

Estos resultados presentan una concordancia con lo evidenciado por Arias (2020), con su estudio de posgrado que se enfocó en implementar la ISO 27001:2013 en una empresa del Callao, para optimizar el manejo de su información, durante la fase metodológica se consideró de diseño experimental, aplicando estrategias que le permitan establecer las directivas de seguridad necesaria que resguarde la información y proteja los datos de la empresa, desarrollada con un alcance longitudinal, la muestra utilizada en el proyecto fue de 38 trabajadores de la empresa, para ello se registró como resultados que antes de aplicar la norma ISO se ha presenta un vulnerabilidad de información de 49.0% y en el post-test se ha reducido en 18.0%, con ello se ha demostrado una afectividad del 31.0%, logrando concluir: Los procesos de proteger a la información de la empresa se basa en la ISO que establece las directrices necesarias que permitan

contar con los lineamientos de protección de datos y le brinde las garantías necesarias de confidencialidad de datos, quedando demostrado que la implementación de la ISO y su monitoreo respectivo garantiza la seguridad de la información.

Con la afirmación realizada se tiene que las características (o controles) de seguridad que se aplicarán generalmente tienen la forma de políticas, procesos e implementación técnica (como una instancia, un programa de software y un equipo). Bajo la misma línea, en gran parte de los casos, las corporaciones ya se cuentan con todo el programa de hardware y software, pero lo usan de manera insegura; en otras palabras, la mayoría que desarrolla la implementación de ISO 27001 puede estar asociada con la determinación de las reglas organizativas (por ejemplo, la escritura de registros) importantes para evitar infracciones de seguridad (Aguilera et al., 2017).

A través de los hallazgos obtenidos para el objetivo específico que se basa en determinar la influencia de la implementación ISO 27001:2013 en la integridad de la UGEL Bolognesi, con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido del método de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la disponibilidad en la UGEL Bolognesi Ancash 2023. Dentro de la mejora registrada en el estudio se obtuvo que el nivel deficiente se redujo en 57.1% en el post-test, luego para el nivel regular se mejoró en 7.1% y el nivel eficiente se incrementó en 50.0%.

Estos resultados presentan una concordancia con lo evidenciado por Jara (2018), con su estudio de maestría relacionado con la seguridad de la información y la gestión de los procesos de riesgos de una entidad de Perú, para ello se consideró de diseño experimental, presentando un alcance longitudinal, procediendo con la aplicación de técnicas e instrumentos necesarios que le permitieron recopilar la información necesaria, la muestra fue de 55 trabajadores, los resultados que se alcanzaron en el estudio fue de 52.0% para el pre test, datos que fueron reducidos en el post-test alcanzando un valor de 27.0%, permitiendo obtener una mejora del 25.0%, que le permitió concluir: Se logro mejorar la

seguridad de datos de la entidad a través de la implementación de las directivas que se establecen en la ISO, para ello se ha tenido que realizar las modificaciones necesarias en la infraestructura de la red y creado políticas que permitan resguardar la información.

Con la afirmación realizada se tiene que la óptima gestión de la protección de la información indaga el establecimiento y preservación de aplicaciones, controles y lineamientos, los cuales pueden estar destinados a mantener la confidencialidad, integridad y disponibilidad de los datos, si alguna de esas particularidades falla no es nada positivo (Sánchez y Ledesma, 2021).

A través de los hallazgos obtenidos para el objetivo específico que se basa en determinar la influencia de la implementación ISO 27001:2013 en la confidencialidad de la UGEL Bolognesi, con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido del método de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la confidencialidad en la UGEL Bolognesi Ancash 2023. Dentro de la mejora registrada en el estudio se obtuvo que el nivel deficiente se redujo en 42.9% en el post-test, luego para el nivel regular se mejoró en 2.4% y el nivel eficiente se incrementó en 40.5%.

Estos resultados presentan una concordancia con lo evidenciado por Huerta (2020), desarrollo su estudio de posgrado con la finalidad de implementar políticas de seguridad de la información para resguardar los datos de una empresa de Lima, durante el proceso se consideró de diseño experimental, basado en dos momentos para el análisis de información y demostrando el efecto generado con la implementación, la muestra seleccionada la conforman 53 trabajadores, mostrando como resultados que la información presento una vulneración del 43.0%, mientras que los hallazgos del post-test han revelado una vulneración de información del 21.0%, mejorando en 22..0%, logrando concluir: Definir los protocolos de seguridad y transmitirlas al personal es relevante para que se alcance la seguridad necesaria de la integridad de datos, estableciendo las fases necesarias y los controles pertinentes en cada uno de los procesos. Se ha demostrado que la ISO es una

herramienta que permite a toda empresa proteger su información con los procedimientos necesarios.

Con la afirmación realizada se tiene que implicar que la información está disponible mejor a través de empleados legales. Esto es lo que se llama necesidad de reconocer. Con este plazo, se hace referencia al hecho de que los hechos han de ser más efectivos respecto de las personas, entidades o estructuras jurídicas a las que se les otorga derecho de entrada. Ejemplos de violaciones de la confidencialidad son el robo de registros privados por parte de un atacante por medio de Internet, la divulgación no autorizada de registros personales por medio de las redes sociales o el acceso por parte de un trabajador a datos esenciales de la organización ubicados en carpetas sin permisos asignados, que debe ya no tiene derecho de entrada (Peñafiel, 2021).

A través de los hallazgos obtenidos para el objetivo específico que se basa en determinar la influencia de la implementación ISO 27001:2013 en la trazabilidad de la UGEL Bolognesi, con la finalidad de realizar la contrastación de la hipótesis propuesta en el estudio se ha analizado el valor obtenido del método de Wilcoxon, donde se ha dado a conocer un valor de sig. = 0.000 < 0.05, de esa manera se ha logrado confirmar la hipótesis del estudio, puesto que el valor de la significancia obtenida cae por debajo del 0.05, por lo tanto, se toma la decisión de confirmar que la implementación ISO 27001:2013 incide significativamente en la trazabilidad en la UGEL Bolognesi Ancash 2023. Dentro de la mejora registrada en el estudio se obtuvo que el nivel deficiente se redujo en 40.5% en el post-test, luego para el nivel regular se mejoró en 14.3% y el nivel eficiente se incrementó en 54.8%.

Estos resultados presentan una concordancia con lo evidenciado por Calderón (2019), presentó su estudio de posgrado con el objetivo de implementar la seguridad de la información por medio de la ISO 27001:2013 y resguardar los datos de una entidad de Lima, durante esta fase del estudio se consideró utilizar el diseño experimental, bajo una categoría pre experimental, la muestra seleccionada en el estudio fue de 41 trabajadores, los resultados han arrojado que durante la etapa evaluativa del estudio se ha registrado una vulneración de la información del 62.0%, luego con la aplicación de la norma ISO se ha reducido en 24.0% en el post-test, alcanzando unas mejora del 38.0%, concluyendo que la buenas prácticas de las fases de la ISO favorecen para fortalecer la información de la entidad y brinda

los lineamientos para proteger la transmisión de datos internos, además establece la estructura de la red necesaria para garantizar la protección de datos.

Con la afirmación realizada se tiene que la seguridad de la información es un tema importante para la era en la que los registros de innumerables personas y grupos se guardan en una variedad de sistemas informáticos, por lo general fuera de nuestro control directo. Cuando se habla de la seguridad de los datos de forma generalizada, es muy importante comprender que la seguridad y la productividad suelen ser ideas diametralmente adversas, y ser capaz de señalar exactamente cuándo nos sentimos cómodos es una tarea difícil (Castillo y Pérez, 2017).

VI. CONCLUSIONES

Primera: Del objetivo general. Se mejoró significativamente (sig. = 0.000 < 0.05) la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 52.4% en el post-test, luego para el nivel regular se mejoró en 19.0% y el nivel eficiente se incrementó en 71.4%, a partir de estos hallazgos se asegura la información de la entidad y se evita vulneración de la información que se maneja en la parte administrativa.

Segunda: Del primer objetivo específico. Se mejoró significativamente (sig. = 0.000 < 0.05) la **disponibilidad** en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 66.7% en el post-test, luego para el nivel regular se mejoró en 14.3% y el nivel eficiente se incrementó en 52.4%, ello ha permitido que los trabajadores puedan acceder a la información de la entidad estando fuera de la entidad, porque se ha incorporado la seguridad necesaria para los accesos.

Tercera: Del segundo objetivo específico. Se mejoró significativamente (sig. = 0.000 < 0.05) la **autenticidad** en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 57.1% en el post-test, luego para el nivel regular se mejoró en 7.1% y el nivel eficiente se incrementó en 50.0%. Lo mencionado ha permitido que se mejore los procedimientos de acceso a la información de la entidad, requiriendo usuario y contraseña para ingresar a la información.

Cuarta: Del tercer objetivo específico. Se mejoró significativamente (sig. = 0.000 < 0.05) la **integridad** en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 57.1% en el post-test, luego para el nivel regular se mejoró en 7.1% y el nivel eficiente se incrementó en 50.0%. Con ello la información se encuentra resguarda por los sistemas informáticos y el conocimiento que presentan los trabajadores para acceder a la información.

Quinta: Del cuarto objetivo específico. Se mejoró significativamente (sig. = 0.000 < 0.05) la **confidencialidad** en la UGEL Bolognesi Ancash 2023, a

través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 42.9% en el post-test, luego para el nivel regular se mejoró en 2.4% y el nivel eficiente se incrementó en 40.5%. con estos hallazgos la información se encuentra protegida porque no deja registros de los usuarios que acceden de manera remota, permitiendo que se proteja a la información.

Sexta: Del quinto objetivo específico. Se mejoró significativamente (sig. = 0.000 < 0.05) la **trazabilidad** en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 40.5% en el post-test, luego para el nivel regular se mejoró en 14.3% y el nivel eficiente se incrementó en 54.8%. Con ello, se ha incorporado métodos de rastreo en los accesos que se producen a los sistemas de la entidad, asegurando la información.

VII. RECOMENDACIONES

Primera: Al director de la UGEL solicitar los reportes de los accesos y posibles vulneraciones al jefe de informática para que se puedan implementar políticas que refuercen las debilidades que se puedan presentar en la gestión del manejo de información.

Segunda: A los jefes de las áreas como informática, recursos humanos, logística, seguir los lineamientos adoptados en la implementación de la ISO 27001:2013 para resguardar la información de la UGEL Bolognesi e impedir la filtración de información que pueda perjudicar a la gestión que se viene realizando.

Tercera: Al jefe de informática monitorear los procesos que se realizan referente al manejo de la información de la UGEL, para que el trabajo que se realiza se pueda desarrollar con la protección de la información.

Cuarta: Al jefe de informática monitorear los equipos informáticos, analizando que no se instalen programas que puedan vulnerar la seguridad de la información de la UGEL e informar de los posibles incidentes que se presenten.

Quinta: A la comunidad científica continuar desarrollando estudios experimentales que permitan poner en práctica los conocimientos adquiridos como profesionales y se aporte a las instituciones con estrategias que permitan asegurar la información que manejan.

REFERENCIAS

Arias, E. *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac*, Callao. 2020. [Tesis de posgrado; Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1

Aguinaga et al. (2014). *El uso de las TIC. Su influencia en los cambios individuales y sociales.* 16 (111). http://www.injuve.es/sites/default/files/revista111_cap1.pdf

Azán et al. *The security risk of information in database managers based on trapezoidal fuzzy numbers*. *2017*. 11 (4). Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992017000400005

Abrego, D, Sánchez, y Medina, J. *Influencia de los sistemas de información en los resultados organizacionales. 2017*. Revista Scielo. 62 (1). https://www.scielo.org.mx/pdf/cya/v62n2/0186-1042-cya-62-02-00303-en.pdf

Aguilera et al. *The protection of the information. A vision from the cuban educational entities.* Revista Redalyc. 48 (3). 2017. Disponible en: https://www.redalyc.org/pdf/1814/181457243006.pdf

Baena, G. *Metodología de la investigación. 2017*. ISBN ebook: 978-607-744-748-1. Disponible en http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Bustamante et al. *Policies based on ISO 27001: 2013 and its influence on information security management in municipalities of Peru. 2021*. 12 (2). Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422021000200069

Benussi, C. *Security obligations on the personal data processing in Chile: current landscape and outstanding regulatory challenges. 2020*. Revista Scielo. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100227

Bornas, W. *Modelo de análisis para la implantación de un SGSI basado en ISO 27001 y COBIT para una empresa del sector educación*. [Tesis de posgrado; Universidad Nacional De San Agustín De Arequipa]. Disponible en: http://repositorio.unsa.edu.pe/bitstream/handle/20.500.12773/11487/UPboriwm.pdf?sequence=1&isAllowed=y

Concepción, T, González, S, García, P y Miño, J. *Investigation methodology: Origin and construction of a doctoral tesis. 2019*. 6(1). Disponible en: 76-87. http://scielo.iics.una.py/pdf/ucsa/v6n1/2409-8752-ucsa-6-01-76.pdf

Córdoba, J. *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia*. [Tesis de posgrado; Universidad Peruana Unión]. Disponible en: https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/4789/Javier_Tesis_Maestro_2021.pdf?sequence=1&isAllowed=y

Carrasco, R. *Telecommuting: advantages and disadvantages in organizations and collaborators. 2021*. Revista FAECO sapiens. 4 (2). http://portal.amelica.org/ameli/journal/221/2212240001/html/

Calderón, J. *Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018*. [Tesis de posgrado; Universidad César Vallejo]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/30014/Calder%c3%b3n_SJA.pdf?sequence=1&isAllowed=y

Castillejos et al. *Safety in the digital skills of millennials.* 8 (2). 2016. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-61802016000300054

Carhuancho, I., Nolazco Labajos, F., Sicheri Monteverde, L., Guerrero Bejarano, M., & Casana Jara, k. (2019). *Metodología de la investigación holística. Guayaquil: Editorial UIDE. Repositorio Digital UIDE* https://repositorio.uide.edu.ec/handle/37000/3893

Cabezas, E., Andrade, A. y Torres, J. (2018). *Introducción a la metodología de la investigación científica.* ISBN: 978-9942-765-44-4.

http://repositorio.espe.edu.ec/jspui/bitstream/21000/15424/1/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Cohen, N. y Gómez, G. (2019). Metodología de la investigación, ¿para qué?: la producción de los datos y los diseños. ISBN 978-987-723-190-8. Editorial Teseo. http://biblioteca.clacso.edu.ar/clacso/se/20190823024606/Metodologia_para_que.pdf

Carvajal et al. *A proposal for the management of the information security applied to a Colombian public entity. 2019*. Revista Scielo. 13 (25). Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-83672019000100068

Contero, W. *Diseño de una política de seguridad de la información basada en la norma ISO 27002:2013, para el sistema de botones de seguridad del ministerio del interior. 2019*. [Tesis de posgrado; Universidad Internacional SEK]. Disponible en: https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Castillo, G y Pérez, E. *The state of the systems of information in the companies prioritized according to the current requirements. 2017*. 6 (2). http://www.scielo.org.ar/pdf/pacla/v6n2/v6n2a07.pdf

Cueva, M. y Alvarado, D. *Analysis of free SSL/TLS Certificates and their implementation as Security Mechanism in Application Servers. 2017*. 8 (1). Disponible en: https://ingenieria.ute.edu.ec/enfoqueute/index.php/revista/article/view/128

De la Rosa. *Automation of an information security management system based on the ISO / IEC 27001 Standard. 2021*. Revista Scielo. 13 (5). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495

Estrada, R, Unás, J y Flórez, O*. Information Security Practices in Times of Pandemic. Case Universidad del Valle, Tuluá campus. 2021.* 13 (3). Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2422-42002021000300098

Flores D, Carhuancho I, Venturo C, Sicheri L, M. I. (2019). Expert System for Information Technology Services Management. *International Journal of Recent Technology and Engineering*, *8*(4), 9986–9992. https://doi.org/10.35940/ijrte.d4423.118419

Flores, D., & Gardi, V. (2020). Sistema experto para la SGTI en la empresa Sion Global Solutions. *INNOVA Research Journal*, *5*(3.2), 235–248. https://doi.org/10.33890/innova.v5.n3.2.2020.1568

Florencia, M. *Gestión, implementación y control de los riesgos relacionados con tecnología de la información en los bancos.* 2012. Revista Scielo. 4 (2). http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1852-42222012000200004

Guerra et al. *Development of an information security management system based on analysis methodology and risk identification in university libraries. 2021*. 32(5). Disponible en: https://www.scielo.cl/scielo.php?pid=S0718-07642021000500145&script=sci_arttext

Guevara, R. *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. 2017*. Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Tesis_t1339si.pdf

Hernández. R. y Mendoza, C. *Metodología de la investigación- rutas cuantitativa-cualitativa-mixta.* 2018. ISBN 1456260960. Editor McGraw-Hill Interamericana

Huerta, C. *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019*. [Tesis de posgrado; Universidad César Vallejo]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/46037/Huerta_ACA-SD.pdf?sequence=1&isAllowed=y

Instituto Nacional de Ciberseguridad de España (2020). Ciberseguridad en el teletrabajo. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf

Iturralde, C. y Duque, L. *precarisation of teleworking in ecuador in the context of Covid-19: analysis variables from the marxist approach. 2021*. Revista Scielo. 14 (1). http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2550-67222021000200146

Jara, O. *Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018*. [Tesis de posgrado; Universidad César Vallejo]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31209/Jara_MOY.pdf?sequence=1&isAllowed=y

Jiménez, I. (2020). El triángulo lógico. Una ecuación didáctica emergente para aprender metodología de la investigación. Universidad de La Sabana. https://web.p.ebscohost.com/ehost/detail/detail?vid=0&sid=7be0c0b1-aae9-471f-ba3a-42032829f293%40redis&bdata=Jmxhbmc9ZXMmc2l0ZT1laG9zdC1saXZl#db=e000xww&AN=2659814

Lizárraga et al. *Impact of computer auditing in organizations: A bibliographical review. 2022*. 4 (638). Disponible en: https://revistas.upt.edu.pe/ojs/index.php/ingenieria/article/view/638/632

Llanos, Enrique. Implementación un sistema de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. caso de estudio: unidad de gestión educativa local 01. (Tesis; Universidad Señorde Sipan). Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/6400/Llanos%20Guill%c3%a9n%20Enrique%20Guillermo.pdf?sequence=1&isAllowed=y

Martelo et al. Basic Logical Safety Model. Study Case: The Network Laboratory of the University of Cartagena in Colombia. 2018. Revista Scielo. 13 (1). Disponible en: https://scielo.conicyt.cl/pdf/infotec/v29n1/0718-0764-infotec-29-01-00003.pdf

Machicao, S. *Análisis de riesgo y políticas de seguridad de información de la Oficina de Tecnologías De Información (Oti) – UNA Puno 2018*. Disponible en:

http://repositorio.unap.edu.pe/bitstream/handle/UNAP/13958/Machicao_Mollocondo_Saulo_Gustavo.pdf?sequence=1&isAllowed=y

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

Montenegro, C, Larco, A, y Fonseca, E. *Agile Approach for Model Harmonization to IT Process Improvement. 2017*. Revista Redalyc. Disponible en: https://www.redalyc.org/pdf/5122/512254534002.pdf

Moreira et al. *Low-Cost Solutions Using the Infrastructure as a Service with High Availability and Virtualization Model. 2017*. Revista Scielo. 8 (1). http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-65422017000100186

Nieves, Y. y Ponjuan, G. *Access to information and processing of personal data. Visions from the academy*. 35 (1). Disponible en: http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-86342021000200167

Osorio, J. *Workplace safety and health in micro businesses in a neighborhood in the city of Itagüí, Antioquia, Colombia. 2021*. 11 (22). Disponible en: https://www.scielosp.org/article/csp/2021.v37n11/e00175320/

Parada et al. *Analysis of the Components of Security from a Systemic System Dynamics Perspective. 2018*. 29(1). Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000100027

Peñafiel, Kevin. *Factors that determine computer vulneration and the development of a mobile app to raise awareness about the impacts on assets. 2021*. Revista Scielo. 21 (21). http://www.scielo.org.bo/scielo.php?pid=S2071-081X2021000100009&script=sci_arttext

Rodríguez et al. *Application of ISO 27001 and its influence on the information security of a Peruvian private company. 2020*. 8 (3). Disponible en: http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992020000400011

Saltos, M, Robalino, J. y Pazmiño, L. *Conceptual analysis of computer crime in Ecuador. 2020*. Revista Scielo. 17 (78). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343

Salgado, C. *Manual de investigación. Teoría y práctica para hacer la tesis según la metodología cuantitativa. 2018*. Universidad Marcelino Champagnat.

Sánchez, A, y Ledesma, T. *Effects of home-office on workers' well-being. 2021*. Revista Scielo. 30 (2). https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1132-62552021000200234

Torres, C. *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa Privada Megaprofer S.A. 2020*. (Tesis, Universidad Técnica de Abanto). Disponible en: https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

Valencia, A. *Regulatory Aspects of Teleworking in Peru: Analysis and Perspectives. 2018.* 12(41). Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100203

Vela et al. (2019). *Analyzing the classification of technical standards for the management of information technology infrastructure and services.* 94(1). https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073469736&doi=10.6036%2f9303&partnerID=40&md5=d1926e75dbd8798e95a511b4bfa6e214

Vite, H, Molina, B, y Dávila, J. *Gestión de la Información en las Instituciones de Educación Superior (IES) con base a la norma ISO 27001*. *2018*. Revista Scielo. 22 (2). https://revistas.utm.edu.ec/index.php/Informaticaysistemas/article/view/1434

Zuña et al. *Analysis of the security of the information in the SMES of the city of Milagro. 2019*. 11 (4). Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487

ANEXOS

Anexo 01: Operacionalización de variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	TÉCNICA	INSTRUMENTO	ÍTEMS	ESCALA DE MEDICIÓN
V.I. ISO 27001:2013	Según ISO/IEC, la seguridad de la información se describe como aquellas tácticas, prácticas exactas y metodologías que se buscan para proteger los datos y los sistemas de registros de la entrada, el uso, la divulgación, la interrupción, la modificación o la destrucción no autorizados. Esta definición esencialmente significa que tenemos que proteger	Es la aplicación de la norma ISO27001, en sus diversas etapas y ver el efecto que genera en la gestión de la información de la Ugel Bolognesi, para ello se detallan los parámetros necesarios para aplicación	Evaluación del desempeño	Plan de medición del SGSI	Encuesta	Cuestionario	1 al 10	Likert
				Medición del SGSI				
			Mejora continua	Identificar oportunidades de mejoras	Encuesta	Cuestionario	11 al 20	
				Plan de acción				

	nuestras estadísticas y fuentes de infraestructura de generación de personas que intentarían hacer un mal uso de ellas (Guerra et al., 2021).							
VARIABLES DE ESTUDIO	**DEFINICIÓN CONCEPTUAL**	**DEFINICIÓN OPERACIONAL**	**DIMENSIONES**	**INDICADORES**	**TÉCNICA**	**INSTRUMENTO**	**ÍTEMS**	**ESCALA DE MEDICIÓN**
V.D. GESTIÓN DEL MANEJO DE INFORMACIÓN	El conjunto de actividades que se realizan con el motivo de obtener, procesar, almacenar y, tarde o temprano, mejorar, de manera adecuada, la información que ésta produce o adquiere en una empresa y que permite el desarrollo de su interés.	Es el análisis de la percepción de los trabajadores de la Ugel Bolognesi sobre la gestión de la información por medio de un instrumento elaborado en base a las dimensiones detalladas en el marco teórico, presentando opciones de respuestas de tipo	D1. Disponibilidad	• Acceso las 24 horas • Estabilidad de la red • Capacidad tecnológica • Ancho de banda	Encuesta	Cuestionario	1 al 5	Likert
			D2. Autenticidad	• Política de seguridad • Control de usuarios • Administración de equipos • Vulneración de información	Encuesta	Cuestionario	6 al 10	

		Likert y analizada por medio de una escala ordinal	D3. Integridad	• Copias de seguridad • Soporte técnico • Administración de los sistemas	Encuesta	Cuestionario	11 al 15	
			D4. Confidencialidad	• Protección de datos • Privilegios de acceso • Políticas institucionales	Encuesta	Cuestionario	16 al 20	
			D5. Trazabilidad	• Seguimiento de los procesos. • Rastreo de usuarios	Encuesta	Cuestionario	21 al 24	

Anexo 02: Instrumento de medición.

Cuestionario: GESTIÓN DEL MANEJO DE INFORMACIÓN

Fecha: / /

Sexo: Femenino [ ] Masculino [ ]

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de evaluar ***el manejo de la información*** de la entidad. Las opiniones podrían ayudar a optimizar la gestión, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Nº	DIMENSIÓN	INDICADOR	PREGUNTA	1	2	3	4	5
1.	**Disponibilidad**	Acceso las 24 horas	Se cuenta con acceso a los sistemas de información durante las 24 horas al día.					
2.			Es necesario que la UGEL Bolognesi cuente con acceso a los sistemas de información las 24 horas al día.					
3.		Estabilidad de la red	La red de datos actual permite que los servicios de los sistemas se mantengan disponibles las 24 horas del día.					
4.		Capacidad tecnológica	Considera necesario que se optimice la capacidad tecnológica de la UGEL Bolognesi.					
5.		Ancho de banda	El ancho de banda de internet que cuenta la UGEL Bolognesi permite trabajar con normalidad y evita saturación de datos.					
6.	**Autenticidad**	Política de seguridad	La UGEL Bolognesi cuenta con políticas de seguridad para el acceso de los usuarios a su información.					

7.		Control de usuarios	Se cuenta con un control de usuarios basados en un servidor de dominio.					
8.		Administración de equipos	Los usuarios que se conectan de manera remota presentan una identificación de nombre de equipo.					
9.			Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto.					
10.		Vulneración de información	Se han registrado durante los últimos 6 meses ataques de vulneración de información a la UGEL Bolognesi.					
11.	**Integridad**	Copias de seguridad	La UGEL Bolognesi realiza copias de seguridad de los sistemas informáticos de manera periódica.					
12.			Los usuarios que realizan trabajo remoto tienen una carpeta compartida en el servidor para almacenar su información.					
13.		Soporte técnico	Cuando se presentan inconvenientes con los equipos de computadoras, se cuenta con un personal que brinda soporte de manera oportuna.					
14.		Administración de los sistemas	La UGEL Bolognesi cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas.					
15.			Se presentan problemas en los sistemas como información duplicada o reportes sin información.					
16.	**Confidencialidad**	Protección de datos	La UGEL Bolognesi cuenta con lineamientos que permite la protección de datos de los trabajadores y usuarios.					
17.			Se puede extraer información de la UGEL Bolognesi con facilidad por medio de dispositivos extraíbles como USB.					
18.		Privilegios de acceso	Se cuenta con un administrador que administra los privilegios de los usuarios, de acuerdos a sus necesidades.					
19.			Todos los usuarios tienen los mismos accesos al sistema.					

20.		Políticas institucionales	La UGEL Bolognesi cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información.					
21.	**Trazabilidad**	Seguimiento de los procesos.	La política que presenta la UGEL Bolognesi es que cada usuario es responsable de las acciones realizadas en los sistemas de información.					
22.			Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema.					
23.		Rastreo de usuarios	La UGEL Bolognesi cuenta con un sistema que permita monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.					
24.			Se cuenta con un firewall para realizar la protección de información de los clientes.					

Anexo 03: Validación de instrumento.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA GESTIÓN DEL MANEJO DE INFORMACIÓN

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad [3]		Sugerencias
	DIMENSIÓN 1: Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se cuenta con acceso a los sistemas de información durante las 24 horas al día.	X		X		X		
2	Es necesario que la UGEL Bolognesi cuente con acceso a los sistemas de información las 24 horas al día.	X		X		X		
3	La red de datos actual permite que los servicios de los sistemas se mantengan disponibles las 24 horas del día.	X		X		X		
4	Considera necesario que se optimice la capacidad tecnológica de la UGEL Bolognesi.	X		X		X		
5	El ancho de banda de internet que cuenta la UGEL Bolognesi permite trabajar con normalidad y evita saturación de datos.	X		X		X		
	DIMENSIÓN 2: Autenticidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	La UGEL Bolognesi cuenta con políticas de seguridad para el acceso de los usuarios a su información.	X		X		X		
7	Se cuenta con un control de usuarios basados en un servidor de dominio.	X		X		X		
8	Los usuarios que se conectan de manera remota presentan una identificación de nombre de equipo.	X		X		X		
9	Se han registrado durante los últimos 6 meses ataques de vulneración de información a la UGEL Bolognesi.	X		X		X		
10	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto.	X		X		X		
	DIMENSIÓN 3: Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	La UGEL Bolognesi realiza copias de seguridad de los sistemas informáticos de manera periódica.	X		X		X		
12	Los usuarios que realizan trabajo remoto tienen una carpeta compartida en el servidor para almacenar su información.	X		X		X		
13	Cuando se presentan inconvenientes con los equipos de computadoras, se cuenta con un personal que brinda soporte de manera oportuna.	X		X		X		
14	La UGEL Bolognesi cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas.	X		X		X		
15	Se presentan problemas en los sistemas como información duplicada o reportes sin información.	X		X		X		
	DIMENSIÓN 4: Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	La UGEL Bolognesi cuenta con lineamientos que permite la protección de datos de los trabajadores y usuarios.	X		X		X		
17	Se puede extraer información de la UGEL Bolognesi con facilidad por medio de dispositivos extraíbles como USB.	X		X		X		
18	Se cuenta con un administrador que administra los privilegios de los usuarios, de acuerdos a sus necesidades.	X		X		X		
19	Todos los usuarios tienen los mismos accesos al sistema.	X		X		X		

20	La UGEL Bolognesi cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información.	X		X		X		
	DIMENSIÓN 5: Trazabilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	La política que presenta la UGEL Bolognesi es que cada usuario es responsable de las acciones realizadas en los sistemas de información.	X		X		X		
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema.	X		X		X		
23	La UGEL Bolognesi cuenta con un sistema que permita monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.	X		X		X		
24	Se cuenta con un firewall para realizar la protección de información de los usuarios.	X		X		X		

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr: **Lezama Gonzales Pedro Martin DNI: 09656793**

Especialidad del validador: Ingeniero de Sistemas

21 de noviembre del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA GESTIÓN DEL MANEJO DE INFORMACIÓN

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad [3]		Sugerencias
	DIMENSIÓN 1: Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se cuenta con acceso a los sistemas de información durante las 24 horas al día.							
2	Es necesario que la UGEL Bolognesi cuente con acceso a los sistemas de información las 24 horas al día.							
3	La red de datos actual permite que los servicios de los sistemas se mantengan disponibles las 24 horas del día.							
4	Considera necesario que se optimice la capacidad tecnológica de la UGEL Bolognesi.							
5	El ancho de banda de internet que cuenta la UGEL Bolognesi permite trabajar con normalidad y evita saturación de datos.							
	DIMENSIÓN 2: Autenticidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	La UGEL Bolognesi cuenta con políticas de seguridad para el acceso de los usuarios a su información.							
7	Se cuenta con un control de usuarios basados en un servidor de dominio.							
8	Los usuarios que se conectan de manera remota presentan una identificación de nombre de equipo.							
9	Se han registrado durante los últimos 6 meses ataques de vulneración de información a la UGEL Bolognesi.							
10	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto.							
	DIMENSIÓN 3: Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	La UGEL Bolognesi realiza copias de seguridad de los sistemas informáticos de manera periódica.							
12	Los usuarios que realizan trabajo remoto tienen una carpeta compartida en el servidor para almacenar su información.							
13	Cuando se presentan inconvenientes con los equipos de computadoras, se cuenta con un personal que brinda soporte de manera oportuna.							
14	La UGEL Bolognesi cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas.							
15	Se presentan problemas en los sistemas como información duplicada o reportes sin información.							
	DIMENSIÓN 4: Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	La UGEL Bolognesi cuenta con lineamientos que permite la protección de datos de los trabajadores y usuarios.							
17	Se puede extraer información de la UGEL Bolognesi con facilidad por medio de dispositivos extraíbles como USB.							
18	Se cuenta con un administrador que administra los privilegios de los usuarios, de acuerdos a sus necesidades.							
19	Todos los usuarios tienen los mismos accesos al sistema.							

20	La UGEL Bolognesi cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información.							
	DIMENSIÓN 5: Trazabilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	La política que presenta la UGEL Bolognesi es que cada usuario es responsable de las acciones realizadas en los sistemas de información.							
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema.							
23	La UGEL Bolognesi cuenta con un sistema que permita monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.							
24	Se cuenta con un firewall para realizar la protección de información de los clientes.							

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr: **ACUÑA BENITES MARLON FRANK** **DNI: 42097456**

Especialidad del validador: Ingeniero de Sistemas

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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

21 de noviembre del 2022

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: LA GESTIÓN DEL MANEJO DE INFORMACIÓN

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad [3]		Sugerencias
	DIMENSIÓN 1: Disponibilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	Se cuenta con acceso a los sistemas de información durante las 24 horas al día.							
2	Es necesario que la UGEL Bolognesi cuente con acceso a los sistemas de información las 24 horas al día.							
3	La red de datos actual permite que los servicios de los sistemas se mantengan disponibles las 24 horas del día.							
4	Considera necesario que se optimice la capacidad tecnológica de la UGEL Bolognesi.							
5	El ancho de banda de internet que cuenta la UGEL Bolognesi permite trabajar con normalidad y evita saturación de datos.							
	DIMENSIÓN 2: Autenticidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
6	La UGEL Bolognesi cuenta con políticas de seguridad para el acceso de los usuarios a su información.							
7	Se cuenta con un control de usuarios basados en un servidor de dominio.							
8	Los usuarios que se conectan de manera remota presentan una identificación de nombre de equipo.							
9	Se han registrado durante los últimos 6 meses ataques de vulneración de información a la UGEL Bolognesi.							
10	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto.							
	DIMENSIÓN 3: Integridad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	La UGEL Bolognesi realiza copias de seguridad de los sistemas informáticos de manera periódica.							
12	Los usuarios que realizan trabajo remoto tienen una carpeta compartida en el servidor para almacenar su información.							
13	Cuando se presentan inconvenientes con los equipos de computadoras, se cuenta con un personal que brinda soporte de manera oportuna.							
14	La UGEL Bolognesi cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas.							
15	Se presentan problemas en los sistemas como información duplicada o reportes sin información.							
	DIMENSIÓN 4: Confidencialidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
16	La UGEL Bolognesi cuenta con lineamientos que permite la protección de datos de los trabajadores y usuarios.							
17	Se puede extraer información de la UGEL Bolognesi con facilidad por medio de dispositivos extraíbles como USB.							
18	Se cuenta con un administrador que administra los privilegios de los usuarios, de acuerdos a sus necesidades.							
19	Todos los usuarios tienen los mismos accesos al sistema.							

20	La UGEL Bolognesi cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información.							
	DIMENSIÓN 5: Trazabilidad	**Si**	**No**	**Si**	**No**	**Si**	**No**	
21	La política que presenta la UGEL Bolognesi es que cada usuario es responsable de las acciones realizadas en los sistemas de información.							
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema.							
23	La UGEL Bolognesi cuenta con un sistema que permita monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.							
24	Se cuenta con un firewall para realizar la protección de información de los usuarios.							

Observaciones (precisar si hay suficiencia):_____

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

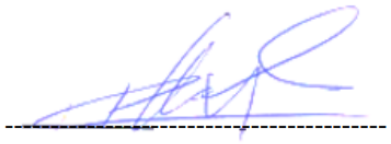
Apellidos y nombres del juez validador. Dr: Ponte Quiñones Elvis Jerson **DNI: 44199834**

Especialidad del validador: Ingeniero de Sistemas

21 de noviembre del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

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



Firma del Experto Informante.

Anexo 04: Confiabilidad del instrumento

CALCULO DE LA CONFIABILIDAD DEL INSTRUMENTO GESTIÓN DE LA INFORMACIÓN MEDIANTE METODO DE ALFA DE CROMBACH

Sujetos	Preguntas																								TOTAL
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	3	4	5	4	2	3	2	3	5	4	5	4	2	3	2	5	4	2	3	5	4	4	5	3	86
2	2	3	2	4	5	3	2	3	2	4	5	3	2	3	2	4	5	2	3	2	4	2	3	2	72
3	3	2	5	4	2	3	2	5	4	2	3	2	3	2	4	5	4	2	3	2	5	4	2	3	76
4	2	4	5	2	3	2	4	5	2	3	2	4	5	2	3	2	4	5	2	3	2	4	5	2	77
5	5	4	2	3	2	5	4	2	3	2	3	2	5	4	2	3	2	5	4	2	3	2	3	2	74
6	3	2	4	5	2	3	2	3	2	4	5	4	5	2	3	2	2	3	2	4	5	4	2	3	76
7	2	5	4	2	3	2	3	5	4	2	2	5	4	4	4	4	5	4	5	4	5	2	3	4	87
8	4	5	3	4	5	4	4	5	3	4	5	3	4	5	3	4	5	4	4	5	3	4	5	4	99
9	4	3	5	4	5	4	5	4	5	4	4	4	4	5	4	3	5	4	5	4	5	4	5	4	103
10	2	3	2	3	3	3	2	3	2	3	2	3	2	3	2	4	3	2	3	2	3	2	3	2	62
11	3	2	4	2	2	3	2	3	2	3	2	1	2	3	2	3	2	3	2	3	2	3	2	3	59
12	3	2	3	2	3	2	3	2	3	2	3	2	3	2	4	3	2	3	2	5	3	2	3	2	64
13	2	3	5	4	4	2	2	2	3	2	3	2	4	5	2	3	2	3	2	3	1	2	3	2	66
14	2	3	2	5	5	2	3	2	5	2	5	2	2	3	2	3	2	3	2	5	2	5	2	3	72
15	3	2	3	2	4	2	3	2	3	2	3	2	3	2	3	2	3	2	5	5	2	3	2	3	66
VARIANZA	0.8	1.0	1.4	1.2	1.4	0.8	0.9	1.4	1.2	0.8	1.4	1.2	1.3	1.2	0.7	0.9	1.6	1.0	1.3	1.4	1.7	1.0	1.4	0.6	156.3
TOTAL	27.7																								

CALCULO DEL COEFICIENTE DE CONFIABILIDAD:

$$\alpha = \frac{K}{K-1}\left(1 - \frac{\sum S^2 Items}{\sum S^2 T}\right)$$

DATOS	
K	Número de Items
$\sum S^2 Items$	CALCULO VARIANZA POR ITEMS
$\sum S^2 T$	CALCULO VARIANZA TOTAL

$$\alpha = \frac{24}{23}\left[1 - \frac{27.7}{156.3}\right]$$

$$\alpha = 1.043\left[1 - 0.177006\right]$$

$$\alpha = 1.043\left[0.822994257\right]$$

$$\alpha = 0.859$$

Anexo 05: Carta de Presentación

UNIVERSIDAD CÉSAR VALLEJO

POSGRADO

"Año del Fortalecimiento de la Soberanía Nacional"

Lima, 24 de octubre de 2022
Carta P. 1054-2022-UCV-VA-EPG-F01/J

Prof.
VICENTE RAMÓN RODRÍGUEZ ESPEJO
Director del Programa Sectorial III
Unidad de Gestión Educativa Local de Bolognesi

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a IBARRA CAQUI, LUCIO; identificado con DNI N° 44854929 y con código de matrícula N° 7002729502; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

ISO 27001:2013 PARA LA GESTIÓN DEL MANEJO DE INFORMACIÓN EN LA UGEL BOLOGNESI ANCASH 2023

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador IBARRA CAQUI, LUCIO asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dra. Estrella A. Esquiagola Aranda
Jefa
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

Anexo 06: Carta de Aceptación

GOBIERNO REGIONAL DE ANCASH
UNIDAD DE GESTIÓN EDUCATIVA LOCAL DE BOLOGNESI
"AÑO DEL FORTALECIMIENTO DE LA SOBERANÍA NACIONAL"

Chiquián, 17 NOV. 2022

OFICIO N° 0699 -2022-ME/GRA/DREA/UGELB-D.

SEÑOR (A):
Dra. Estrella A. ESQUIAGOLA ARANDA
Jefa de la Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

PRESENTE.

ASUNTO: CONCEDE PERMISO PARA REALIZACIÓN DE TRABAJO DE INVESTIGACIÓN.

REF.: Carta P. 1054-2022-UCV-VA-EPG-F01/J

Tengo el agrado de dirigirme a Ud. con la finalidad de hacerle llegar mi cordial saludo a nombre de la Unidad de Gestión Educativa Local de Bolognesi, a su vez de acuerdo al documento de la referencia se OTORGA el permiso correspondiente al estudiante IBARRA CAQUI Lucio; estudiante del programa de MAESTRÍA en Ingeniería de Sistemas con Mención en Tecnologías de la Información, para que realice la investigación de su trabajo titulado: ISO 27001:2013 Para la Gestión del Manejo de Información en la UGEL Bolognesi – Ancash 2023.

Es ocasión propicia para expresarle las muestras de mi especial consideración y estima personal.

Atentamente;

Prof. Vicente Ramón RODRÍGUEZ ESPEJO
DIRECTOR DEL PROGRAMA SECTORIAL III
UGEL BOLOGNESI

UGELB/VRRE
SAGA/KMA
PERS/ROP

DIRECCIÓN: JR. BRACALE RAMOS N° 303 – CHIQUIÁN – BOLOGNESI – ANCASH
Mesa de partes: tramiteugelb2020@gmail.com

Anexo 07: Matriz de Consistencia

Título: ISO 27001:2013 para la Gestión del Manejo de Información en la UGEL Bolognesi Ancash 2023
Autor: Lucio Ibarra Caqui.

Problema	Objetivos	Hipótesis	Variables e indicadores
¿De qué manera la implementación ISO 27001:2013 incide en la gestión del manejo de información en la Ugel Bolognesi Ancash 2023? **Problemas Específicos:** PE1: ¿De qué manera la implementación ISO 27001:2013 incide la disponibilidad en la Ugel Bolognesi? PE2: ¿De qué manera la implementación ISO	**Objetivo general:** Determinar la influencia de la implementación ISO 27001:2013 en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023. **Objetivos específicos:** OE1: Determinar la influencia de la implementación ISO 27001:2013 en la disponibilidad de la UGEL Bolognesi. OE2: Determinar la influencia de la implementación	**Hipótesis general:** La implementación ISO 27001:2013 incide significativamente en la gestión del manejo de información en la UGEL BOLOGNESI Ancash 2023. **Hipótesis específicas:** HE1: la implementación ISO 27001:2013 incide significativamente en la disponibilidad de la entidad.	**Variable 1: ISO 27001:2013.**

Dimensiones	Indicadores	Ítems	Escala de medición	Niveles y rangos
Evaluación del desempeño	• Plan de medición del SGSI • Medición del SGSI	1 al 12	**Escala de Likert** Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)	Bajo 1-8 Medio 9-16 Alto 17-24
Mejora continua	• Identificar oportunidades de mejoras • Plan de acción	12 al 24		

Variable 2: Gestión del manejo de información.

Dimensiones	Indicadores	Ítems	Escala de medición	Niveles y rangos
Disponibilidad	• Acceso las 24 horas • Estabilidad de la red • Capacidad	1 al 5	**Escala de Likert** Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4)	Bajo 1-8 Medio 9-16 Alto 17-24

27001:2013 incide la autenticidad en la Ugel Bolognesi? PE3: De qué manera la implementación ISO 27001:2013 incide la integridad en la Ugel Bolognesi? PE4: ¿De qué manera la implementación ISO 27001:2013 incide la confidencialidad en la Ugel Bolognesi? PE5: ¿De qué manera la implementación ISO 27001:2013 incide en la trazabilidad en la Ugel Bolognesi?	ISO 27001:2013 en la autenticidad de la UGEL Bolognesi. OE3: Determinar la influencia de la implementación ISO 27001:2013 en la integridad de la UGEL Bolognesi OE4: Determinar la influencia de la implementación ISO 27001:2013 en la confidencialidad de la UGEL Bolognesi. OE5: Determinar la influencia de la implementación ISO 27001:2013 en la trazabilidad de la UGEL Bolognesi.	HE2: la implementación ISO 27001:2013 incide significativamente en la autenticidad de la UGEL Bolognesi. HE3: la implementación ISO 27001:2013 incide significativamente en la integridad de la UGEL Bolognesi. HE4: la implementación ISO 27001:2013 incide significativamente en la confidencialidad de la UGEL Bolognesi. HE5: la implementación ISO 27001:2013 incide significativamente en la trazabilidad de la UGEL Bolognesi.		tecnológica • Ancho de banda		Siempre (5)	
			Autenticidad	• Política de seguridad • Control de usuarios • Administración de equipos • Vulneración de información	6 al 10		
			Integridad	• Copias de seguridad • Soporte técnico • Administración de los sistemas	11 al 15		
			Confidencialidad	• Protección de datos • Privilegios de acceso • Políticas institucionales	16 al 20		
			Trazabilidad	• Seguimiento de los procesos. • Rastreo de usuarios	21 al 24		

Anexo 08: Aplicación de la ISO

El 15 de agosto de 2022 se dio inicio al proyecto de implementación del SGSI para los procesos de TI para proteger la información crítica del proyecto, para lo cual se elaboró y aprobó el siguiente Project Charter.

CUADRO N° 1. PROJECT CHARTER

<table>
<tr><td>NOMBRE DEL PROYECTO</td><td>SIGLAS DEL PROYECTO</td></tr>
<tr><td>IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN ISO 27001:2013</td><td>SGSI</td></tr>
<tr><td colspan="2">DESCRIPCIÓN DEL PROYECTO</td></tr>
<tr><td colspan="2">El proyecto: Implementación de un sistema de gestión de seguridad de la información bajo el estándar ISO/IEC 27001:2013 consiste en la adecuación de los requisitos exigidos en la norma como la implementación de controles aplicables del Anexo A de la norma en mención. La implementación consiste en las siguientes etapas:
Etapas:
❖ DIAGNOSTICO
❖ PLANIFICAR
➢ Contexto de la organización
➢ Liderazgo
➢ Planeación
➢ Soporte
❖ HACER
➢ Operación
❖ MEDIR
➢ Evaluación del desempeño
❖ ACTUAR
➢ Mejora
❖ AUDITORÍA DE CERTIFICACIÓN
➢ Equipo de Trabajo:
El proyecto será realizado desde el 16 de agosto de 2022 al 14 de octubre de 2022.</td></tr>
<tr><td colspan="2">DEFINICIÓN DEL PRODUCTO DEL PROYECTO</td></tr>
</table>

Implementación de un sistema de gestión de seguridad de la información bajo el estándar ISO/IEC 27001:2013 para los procesos de tecnología de la información de la UGEL.
DEFINICIÓN DE REQUISITOS DEL PROYECTO
- Se entregará un informe del avance mensual del proyecto – Entregar un documento final con los resultados obtenidos post implementación

PRESUPUESTO PRELIMINAR DEL PROYECTO		
CONCEPTO		MONTO (S/.)
PERSONAL	Oficial de Seguridad de la Información y Analista de Procesos (MO Anual)	**20.000**
MATERIALES	Licencias de Office	**3200.00**
MAQUINAS	Notebook, Desktop y Proyector	**4500.00**
OTROS COSTOS	Capacitaciones (Auditor Interno, Líder y Riesgos)	**5000.00**
TOTAL PRESUPUESTO		**32.720**

ANÁLISIS COSTO / BENEFICIO

A continuación, se presenta el detalle económico para la viabilidad del proyecto (análisis costo/beneficio) según el cuadro

CUADRO N° 2. AHORRO DE IMPLEMENTAR EL SGSI

Ahorro de Implementar el SGSI	Costo Anual (s/.)
Incumplimiento de los entregables en la fecha requerida	**15.000**
Por incumplimiento de los niveles de servicio (SLA)	**6.000**
Difundir información a terceros sin contar con autorización	**8.000**
Acceder de forma remota a un computador sin la autorización respectiva	**9 200.00**
Por ingresar o retirar equipos informáticos sin la autorización respectiva	**7 500.00**

Por compartir información, música, videos a otros usuarios o terceros sin la autorización respectiva	**4 500.00**
Por no contar con licencias para brindar el servicio	**6 500.00**
Por no realizar pruebas de contingencia	**5 000.00**
Por errores que afecten el pago de uno o varios pensionistas	**6 500.00**
Por efectuar cambios en la plataforma y que afecten la operativa de los sistemas	**7 000.00**
Por la indisponibilidad de la mesa de servicios	**9 000.00**
Por realizar cambios de personal que no hayan sido autorizados	**8 000.00**
TOTAL DE PENALIDADES EFECTUADAS	**92 200.00**

Nota: Elaboración propia

CUADRO N° 3. COSTO DE IMPLEMENTAR EL SGSI

Costo Implementación del SGSI	Costo Anual (s/.)
Oficial de Seguridad	**12 000.00**
Analista de Procesos	**15 000.00**
Curso Interpretación y Auditor Interno SGSI	**500.00**
Curso Auditor Líder ISO/IEC 27001:2013	**500.00**
Curso de gestión de riesgos ISO 31000	**800.00**
Microsoft Office Estándar (2 licencias)	**1600.00**
Microsoft Visio (2 licencias)	**1600.00**
Microsoft Project (2 licencias)	**1600.00**
Notebook i7 - 320 GB, 8GB RAM (Oficial de Seguridad)	**3500.00**
Desktop + Monitor + Mouse (Analista de Procesos)	**3000.00**
Proyector Home Cinema 2030 para las charlas de seguridad	**3200.00**
TOTAL DE PENALIDADES EFECTUADAS	**43 300.00**

Nota: Elaboración propia

CUADRO N° 4. ANÁLISIS COSTO/BENEFICIO

Beneficio (B)	**92 200.00**
Costo (C)	**43 300.00**
B/C	2.13

Nota: Elaboración propia

Del cuadro 4, como B/C > 1 → EL PROYECTO ES RENTABLE

CUADRO N° 5 TIEMPO DE RECUPERACIÓN

Meses	**12**
Meses/(B/C)	**2.13**
Tiempo Recuperación	6 meses

Nota: Elaboración propia

El tiempo de recuperación de la inversión del proyecto de implantación del SGSI es de 6 meses.

RECURSOS

Los recursos o insumos que se requieren para el proyecto de implementación son los que figuran en la tabla 5.

CUADRO N° 6 RECURSOS DEL PROYECTO

Nro.	TIPO	RECURSO	PROVEEDOR
1	Humano	Oficial de Seguridad de la Información	GMD
2	Humano	Analista de Procesos	GMD
3	Capacitación	Curso Interpretación y Auditor Interno SGSI	SGSI SGS DEL PERÚ
4	Capacitación	Curso Auditor Líder ISO/IEC 27001:2013	TUV RHEINLAND
5	Capacitación	Curso de gestión de riesgos ISO 31000	PRIME PROFESIONAL
6	Software	Microsoft Office Standard / Visio / Project	MICROSOFT
7	Hardware	Notebook i7 - 320 GB, 8GB RAM	LENOVO
8	Hardware	Desktop + Monitor + Mouse	LENOVO
9	Hardware	Proyector Home Cinema 2030	EPSON

1. PLANIFICAR

1.1. COMPRENDER LA ORGANIZACIÓN Y SU CONTEXTO

La organización es el proyecto que la UGEL brinda a sus usuarios en la administración de la plataforma central y mesa de servicios, cuyos procesos fueron graficados según la Identificación de los procesos de negocio. El SGSI busca identificar aquellos factores internos y externos relacionados a la seguridad de la información, los cuales se muestran a continuación:

CUADRO N° 7 LINEAMIENTOS ESTRATÉGICOS

LINEAMIENTOS ESTRATÉGICOS	OBJETIVOS
VALOR	Incrementar Actividad Asegurar rentabilidad
ESTABILIDAD	Mayor eficiencia
PRESTIGIO	Orientar cultura de servicio al cliente Desarrollar y retener talento

CUADRO N° 8 FACTORES INTERNOS

FACTORES INTERNOS	RELACIÓN CON LA SEGURIDAD
PRODUCTOS Y SERVICIOS	Mayor demanda de seguridad en los servicios de tecnología
ORGANIZACIÓN - PERSONAL	La seguridad de la información requiere la participación de todas las áreas del negocio
FINANZAS - CONTABILIDAD	Se requiere mantener confidencialidad, integridad y disponibilidad de la información financiera-contable

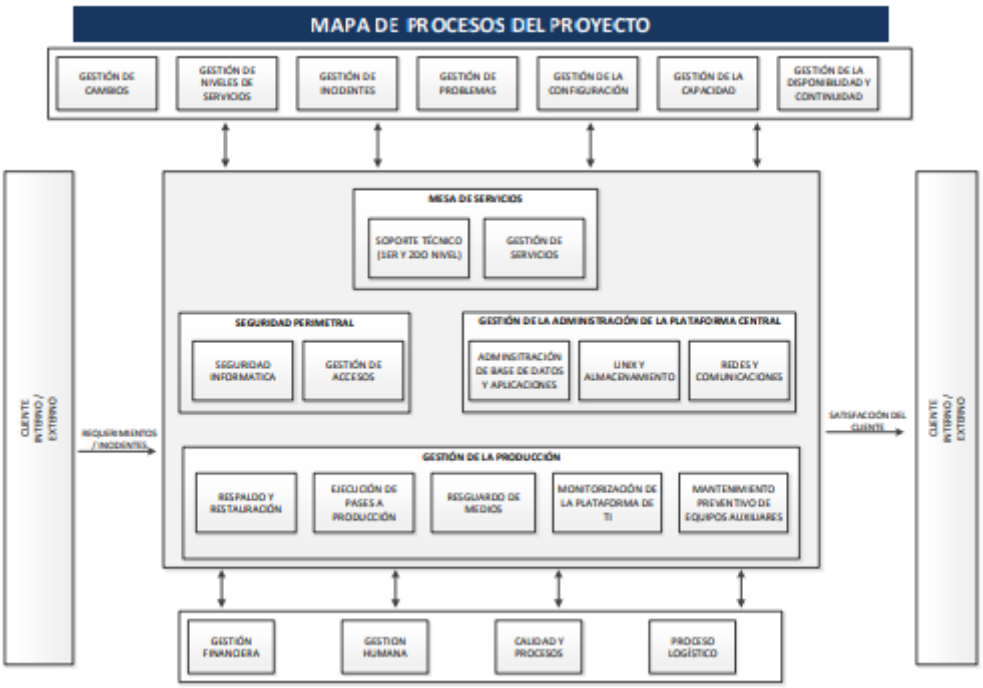
CUADRO N° 9 FACTORES EXTERNOS

FACTORES INTERNOS	RELACIÓN CON LA SEGURIDAD
POLÍTICO – LEGAL	Cumplir con las leyes y regulaciones relacionadas con la seguridad de la información

ECONÓMICO - FINANCIERO	Incremento del Cibercrimen en el Perú está afectando la economía y financieramente a las organizaciones en general
SOCIAL - CULTURAL	Se inicia el desarrollo en una cultura basada en la seguridad.

IDENTIFICACIÓN DE LOS PROCESOS DEL NEGOCIO

Un proceso es un conjunto de tareas lógicamente relacionadas que existen para conseguir un resultado bien definido dentro de un negocio; por lo tanto, toman una entrada y le agregan valor para producir una salida. A continuación, se muestra el diagrama de procesos del proyecto.



Nota: Vásquez (2018).

PROCESOS CORE

Los procesos core son aquellos procesos que dan valor al cliente, es decir, que son la parte principal del negocio, para el presente trabajo tenemos los siguientes:

Gestión de Incidentes: El objetivo es describir las actividades a realizar para restaurar la operación normal del servicio tan pronto como sea posible y minimizar el impacto adverso en las operaciones del negocio, lo que garantiza que los niveles acordados de calidad del servicio se mantengan.

Gestión de Problemas: El objetivo es describir las actividades a realizar para lograr estabilidad en la infraestructura de TI minimizando el impacto que puedan tener los incidentes y problemas en el negocio y prevenir la recurrencia de incidentes y problemas encontrando las causas raíces e iniciando las acciones para mejorar y corregir la situación.

Gestión de Cambio: Asegurar que los cambios que afectan al servicio sean controlados, para ello se deberá analizar los criterios de aceptación, elaborar planes de implementación (responsabilidades, tiempos, recursos, etc.), evaluar el impacto a los demás servicios o al negocio y controlar los riesgos logrando mantener los niveles aceptables de disponibilidad y continuidad del servicio.

Gestión de Configuración: El proceso establece los procedimientos y herramientas para la identificación registro, control y recuperación de elementos de configuración relacionados con los servicios de la organización. De igual forma asegura que todos los elementos de configuración están registrados, proteger y asegurar la integridad de todos los elementos de configuración, monitoriza el estado de todos los elementos de configuración y controla las interrelaciones entre los elementos de configuración.

Gestión de Niveles de Servicio: El objetivo del presente proceso es asegurar que todos los servicios vigentes, se proveen bajo el marco de objetivos y niveles de provisión acordados, alcanzables y medibles; mediante evaluación y revisión constante del cumplimiento de estos objetivos contra los valores logrados en la provisión, para lograr mantener un nivel de calidad permanente en la provisión de los servicios.

Gestión de Capacidad: El objetivo del proceso es asegurar la garantía del servicio a través del cumplimiento de los requisitos de capacidad y rendimiento de manera eficiente en cuanto al tiempo y al costo para que el negocio experimente el valor que se le prometió.

Gestión de Disponibilidad y Continuidad: El principal objetivo es planificar, ejecutar y controlar la disponibilidad del servicio para el cumplimiento de los acuerdos de niveles de servicio (ANS / OLA); así mismo definir las acciones y procedimientos necesarios para garantizar la rápida y oportuna recuperación y puesta en marcha de los sistemas que soportan las operaciones.

PROCESOS OPERATIVOS

Entre los procesos operativos identificados, se encuentra el proceso de cobranzas, el proceso de ventas y el proceso de emisión, pero los dos últimos van de la mano con el proceso de Riesgos, por lo que han sido mencionados anteriormente.

Mesa de Servicios: El alcance del servicio consta de los siguientes puntos:

Proporcionar equipamiento tecnológico a los usuarios y/o los que demande en materia de dispositivos conocidos como equipamiento tecnológico. El servicio de equipamiento tecnológico consta de: alquiler de equipamiento, soporte técnico, así como el mantenimiento preventivo y correctivo. (Desktop, Laptops, Equipos All in One, Lectora de Código de Barras, Estación de trabajo de equipo de diseño, Equipo portátil de diseño).

Atender las solicitudes e incidentes a nivel nacional de los usuarios de acuerdo con el Catálogo de Servicios.

Brindar el soporte en sitio sobre el equipamiento tecnológico brindado por el contratista para el servicio (instalación de hardware y software en sitio, traslados, incidentes microinformáticos, reparaciones, etc.).

Administración de la Plataforma Central

Base de Datos:

- Administración, monitoreo, configuración y gestión de accesos de la base de datos
- Monitoreo proactivo de las bases de datos en base
- Mantenimientos preventivos y correctivos de las bases de datos
- Afinamiento de la Base de datos
- Auditorías a las bases de datos
- Servidores Unix y Linux:
- Gestión de los ambientes (Creación / Modificación / Eliminación de ambientes)
- Monitoreo proactivo y automatizado de los servidores
- Mantenimientos preventivos y correctivos.
- Aplicaciones:
- Creación / Modificación / Eliminación de las aplicaciones
- Monitoreo y afinamiento proactivo de los Servidores de Aplicaciones, Procesos y Servidores de Gestión documental.

- Mantenimientos preventivos y correctivos de los Servidores de Aplicaciones, Procesos y Servidores de Gestión documental.
- Modificaciones en las aplicaciones y configuración de las mismas (incluye accesos)
- Redes y Comunicaciones
- Administración de servidores físicos / virtuales Windows, VMWare, otros.
- Mantenimiento de Licencias y Soporte Técnico
- Implementar un servidor de archivos para disponer de la información necesaria de cada área de manera centralizada.
- Realizar mantenimiento periódico físico y lógico a los equipos (hardware) que soportan el servicio.
- Mantener actualizado todo el hardware que soporta los servicios con las últimas versiones estables de BIOS y/o Firmware
- Mantener actualizado todo el software que soporta los servicios con las últimas versiones, hotfix, support packages, service pack y parches, para garantizar la disponibilidad y estabilidad del servicio.
- Monitorear los componentes de todos los servicios (hardware, software)
- Monitorear permanentemente la atención a incidentes y requerimientos.
- Mantener un inventario actualizado de todo el hardware y software que administre (switches, teléfonos IP, Access Point, equipos de videoconferencia, Rack de comunicaciones).
- Seguridad Perimetral
- Atender los requerimientos de creación, modificación y eliminación de cuentas de accesos.
- Atender en el momento adecuado las vulnerabilidades detectadas.
- Realizar el mantenimiento preventivo del equipamiento que soporta los servicios de Seguridad Perimetral, Acceso a Internet y acceso remoto.
- Mantener actualizados los equipos con las últimas actualizaciones liberadas y estables.
- Distribuir la actualización de antivirus a los servidores y estaciones de trabajo de la ONP y de las empresas que le brindan servicios.

- Gestión de las Operaciones
- Gestión de acceso físico al data center
- Pases a QA y producción
- Ejecución de scripts
- Respaldo de información
- Restauración de información
- Traslado, almacenamiento y custodia de medios magnéticos
- Mantenimiento de los equipos de apoyo (UPS, aire acondicionado, extintores, cámara de vigilancia, panel eléctrico, etc.)
- Monitoreo de los elementos del servicio.

PROCESOS DE SOPORTE

Procesos que brindan soporte o apoyo a los procesos operativos, entre los cuales podemos mencionar:

Gestión Financiera: Evaluar y controlar los costos asociados a los servicios de forma que se ofrezca un servicio de calidad a los clientes con un uso eficiente de los recursos de TI necesarios; además el proceso indicará el establecimiento del presupuesto del servicio.

Gestión Humana: Gestiona las contrataciones del personal, asimismo evalúa las competencias de las personas que laboran en el proyecto.

Calidad y Procesos: Realiza el seguimiento del proyecto, identifica oportunidades de mejora y evalúa la eficacia del sistema de gestión implementado.

Proceso Logística: Gestionar las relaciones con los suministradores durante todo su ciclo de vida desde la elección hasta el término de las relaciones contractuales de manera que éstas satisfagan los acuerdos de niveles de servicios establecidos con nuestros clientes actuales y futuros.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El servicio de administración de la plataforma central y mesa de administración de servicios responsable de administrar la plataforma central y de atender los requerimientos e incidentes reportados por los usuarios finales (cliente) administrados por la UGEL, consciente de la importancia de proteger la información

importante para el negocio, decidió implementar un sistema de gestión de seguridad de la información (SGSI), para lo cual suscribe la presente política:

La alta dirección ha adoptado una Política de Seguridad de la Información, para asegurar la protección de la información en la prestación de los servicios del Centro de Datos y Comunicaciones; y Mesa de Administración de Servicios, por ello se compromete en:

- ❖ Cumplir con las regulaciones aplicables en torno a la seguridad de la información.
- ❖ Mejorar continuamente la eficacia del SGSI
- ❖ Mantener una cultura organizacional que aliente a todos los trabajadores a asumir una responsabilidad por la seguridad de la información
- ❖ Mejorar continuamente el SGSI
- ❖ Proteger la información y sus activos de información a través de un SGSI para garantizar su confidencialidad, integridad y disponibilidad.
- ❖ Dar respuesta inmediata a los incidentes que se presenten

ROLES Y RESPONSABILIDADES DEL SGSI

Comité del SGSI

Comité Conformado por: Gerente del Proyecto, Jefe de Proyecto y el Oficial de Seguridad de la Información; cuyas principales responsabilidades son las siguientes:

- ✓ Establecer, revisar, aprobar y comunicar la política y los objetivos de seguridad de la información y la importancia de su cumplimiento, asegurando que estos sean compatibles con el plan estratégico de la organización, y la importancia de su cumplimiento.
- ✓ Asegurar que los requisitos del sistema de gestión de la seguridad de la información están integrados a los procesos de la organización definiéndolos en los procedimientos y políticas del SGSI.
- ✓ Asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información están disponibles.
- ✓ Dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información.
- ✓ Promover la mejora continua.

- ✓ Revisar el SGSI de manera periódica (mínimo 1 vez al año), para la toma de decisiones para la mejora del sistema.
- ✓ Asignar roles específicos y responsabilidades para la seguridad de información en la organización.
- ✓ Revisar los resultados de las evaluaciones de riesgo y aprobar el tratamiento de los riesgos identificados, justificando aquellos que no serán tratados (aceptados).
- ✓ Revisar los hallazgos de auditoria del SGSI y definir las acciones necesarias al respecto.

Oficial de Seguridad de la Información

- ✓ Informar a la Alta Dirección sobre el desempeño del SGSI.
- ✓ Controlar los documentos del SGSI.
- ✓ Consolidar los resultados de la gestión del SGSI y comunicar esta información a las partes interesadas.
- ✓ Organizar la realización de las auditorías internas y externas del SGSI.
- ✓ Promover la capacitación y concientización del personal acerca de la gestión de la seguridad de la información.
- ✓ Liderar los proyectos de mejora del SGSI.
- ✓ Gestión de los acuerdos de niveles de servicio.

Propietario del Activo de Información

- ✓ Controlar el uso y seguridad de los activos que le son asignados para la creación, procesamiento, transmisión y almacenamiento de información relacionadas al proceso o área que le compete.
- ✓ Autorizar el uso del activo de información del cual es propietario, bajo responsabilidad, de manera que se preserve la seguridad de la información.
- ✓ Entender y abordar los riesgos/oportunidades relacionados a la seguridad de la información de los activos del proceso o área de su responsabilidad.
- ✓ Asegurar que el activo de información se utiliza únicamente para los propósitos de la organización.

Custodio del Activo de Información

- ✓ Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos para el uso aceptable de los activos de información que le compete.

- ✓ Hacer uso correcto y seguro del activo de información que le compete.
- ✓ Comunicar al propietario del activo de información las amenazas y vulnerabilidades que identifique durante el desarrollo de sus actividades.
- ✓ Facilitar las actividades de implementación de controles de seguridad de la información sobre los activos de su competencia.

Propietario del Riesgo

- ✓ Asegurar que se implementen los controles de seguridad definidos para reducir a un nivel aceptable el riesgo que le fue asignado.

ACCIONES PARA ABORDAR LOS RIESGOS Y OPORTUNIDADES

A continuación, se detalla la metodología diseñada por el autor del presente trabajo para la gestión de riesgos de seguridad de la información el cual comprende las siguientes etapas:

- ✓ Identificar los activos y/ grupos de activos de información relevantes para el negocio.
- ✓ Identificar los eventos potenciales que pueden tener un efecto positivo o negativo sobre los activos de información
- ✓ Determinar la probabilidad de ocurrencia del evento.
- ✓ Estimar el nivel de impacto en función de la confidencialidad, integridad o disponibilidad.
- ✓ Estimar el nivel del riesgo
- ✓ Evaluar la prioridad para la atención del riesgo
- ✓ Identificar las acciones necesarias (Tratamiento de los riesgos)
- ✓ Calcular el riesgo residual

CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Planificación de la continuidad de la Seguridad de la Información: La continuidad de la seguridad de la información es planificada para ello se elaboran Planes de Continuidad y Disponibilidad con la finalidad de establecer los requisitos para asegurar la continuidad y disponibilidad de la operación, incluida la seguridad de la información.

Implementación de la continuidad de la seguridad de la información: Se establece, documenta, implementa y mantiene procesos, procedimientos y

controles para asegurar el nivel necesario de continuidad; para la seguridad de la información durante una situación adversa.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información: Los planes de continuidad y disponibilidad son probados, revisados y actualizados de manera anual. Posteriormente, el personal a cargo elabora un informe acerca del resultado obtenido y lo presenta al responsable del Área o Proyecto para la toma de decisiones correspondiente.

Cuando se encuentren resultados no favorables de dichas pruebas, el responsable del Área o proyecto se encargará de gestionar la corrección de dichos resultados.

Disponibilidad de las instalaciones de procesamiento de la Información los cuales tienen redundancia debido a que cada site cuenta con dos sistemas eléctricos independientes, lo que permite cumplir con los requisitos de disponibilidad de los servicios que brinda.

AUDITORIA INTERNA

Proceso que permite verificar en forma objetiva el cumplimiento y efectividad de todos los procesos que conforman el sistema de gestión de seguridad de la información.

Los lineamientos para la realización de la auditoría interna son los siguientes;

La auditoría interna podrá ser ejecutada por un auditor y/o equipo auditor externo de acuerdo con los requisitos que establezca la organización y debe contar con los siguientes perfiles:

Debe ser liderada por un Líder Auditor y el equipo auditor que deben de ser Auditores Internos certificados en el Sistema de Gestión que se auditará.

- ✓ Demostrar habilidades y conocimientos suficientes, relacionados con la disciplina y la aplicación de métodos, técnicas, procesos y prácticas específicos del sistema de gestión a examinar, permitiéndole generar hallazgos y conclusiones apropiados. (Lo cual se evidenciará a través de certificados de cursos especializados correspondientes al Sistema de Gestión que será Auditado).
- ✓ Tener experiencia del auditor en auditorías internas de procesos (evidencia en horas).

Toda la información generada en el proceso deberá almacenarse en el repositorio correspondiente

Los hallazgos que figuran en los informes deben cumplir con lo siguiente:

- ✓ Deben redactarse de tal forma que sean entendidos fácilmente por el auditado y que posteriormente el área responsable del tratamiento pueda analizar y plantear soluciones acertadas al problema.
- ✓ Las notas deben de ser: objetivas, claras, concretas, concisas, precisas y útiles para el auditado.
- ✓ Deben de contar con la evidencia objetiva específica según sea el caso (código y nombre de documento, ubicación, fecha, etc.)

Los informes finales deberán enviarse al área como máximo 7 días después de finalizada la auditoria.

La Gerencia o Área responsable auditada debe asegurarse de que se establece el tratamiento para los hallazgos, es decir: se designa un responsable, se realizan las correcciones y se establecen las acciones correctivas necesarias para eliminar las no conformidades y sus causas.

A continuación, se muestra el proceso de auditoría interna implementado:

Programar Auditorías Internas

El Oficial de Seguridad de la Información determina el número de auditorías internas que se realizarán a lo largo del año.

Elaborar Programa de Auditorías

El oficial de seguridad de la información elabora el programa de auditorías en función a la naturaleza e importancia de la actividad sometida a auditoría. Existen tres tipos de enfoque de auditoría:

A. Por áreas: Evalúa el grado de conformidad de un área con respecto a todos los procedimientos en los que participe.

B. Por procesos: Evalúa el grado de efectividad de las actividades de un servicio brindado de acuerdo con los procedimientos especificados.

C. Por requisitos de la norma: Evalúa el grado de conformidad que muestre el área auditada con respecto a un requisito específico de la norma.

Coordinar participación del equipo auditor y Elaborar Plan

EL auditor Líder coordina la participación del equipo auditor, asimismo, se encarga de elaborar el Plan de Auditorías, el cual considera lo siguiente:

1. Tipo de Auditoría y número de la misma.
2. Mes y año de realización

3. Enfoque de la auditoría
4. Objetivo de la auditoría
5. Fechas y horas aproximadas de realización.
6. Integrantes del equipo auditor (independientes y sin responsabilidad directa al área auditada)
7. Área o departamento a ser auditados.
8. Procesos afectados (según enfoque)
9. Requisito de la norma a ser evaluado (según enfoque)
10. Representantes del auditado
11. Observaciones (si fuera necesario)

Plan de auditoria

Sistema de Gestión :
Tipo de Auditoria :
Mes/Año :
Jefe Auditor :
Enfoque :
Objetivos :

Dia	Auditores	Hora	Proceso Área / Departamento	Procedimientos, Instrucciones a Auditar	Requisitos del Sistema	Responsable de Área/Proc. Auditado

Observaciones :

Coordinar fecha y hora

El auditor líder coordina con el auditado la fecha y hora exacta en que se realizarán las auditorías, para asegurar que el representante esté presente durante la ejecución de la auditoría. Si existiera algún cambio durante el proceso se actualiza el Plan de Auditorías y se comunica a los involucrados.

Enviar Plan de Auditoría

Una vez coordinados la fecha y hora para la realización de las auditorías, el auditor líder envía el Plan de Auditoría a los auditores, auditados y demás involucrados o interesados.

Realizar la auditoría

Según las fechas establecidas, el equipo auditor procede a la realización de la auditoría y a la recopilación de las evidencias objetivas que permitan identificar no-conformidades, las situaciones destacables, verificar el estado de las notas abiertas y revisar la eficacia de las acciones cerradas. Al término de la auditoria el auditor interno comentará de manera general con el auditado los hallazgos y registra los hallazgos en el Informe de Auditorias, y lo envía al Jefe Auditor.

Centralizar la información del equipo

El auditor líder centraliza, revisa y verifica que los hallazgos de su equipo no se repitan, se entiendan y estén bien redactados. Además, simplifica las notas si es factible, valida que existan las evidencias y valida la categoría de nota asignada.

Desplegar hallazgos con auditados

El auditor líder envía el informe de auditoría vía correo electrónico al auditado para que éste revise y dé su conformidad. El informe se enviará al auditado a más tardar 5 días hábiles luego de realizada la auditoría.

ACTUAR

NO CONFORMIDADES Y ACCIONES CORRECTIVAS

Se han definido los siguientes escenarios como “No Conformidad”:

Incumplimiento de algún requisito legal y/o contractual: Situación donde se evidencia un incumplimiento de algún requisito legal o contractual aplicado al servicio o al Sistema de Gestión de Seguridad de la Información.

Incumplimiento de las Políticas y/o normas de seguridad: Situación donde se evidencia un incumplimiento de las políticas, normas, procedimientos, planes, controles, y similares, definidos dentro del Sistema de Gestión de Seguridad de la Información.

Incumplimiento de los objetivos de seguridad: Situación donde se evidencia que los resultados de medición de los objetivos de seguridad no fueron satisfactorios conforme a las metas establecidas.

Resultados de auditorías internas / externas: No conformidades detectadas por el equipo auditor o auditores en la realización de auditorías internos o externas.

Resultados de investigación de incidentes: Situación donde como resultado de la investigación de incidentes se determine no conformidades en los procesos o

actividades definidas dentro del Sistema de Gestión de Seguridad de la Información.

Resultados de monitoreo y seguimiento: Situación donde como resultado del monitoreo se evidencie eventos de seguridad de manera sistemática y con potencialidad de vulnerar las políticas de seguridad de la información.

Resultados de la revisión por la Dirección: Situación donde se determina que existe algún incumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información.

Incumplimiento de acciones establecidas en las solicitudes de acciones correctivas: Situación donde se evidencie incumplimiento en los plazos o acciones no tomadas, sin justificación, que se definieron en las solicitudes de acciones correctivas / preventivas.

MEJORA CONTINUA

El objetivo de este proceso es mejorar continuamente la eficacia del sistema de gestión de seguridad de la información, considerando principalmente los siguientes términos:

- Los procesos para el aumento del desempeño de la organización, de esta forma beneficiar a las partes interesadas.
- Los procesos para el aumento de la seguridad de la información.

El proceso de mejora continua es el siguiente:

Identificar Oportunidades de Mejora En esta etapa, se definen claramente la oportunidad de mejora y reconocen la importancia de este. Se pueden utilizar principalmente Tormentas de Ideas, Encuestas y Entrevistas, se seleccionan las oportunidades de mejora según las siguientes fuentes:

- ✓ Elevación de los Objetivos.
- ✓ Auditorías Internas / Externas.
- ✓ Encuestas a Clientes.
- ✓ Reclamos e Incidentes.
- ✓ Sugerencias del Personal.

Adicionalmente, los criterios que se toman en cuenta son:

- ✓ La complejidad de la oportunidad de mejora.
- ✓ El impacto que la oportunidad de mejora tiene en los clientes, cómo los afecta, a cuántos y a qué nivel.

- ✓ El tiempo que tomaría solucionarlo.

Se elabora una lista de oportunidades de mejora y se asigna a un responsable o un grupo de responsables y el líder quien propondrá la fecha límite de solución de la oportunidad de mejora y los recursos necesarios para la ejecución de este.

Proponer Plan de Acción:

Se discuten las acciones que deberán ser tomadas. También es importante analizar los posibles efectos colaterales de las acciones propuestas y las actividades adicionales que se tomarán para contrarrestar los mismos si fuese ésta la solución que se adoptase. Las acciones propuestas pueden ser analizadas también a partir del costo/beneficio y el tiempo de implementación y la eficacia de la misma, es decir, si logra el resultado para la cual fue aplicada, eliminando la causa raíz de la oportunidad de mejora.

Teniendo en cuenta estos aspectos, se procede a elaborar el plan de acción a través del Cronograma de Actividades, que incluye actividades detalladas de lo que se debe hacer, las fechas propuestas o duración estimada de cada actividad, responsable de la ejecución de cada una, de ser posible la forma en que deberá realizarse esta actividad, el costo de cada actividad, la meta a ser alcanzada y los mecanismos de control y verificación para determinar si la acción fue efectiva.

Aprobar Plan de Acción Propuesto:

El comité del SGSI deberá aprobar el plan de trabajo para la implementación de la mejora.

Ejecutar Plan de Acción Aprobado

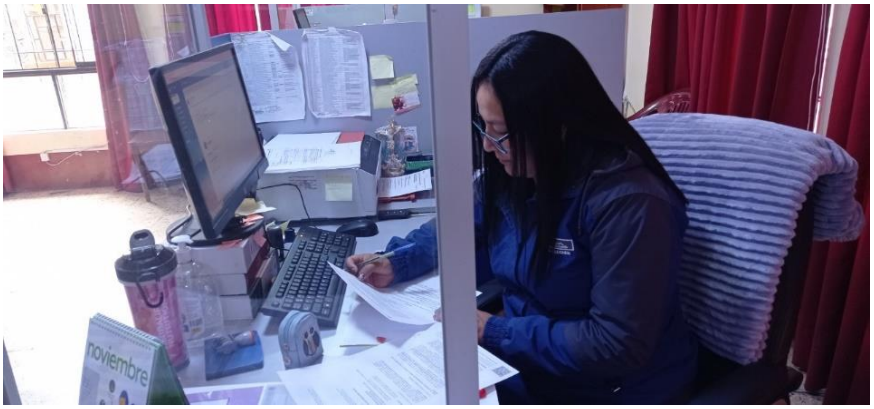
En esta fase se implanta el Plan de Acción Aprobado. Para ello debe asegurarse de que todos los que se vean afectados entiendan la razón por la cual está siendo implantada. El equipo de mejora hace un seguimiento a la implantación del plan asegurándose de que las soluciones sean implantadas de acuerdo con el plan. Cuando al hacer el seguimiento, se encuentra que no se están logrando los objetivos deseados, se hacen los ajustes al Plan.

Verificar Mejora Efectiva

El Equipo de Mejora compara los resultados utilizando los datos recogidos antes y después de la acción tomada para verificar la efectividad de la acción y la reducción de los resultados indeseables. Si el resultado de la acción fue tan satisfactorio como se esperaba se envía el Informe al Comité del SGSI con el detalle correspondiente.

CIERRE DEL PROYECTO

El día 28-10-2022 se procedió al cierre del proyecto de “Implementación de un sistema de gestión de seguridad de la información para proteger la información en los procesos de tecnología de la información de la UGEL.



Seguridad de la información (ISO27001)

Norma	Fases	Procesos	Actividades	Evaluación
Seguridad de la información (ISO27001)	1 Diagnóstico	Diagnóstico GAP	✓ Elaboración del informe del diagnóstico ✓ Presentación del informe de diagnóstico ✓ Actualización del cronograma de trabajo	Check List de cumplimento y avances
	2 Planificar	Contexto de la organización	✓ Comprender la organización y su contexto ✓ Comprender las necesidades y expectativas de las partes interesadas ✓ Determinar los alcances del SGSI	
		Liderazgo	✓ Liderazgo y compromiso ✓ Políticas ✓ Roles organizacionales, responsabilidades	
		Planear	✓ Acciones para abordar los riesgos y oportunidades ✓ Declaración de aplicabilidad (Controles)	
		Soporte	✓ Competencias ✓ Conocimiento ✓ Comunicación ✓ Información documentada ✓ Elaboración de documentos del SGSI	
	3 Hacer	Operación	✓ Controles y planificación organizacional	
	4 Medir	Evaluación del desempeño	✓ Plan de medición del SGSI ✓ Medición del SGSI	
		Auditoría interna	✓ Programa de auditoría	

			✓ Plan de auditoría ✓ Ejecución de la auditoría interna ✓ Informe de auditoría ✓ Revisión de la gestión	
	5 Actuar	No conformidades y acciones correctivas	✓ Análisis de causas ✓ Seguimiento y cierre	
		Mejora continua	✓ Identificar oportunidades de mejoras ✓ Plan de acción ✓ Implementar mejora	
	6 Auditoría	Plan de auditoría	Ejecución de auditoría externa Informe de auditoría Cierre del proyecto	

Fuente: Adaptado de Vásquez (2018).

Anexo 09: Calculo de la muestra

Fórmula para la determinación del tamaño de muestra:

$$n = \frac{N * Z_{\propto}^2 * p * q}{d^2 * (N-1) + Z_{\propto}^2 * p * q}$$

Donde:

n=Tamaño de la muestra.

z = Nivel de confianza 95% siendo Z=1.96

p = 0,5. Probabilidad que el estudio se realice al 50%.

q = 1– p = 1 – 0,5 proporción de la población con la característica deseada.

N = 47. Tamaño de la población.

d= Error susceptible de cometer 5% (d= 0.05)

Remplazando valores:

$$n = \frac{47 * 1.96_{\propto}^2 * 0.5 * 0.5}{0.05^2 * (47-1) + 1.96_{\propto}^2 * 0.5 * 0.5}$$

n = 42 Trabajadores la entidad

Anexo 10: Base de datos

Cuestionario para medir la gestión de la información en el Pre Test

N°	Disponibilidad					Autenticidad					Integridad					Confidencialidad					Trazabilidad			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	2	3	2	2	2	1	2	2	3	2	3	2	3	2	2	4	2	3	2	3	2	3	2	3
2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	3	3	3	2	4	3	2	3	2
3	2	3	4	2	3	2	3	3	3	2	3	2	3	2	2	2	3	2	3	4	2	3	2	3
4	2	3	2	3	2	3	2	3	2	3	3	3	2	3	2	1	1	1	2	2	2	4	4	2
5	3	2	3	2	2	2	3	2	3	2	3	2	3	2	3	4	2	3	2	3	2	3	4	2
6	2	1	2	1	1	1	2	2	2	3	2	2	2	2	3	2	3	2	2	4	4	2	3	2
7	2	2	3	2	3	2	3	2	2	2	2	2	2	3	2	2	2	2	1	2	2	2	2	2
8	3	3	3	3	3	2	3	2	3	2	3	3	3	3	4	4	3	2	2	2	3	2	3	2
9	3	3	2	2	2	2	1	1	2	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2
10	2	3	2	3	2	3	3	3	3	2	3	2	1	1	2	2	3	3	3	2	1	1	1	2
11	3	1	2	3	2	3	2	3	2	3	2	3	2	4	2	3	2	3	2	3	2	3	2	3
12	2	4	4	4	3	4	3	2	3	2	3	2	3	2	2	3	2	3	2	4	4	2	3	2
13	1	2	3	2	2	4	4	2	3	2	3	2	2	3	2	3	2	3	2	3	2	3	2	3
14	2	3	2	3	2	3	2	3	2	3	2	2	2	3	3	3	3	4	4	4	3	2	2	1
15	1	2	2	2	2	3	2	3	2	3	2	3	2	3	4	2	3	2	3	2	2	2	2	2
16	2	3	2	3	2	3	3	3	3	2	3	2	2	1	1	1	1	2	2	3	2	3	2	3
17	3	2	3	4	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	2
18	3	2	3	2	3	2	2	1	3	2	3	2	2	2	2	3	2	2	2	3	2	2	2	3
19	2	3	2	3	4	2	3	2	3	2	3	2	3	2	3	2	3	2	3	4	4	4	4	4
20	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	1	4	5	4	4	4
21	2	2	2	2	1	1	1	1	5	5	5	4	4	4	4	5	4	2	4	5	3	2	3	2
22	2	3	2	3	2	3	2	3	2	5	4	5	4	3	2	4	5	4	4	4	4	5	5	5
23	1	2	2	2	3	2	2	2	3	2	2	2	2	3	2	3	2	3	2	3	2	3	2	3
24	3	2	3	2	3	2	3	2	3	2	3	2	1	1	1	1	1	2	2	2	3	2	2	1
25	2	3	2	3	2	3	2	2	2	2	1	1	1	2	2	3	4	2	3	2	2	2	2	3

26	4	5	4	4	4	5	2	2	3	3	3	3	2	3	2	2	1	1	1	1	2	2	3	2
27	2	2	2	3	2	3	2	2	2	3	2	3	2	3	2	3	2	3	2	3	2	4	2	3
28	2	3	2	3	2	2	2	2	3	2	3	2	3	2	2	1	1	1	2	2	2	2	3	2
29	2	3	2	1	1	1	2	3	2	3	3	4	4	2	2	1	1	1	2	1	2	1	2	2
30	5	5	5	5	5	5	5	5	5	4	4	4	4	4	4	4	5	5	5	5	5	5	5	4
31	2	3	2	2	2	3	2	2	2	1	1	1	2	2	3	2	3	2	3	2	3	2	3	2
32	2	2	3	2	3	2	3	2	3	2	2	2	3	2	1	1	1	1	1	1	2	2	2	3
33	2	2	2	1	1	1	2	2	2	2	3	2	2	2	2	1	1	1	2	2	2	3	2	3
34	2	2	3	2	3	2	2	2	1	1	1	1	2	2	2	3	2	2	1	1	1	2	2	2
35	2	3	2	2	2	1	1	1	2	2	3	2	3	2	3	2	3	2	2	2	2	2	2	2
36	3	2	3	2	3	2	3	3	3	2	3	2	2	2	3	2	2	1	1	1	1	2	2	1
37	2	2	2	1	1	1	2	2	2	2	2	3	2	3	2	3	2	3	2	2	1	1	1	2
38	2	3	2	3	2	3	2	1	1	1	2	2	2	2	3	2	2	2	3	2	2	2	3	2
39	3	2	2	2	2	2	2	1	1	1	2	2	2	3	2	3	2	3	2	3	2	3	2	3
40	3	2	3	2	2	1	1	1	1	2	2	2	3	2	3	2	2	1	1	1	2	2	2	2
41	2	2	2	1	1	1	2	2	3	2	3	2	2	2	2	2	3	3	3	2	2	2	2	2
42	2	2	2	3	2	3	2	3	2	3	2	3	2	3	2	3	2	2	4	1	1	2	2	2

Cuestionario para medir la gestión de la información en el Post-Test

N°	Disponibilidad					Autenticidad					Integridad					Confidencialidad					Trazabilidad			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	4	3	3	5	4	4	4	4	4	4	3	3	3	5	4	4	4	4	4	3	3	3	4	4
2	3	3	3	4	4	4	4	5	3	3	3	3	4	4	4	4	4	5	3	3	3	4	4	4
3	4	4	4	4	2	3	3	3	2	3	3	3	4	4	4	4	4	3	3	3	3	3	5	4
4	3	3	4	4	5	3	3	3	4	4	4	4	4	4	5	5	3	3	3	3	4	4	4	5
5	4	4	4	4	4	4	3	3	3	3	3	3	5	5	5	5	3	3	3	3	3	3	5	5
6	4	5	5	5	5	5	4	4	4	4	4	5	4	5	5	5	5	5	5	4	4	5	4	5
7	5	4	4	4	4	4	4	4	4	5	4	4	4	5	5	5	3	3	3	3	5	4	4	5
8	3	4	4	4	4	3	3	3	3	3	4	4	4	4	4	3	2	4	4	4	2	3	3	5
9	3	4	4	4	4	2	3	3	3	3	2	2	2	2	3	2	3	3	3	3	3	3	3	3
10	2	4	3	3	3	3	2	3	2	3	3	3	3	3	3	2	1	1	1	2	2	3	3	2
11	4	4	4	4	5	4	5	5	5	3	3	3	5	5	5	4	4	4	5	4	4	5	4	5
12	4	4	5	4	4	4	4	4	5	3	3	3	3	4	4	4	5	3	3	3	3	3	2	4
13	4	4	4	5	5	5	5	5	5	5	5	5	5	4	4	4	5	4	5	5	5	5	5	5
14	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	2	2	2	2	2	2	3	2
15	5	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	4	4	4	5	3	4	5	4
16	4	4	4	4	4	4	5	5	3	3	3	3	3	3	3	4	4	4	4	5	5	3	3	4
17	4	3	3	3	5	5	5	4	4	4	3	3	3	3	3	5	5	4	4	4	4	5	4	5
18	4	5	5	5	5	5	3	3	3	3	3	4	4	4	4	4	5	3	3	3	3	4	4	4
19	4	4	4	4	5	4	4	3	3	3	3	5	5	5	4	4	4	4	5	4	5	4	5	4
20	4	5	5	5	5	3	3	3	3	3	5	5	5	4	4	4	4	5	5	3	3	3	3	5
21	1	1	1	1	2	2	2	2	2	2	1	1	1	1	1	1	1	2	1	1	1	1	1	2
22	5	5	3	3	3	5	5	5	5	5	3	3	3	4	4	4	4	4	4	4	5	5	5	5
23	4	3	3	3	5	5	5	4	4	4	5	4	4	5	5	5	3	3	3	3	5	5	5	5
24	4	5	4	4	4	4	4	4	4	4	4	5	5	5	5	5	4	4	4	5	5	5	3	4
25	4	3	3	5	5	4	4	4	3	3	3	3	5	4	4	4	3	3	3	3	5	4	4	4
26	4	4	4	4	4	5	3	3	3	4	4	5	4	4	4	4	5	5	3	3	3	5	5	5

27	3	3	3	5	4	4	4	3	3	3	3	5	4	4	4	3	3	3	2	3	2	3	2	3
28	4	4	4	5	5	5	5	3	3	3	4	4	4	5	5	5	3	3	3	4	4	4	5	3
29	3	3	3	5	5	4	4	4	4	4	3	3	3	5	4	4	4	2	3	2	3	2	3	2
30	5	3	3	3	4	4	4	5	5	3	3	3	3	4	4	4	4	5	5	5	3	3	3	4
31	4	4	4	4	4	4	3	3	3	5	5	5	5	5	5	5	4	4	4	5	4	5	4	5
32	3	3	3	3	3	3	3	3	3	3	4	4	4	5	5	5	3	3	3	3	3	4	4	4
33	4	4	5	5	5	5	5	4	4	4	4	5	5	5	5	5	5	5	2	3	2	3	2	3
34	5	4	5	4	5	4	4	4	4	5	5	5	3	3	3	3	3	3	3	2	3	2	3	4
35	4	4	4	5	4	4	4	5	5	5	5	5	5	4	4	4	3	3	3	2	2	2	3	2
36	5	5	3	3	3	3	3	5	5	4	4	4	4	4	4	5	5	3	3	3	4	4	4	4
37	4	4	4	4	4	3	3	3	3	5	5	5	4	4	4	4	4	5	5	5	5	3	3	5
38	4	4	4	4	4	5	5	5	5	3	3	3	3	3	4	4	5	5	5	2	3	2	3	2
39	4	4	5	4	4	4	5	5	5	5	3	3	3	5	5	4	4	4	4	5	4	5	4	5
40	4	5	5	5	5	5	5	4	4	4	5	5	5	5	5	5	5	5	4	4	5	4	5	5
41	4	4	4	5	4	4	4	5	5	5	3	3	3	3	5	5	5	5	4	5	4	4	5	4
42	5	3	3	3	3	3	3	3	3	4	4	4	4	4	5	5	5	5	3	3	3	5	5	5

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "ISO 27001:2013 para la Gestión del Manejo de Información en la UGEL Bolognesi, Ancash 2023", cuyo autor es IBARRA CAQUI LUCIO, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 06 de Enero del 2023

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 06-01-2023 15:00:07

Código documento Trilce: TRI - 0511379

INVESTIGA UCV