UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba', 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Abad Chavez, Manuel (orcid.org/0000-0001-6717-6068)

Cruz Calderon, Franklyn (orcid.org/0000-0002-2202-3022)

ASESOR:

Dr. Agreda Gamboa, Everson David (orcid.org/0000-0003-1252-9692)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo Económico, Empleo y Emprendimiento

TRUJILLO - PERÚ

2022

Dedicatoria

A mi Madre, gracias a su esfuerzo he logrado llegar hasta esta instancia de mis estudios.

A todas las personas, que me brindaron todo su apoyo para lograrlo.

Manuel

A Dios, gracias a él he logrado concluir mi carrera.

A mis Padres Grimaldo y Eva, porque ellos han dado razón a mi vida, por sus consejos, su apoyo incondicional, todo lo que hoy soy es gracias a ellos.

A mis hermanas y sobrinas por sus palabras y compañía.

A mi Compañera de vida, por su amor y por brindarme el tiempo necesario para realizarme profesionalmente.

A mi hijo ya que él es mi motor de mi vida.

A mis amigos, compañeros, y a todas aquellas personas que de una u otra manera contribuyeron para el logro de mis objetivos.

Franklyn

Agradecimiento

A la Universidad César Vallejo por su apoyo en la obtención de nuestro título profesional de Ingenieros de Sistemas.

A la UGEL ‘Utcubamba’ por facilitarnos la información para el desarrollo de esta investigación.

A nuestro asesor de tesis por sus recomendaciones y permanente orientación en el desarrollo de la investigación.

Los autores

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

El objetivo de la investigación fue acrecentar la seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022 mediante la aplicación de la norma internacional ISO/IEC 27002:2013. El tipo de investigación fue aplicada y de diseño preexperimental. La muestra estuvo constituida por 18 empleados que laboran actualmente en la institución pública. El instrumento empleado fue el Cuestionario. Se desarrolló la solución tecnológica propuesta empleando la norma internacional ISO/IEC 27002:2013. Entre los resultados se tuvo: Se consiguió acrecentar la seguridad informática de la entidad pública en estudio con respecto al grado de confidencialidad, integridad y disponibilidad de la data, obteniéndose específicamente puntuaciones de 2.95 puntos (Δ 59.00%), 3.09 puntos (Δ 61.80%) y 3.25 puntos (Δ 65.00%) respectivamente comprobándose que la aplicación de la solución propuesta acrecentó la seguridad informática de la entidad pública en estudio.

Palabras clave: Norma internacional, ISO/IEC 27002, Seguridad informática, UGEL.

Abstract

The objective of the research was to increase the information security of the Local Educational Management Unit 'Utcubamba' in the year 2022 through the application of the international standard ISO/IEC 27002:2013. The type of research was applied and pre-experimental design. The sample consisted of 18 employees currently working in the public institution. The instrument used was the questionnaire. The proposed technological solution was developed using the international standard ISO/IEC 27002:2013. Among the results were: It was possible to increase the information security of the public entity under study with respect to the degree of confidentiality, integrity and availability of data, specifically obtaining scores of 2.95 points (Δ 59.00%), 3.09 points (Δ 61.80%) and 3.25 points (Δ 65.00%) respectively, proving that the application of the proposed solution increased the information security of the public entity under study.

Keywords: International standard, ISO/IEC 27002, IT security, UGEL.

I. INTRODUCCIÓN

PMG-SSI (2016) manifiesta que, la importancia de la información renovada, exacta y real es la esencia para el correcto desempeño de las múltiples funciones de una compañía en sus diferentes departamentos, sectores y tareas. No obstante, resulta también fundamental mantener esta data de manera segura a fin de que no sea extraviada, robada o dañada. Cuando se habla de seguridad informática, aparece en la mente la norma internacional ISO 27002. Este estándar es super importante en la industria porque conforma una lista de buenas prácticas que, con base en la experiencia, define un conjunto de objetivos de monitoreo y revisiones que consideran todos los riesgos. requerimientos de gestión del estándar ISO 27001. El estándar internacional ISO 27002 en su adaptación del 2013 se encuentra estructurada en 14 capítulos y un total de 114 elementos de control que deben tenerse en cuenta al considerar su posible implementación.

CSS (2017) sostiene que, evitar el hurto de la data como ahorros bancarios, detalles de tarjetas crediticias, contraseñas, informes laborales, salarios, etc., lo cual es imprescindible hoy en día. Muchas de nuestras actividades diarias dependen de la seguridad informática para el flujo de toda la data y, como punto de partida, la data alojada en la computadora a lo largo de este camino también puede ser mal utilizada en caso de una intrusión. Por ejemplo: un atacante puede editar y modificar los programas fuente del software y usar credenciales de correo electrónico para generar contenido malicioso.

VIU (2018) afirma que, también hay ciberdelincuentes que intentan acceder a las computadoras con fines maliciosos, como atacar otras computadoras o sitios de Internet a fin de causar estragos. Los piratas informáticos se especializan en el bloqueo de software empresarial para facilitar el hurto de la data, entre otras cosas.

En el plano internacional, Pereira (2016) afirma que, según los paradigmas más modernos de gestión empresarial, la data es el activo más crítico de cualquier compañía y, tiende a presentarse de diversas maneras: en físico o impresa, en formato electrónico, enviado por correo, exhibida en una película o dialogada en pláticas. En el entorno empresarial actual, la

información está constantemente en riesgo de diversos orígenes a nivel intrínseco o extrínseco, casuales o maliciosos para la compañía; Por ello, es crucial mantener la reserva, probidad y disposición de la data esencial para la empresa y sus consumidores.

Apaza (2021) sostiene que, ejemplo de táctica de administración de la data es prioritario para supervivir en el escenario vigente, por ejemplo, donde los activos de la data de una organización son objetos complejos y las amenazas que los rodean van desde simples virus informáticos hasta el robo de propiedad intelectual corporativa. La jerarquía de la seguridad informática en las compañías y entidades es cada vez más consciente y unánime, independientemente de la industria o el rol que desempeñen en la sociedad, especialmente las medianas y grandes empresas.

ISO Tools (2016) manifiesta que, se utilizan los estándares internacionales ISO/IEC 27001-27002 a fin de armonizar todo lo relacionado con la seguridad informática; Estos estándares están diseñados para exigir la planificación, desarrollo, soporte y optimización de un sistema de administración de seguridad de la data.

En el plano nacional, Tarrillo (2019) indica que, las organizaciones más grandes, como las enfocadas en finanzas, atención médica, operadores, administración, etc., deben abordar la seguridad de manera sistemática y sistemática con planes específicos enfocados en la persistencia del negocio y la optimización. A parte de las diversas medidas y espacios del vínculo coste-beneficio, aparecían razones jurídicas, regulatorias y contractuales que exigían cuidado de la data propia y delicada toda vez que resulta crítica como parte de la estrategia comercial.

PMG-SSI (2016) manifiesta que, según algunos estudios nacionales, la mayor amenaza a la seguridad informática es causada por el aspecto de la persona, especialmente faltas, comportamientos inadecuados y/o desidias internas. Además, se muestran informes que aseguran que la inversión en la administración de la seguridad de la data es más conveniente que la inversión en el campo TI destinada a incrementar el grado de seguridad de la data.

En el plano local, CGR (2020) comenta que, entonces el reto actual consiste es obtener la propuesta de un modelo de seguridad informática orientado a una solución técnica, económicamente adecuada y operativamente que asegure el nivel de cuidado necesario generando la confianza oportuna en el sector público, sus líderes y directivos, así como sus consumidores.

De esta manera, se tiene a la Unidad de Gestión Educativa Local Utcubamba, que es una unidad administrativa desconcentrada del Ministerio de Educación con autonomía en el territorio de la provincia de Utcubamba, atiende la educación básica normal, educación básica alternativa, educación básica especial, CETPROS, instituciones terciarias y pedagógicas de toda la región de Utcubamba (UGEL UTCUBAMBA, 2018).

Con el paso del tiempo, la institución ha progresado; sin embargo, se observa aún limitaciones o inconvenientes (**problemas específicos**) con respecto al manejo de su seguridad informática: Administración poco segura de sus activos informáticos; Ausencia de monitoreo de acceso a los recursos tecnológicos; Políticas de cifrado mínimas; Escasa seguridad a nivel físico y perimetral; Poca seguridad en las actividades administrativas; Escaza seguridad en las comunicaciones e interconexiones; Ausencia de un plan operativo para ejecución y sostenimiento de los sistemas informáticos.

Se expresa la **formulación del problema**: *General:* ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en la seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022?; *Específicos:* Inconveniente concreto 1 - ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022?; Inconveniente concreto 2 - ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en el grado de integridad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022?; Inconveniente concreto 3 - ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022?

Se expresa la **justificación de la investigación**: *Conveniencia*, contribuyó a perfeccionar la imagen de la entidad pública en base a la proyección de una entidad pública segura; *Relevancia social*, incluyó logros positivos para la comuna al disponer de empleados protegidos en el manejo de su información y activos informáticos; *Utilidad metodológica*, sirvió como sustento para las investigaciones similares que pudieran llevarse a cabo en un futuro respecto a seguridad informática; *Implicancias prácticas*, permitió perfeccionar el grado de calidad y seguridad de la data institucional; *Valor teórico*, permitió entender mejor las bases teóricas respecto al estándar internacional ISO/IEC 27002 y la seguridad informática.

Se expresa los **objetivos**: *General*: Acrecentar la seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022 mediante la aplicación de la norma internacional ISO/IEC 27002:2013; *Específicos*: Finalidad específica 1 - Acrecentar el grado de confidencialidad de la data institucional; Finalidad específica 2 - Acrecentar el grado de integridad de la data institucional; Finalidad específica 3 - Acrecentar el grado de disponibilidad de la data institucional.

Se expresa las **hipótesis**: *General:* "La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa la seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022"; *Específicas:* Supuesto específico 1 - "La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022"; Supuesto específico 2 - "La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de integridad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022"; Supuesto específico 3 - "La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

II. MARCO TEÓRICO

Se exhibe un conjunto de **antecedentes**, los mismos que estuvieron direccionados a conocer estudios previos realizados como:

Flores (2018), en su investigación tuvo como finalidad demostrar que, el estudio de las normas y estándares en la educación peruana, especialmente en el campo educativo superior, se difunde de manera destacada. Se registran las situaciones más importantes de cada regla y estándar, donde se inicia la propuesta de un modelo de administración de seguridad informática adecuado para su uso por parte de la institución educativa, que permita el desempeño del procedimiento actual relacionada con la seguridad de la data. En este contexto, este proyecto propone una opción basada en la propuesta de un sistema de seguridad de la data para una entidad de educación superior acorde a la situación de la entidad local. Esta tesis se orienta a la protección de datos de las principales operaciones de esta entidad educativa de acuerdo a los estándares mundiales actuales. Dentro de los motivos, uno en particular que se menciona este estudio es por el uso de estándares aplicables, que pueden ser muy útiles cuando se aplican a al problema descrito en esta investigación.

Basaldúa (2017), en su investigación tuvo como finalidad demostrar que, la auditoría crea una directiva de seguridad que garantiza que se conozca las responsabilidades de todos los involucrados para garantizar la seguridad; aun así, esto solo hace que sea difícil anticipar todas las amenazas potenciales, pero la política puede garantizar que cualquier problema tenga a alguien que pueda manejarlo responsablemente. Una política de seguridad puede incluir muchos niveles de seguridad. Una de los motivos por las que se menciona este estudio es la gestión de la data en las organizaciones.

Novoa (2016), en su investigación tuvo como finalidad analizar diferentes enfoques de estándares para proponer una metodología para implementar, gestionar y mejorar el SGSI en un patronato universitario, destacando también diversas opciones vitales y discutiendo su pertinencia o no. Se discuten varios procedimientos comunes de estudio y administración de riesgos. Se tiene el caso de algunos fomentados por los principales gobiernos y/o el sector industrial y se reconocen como una tendencia ampliamente aceptada en la

seguridad de la data. Esta investigación es recomendada para que la compañía utilice la metodología SGSI.

Corcho (2016), en su investigación tuvo como finalidad demostrar que, el origen de los sistemas de administración de seguridad de la data tiene cuatro componentes principales: la entidad, recursos humanos, tecnología y el lado jurídico, que explican el empleo del estándar ISO/IEC 27001:2013. En definitiva, el departamento de TI es el mecanismo responsable de los productos informáticos de una Universidad, que contribuye a la regular operatividad de las operaciones intrínsecas y se encarga de cuidar a los recursos TI y la seguridad de la data institucional. Por lo tanto, en la fase de planificación, el objetivo es crear los cimientos para la futura implantación del sistema de gestión de seguridad de la data de acuerdo con las recomendaciones de las normas mundiales de seguridad tal cual es la ISO/IEC 27001:2013 y, que con la ayuda de una metodología de análisis de riesgos determinan qué recursos TI son más delicados y tienen el más fuerte impacto, por lo cual se necesita de una protección más completa, creando así un plan de continuidad del servicio. Una de las razones por las que se menciona este estudio es el empleo de la metodología ISO/EIC 27001:2013 en el sector educativo.

Pallas (2019) en su investigación tuvo como finalidad demostrar que, propuesta de un método para implementar, administrar y mejorar el SGSI en un grupo empresarial jerárquico, así como presentar diversas opciones estratégicas y discutir su pertinencia o no. Se discuten varios procedimientos comunes de planificación y administración de riesgos. Dentro de éstos, existe la promoción del gobierno y/o sectores industriales de gobiernos líderes, quienes tienen una registrada tendencia de desarrollo de seguridad ampliamente aceptada. Con esta investigación surgió el empleo de la metodología SGSI en una compañía jerárquica.

Guerrero (2015), en su investigación tuvo como finalidad demostrar que, es frecuente tener un factor primordial de la competitividad de las compañías. La administración de riesgos y la garantía de datos están respaldadas por la presencia de estándares mundiales como la ISO/IEC 27002. Actualmente, la implantación y la gestión continua del estándar se facilitan principalmente

mediante software comercial. Las limitaciones de idioma, la falta de expedientes y la disposición de programas informáticos de corte abierto que se adapte a los requisitos específicos de las compañías en el plano latinoamericano limitan la efectividad de la implementación y uso del estándar. Se exhibe una plataforma de Internet abierta llamada SGSI que soporta la administración del control de seguridad de la información según la norma ISO 27002. Luego de un examen comparativo del empleo de la plataforma a cargo de profesionales especializados en seguridad, se consiguió demostrar su eficacia en una revisión del desempeño de los objetivos de monitoreo contenidos en el estándar. La razón por la que se menciona este estudio es por el uso de controles ISO 27002.

Adicionalmente, se cuenta con un conjunto de **bases teóricas** como soporte de entendimiento de lo investigado:

Norma internacional ISO/IEC 27002 versión 2013 (ISO/IEC 27002:2013): Se estructura en catorce (14) áreas de control, de las cuales sólo la mitad tratan aspectos de seguridad informática como: Administración de activos, se enfoca en la data como un activo y el procedimiento correcto para desplegar las medidas convenientes a fin de protegerla contra incidentes, brechas de seguridad y modificaciones no provocadas; Monitoreo de acceso, control que puede tener acceso a la data. Después de todo, en una compañía no todos requerirán manejar la data para llevar a cabo sus tareas cotidianas, aun así, existen roles que necesitan un acceso mayor y también aquellos que requieren un acceso más restringido. Todas las inspecciones como registro de usuarios, gestión de derechos de acceso, etc. Debieran estar disponibles a fin de conseguir lo anhelado; Cifrado, para información delicada, pudiera ser interesante emplear diversas estrategias de cifrado a fin de cuidar y asegurar su naturalidad, reserva y probidad; Protección real y ambiental, la seguridad va más allá de lo tecnológico, debiera ser real, esto significa la simple tarea de evitar dejar pantallas y dispositivos de impresión en lugares donde los trabajadores externos puedan acceder fácilmente a los documentos en los que están trabajando, además de una adecuada gestión segura, eventualmente se convierten en formas de garantizar que gestionemos de manera efectiva; Seguridad de uso, todas las disponibles tienen un importante

componente técnico, como protección contra malware, copias de seguridad, administración del software empleado, gestión de debilidades, etc.; Seguridad de la comunicación, se basa en que gran parte de la data y los intercambios de información a diferente escala se realizan a través de las redes sociales, las cuales garantizan la seguridad y protegen adecuadamente los medios de transmisión de esta clave de información; Adquisición, implementación y soporte de los sistemas informáticos, la seguridad no es parte de una área específica o correspondiente a un proceso determinado, no es tan general, pues comprende a toda la compañía y debiera estar vigente como un componente continuo en la clave de la administración del ciclo de vida del sistema (ISO Tools Excellence, 2016).

Seguridad informática, la seguridad informática garantiza el uso adecuado de todos los recursos del sistema informático de la compañía y el registro del acceso a los datos, así como verificar que los cambios solo sean posibles para las personas autorizadas, siempre dentro de la autoridad (ISO Tools, 2010). Dentro de los desafíos que enfrenta la seguridad de la data se incluyen: monitorear la exploración de los usuarios; determinar directivas que rijan el empleo e ingreso a las aplicaciones; redes de Internet como Facebook, Twitter, YouTube; escuchar música por Internet como Spotify, oír radio por internet; juegos en línea; mensajes instantáneos a través de Skype, Messenger; Descarga de archivos en línea como Emule, Torrent, Megaupload; buzones electrónicos privados como Gmail, Hotmail; gestión de conectores de almacén recargable como memorias USB; cifrado de data recargable de dispositivos; evitar agresiones de piratas informáticos, presencia de virus; notificar a los consumidores sobre problemas de seguridad informática. Se debe proteger elementos en sus objetivos. Así, los activos se componen de tres elementos: Data, es el componente más valioso para la compañía; Dispositivos, generalmente software, hardware y la misma compañía; Consumidores, aquellos que utilizan los recursos tecnológicos de la compañía. Cuando se trata de análisis de riesgos, el elemento más sensible que posee una compañía es la data en sí misma, de tal forma que para asegurarla debe estar disponible técnicas que sobrepasan la misma seguridad en físico derivado de los mismos dispositivos. Los mecanismos necesarios

para lograrlo son: limitar el uso de los consumidores dentro de la compañía al software y documentos relevantes; Se busca el aseguramiento de que los operadores puedan hacer su tarea, sin que incluya hacer cambios innecesarios a los programas o archivos; es necesario asegurar el uso de la data, documentos y software adecuado en los procesos seleccionados; se debe verificar los datos transmitidos, es decir, que los datos transmitidos sean los mismos que recibió el receptor; asegurarse de que varios sistemas estén operativos en una emergencia y distribuidos en toda la organización; todas las contraseñas de acceso a la computadora deben actualizarse continuamente. En términos de alcance, la seguridad de la data física es el más destacado de los conceptos de seguridad de la data, pues incluye todo lo relacionado con la tecnología informática, computadoras, servidores y dispositivos de redes. La protección lógica corresponde a los diversos programas utilizadas en los mismos dispositivos. Las intimidaciones a la seguridad física son: Catástrofes de la naturaleza: (igniciones, desbordamientos, sismos), se tornan importantes al momento de determinar la ubicación del punto principal de la data que contiene los servidores fundamentales de la compañía; no obstante, aun cuando se cuente con el mejor sistema de apaga incendios o que la oficina esté completamente cerrada, siempre será clave tener otro dentro de data a fin de que no se interrumpa el funcionamiento; Hurto: Los ordenadores y esencialmente la data contenida, son valiosas para todos los consumidores y compañías. Por ende, se debe cuidar el ingreso al espacio del centro de data con una serie de medidas seguras como: resguardos, credenciales físicas, credenciales lógicas (usuario y contraseña), entre otras.; Cortes de energía: las computadoras usan electricidad para operar y requieren de la extranet para interconectarse con otras compañías y consumidores. Se puede concordar con algunos proveedores de estos servicios, pero se debe estar listo para situaciones imprevistas como: baterías o de ser el caso un generador energético, otra interconexión a proveedores de Internet como respaldo adicional, incluso se puede elegir una solución inalámbrica para proteger antes de interrumpir la conexión física de cable. Las intimidaciones de seguridad lógica incluyen: programas de virus, programas troyanos y programas malware incluso. Al igual que los mensajes no deseados, el programa malware es una aplicación

no deseada del que se debe deshacer. El detrimento de la data, un error en el programa origen del software o incluso una mala distribución pueden provocar cambios inexplicables en los datos almacenados, incluida el extravío de la data. Es por ello, que contar con copias de seguridad como estrategia de respaldo resulta muy conveniente toda vez que se debe planificar su aplicación oportunamente (ISO Tools, 2010). De otra parte, se puede mencionar a la seguridad pasiva y activa. La primera es cualquier mecanismo que nos permite recuperarnos relativamente bien en caso de un ataque. Por ejemplo, baterías en caso de caída de voltaje o respaldo si los datos en el disco están dañados, mientras que la segunda trata de proteger las agresiones implementando mecanismos de protección de los activos de la compañía, como se apreció en el apartado pasado: dispositivos, programas, data e interconexiones (XULETAS, 2016).

También, se ha dispuesto de una colección de **enfoques conceptuales** que complementan la investigación como:

*Norma internacional de seguridad***,** los estándares ISO son reglas o normas de seguridad desarrolladas por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), las cuales se responsabilizar de crear normas y lineamientos vinculados con los métodos de control y pueden ser implementadas en todo tipo de organizaciones internacionales teniendo como objetivo promover la comercialización informática, flexibilizar el intercambio de data y promover la compartición de tecnología (ISO Tools, 2017)

Grupo de normas ISO/IEC 27000: Según la norma ISO 27001, la seguridad de la data se basa en mantener la confidencialidad, integridad y usabilidad de ésta y de los sistemas implementados en su aplicabilidad. Esta serie incluye: ISO/IEC 27000, ISMS Standard Vocabulary para todos los estándares del grupo. Se tiene entonces: ISO/IEC 27001, estándar para la certificación en seguridad de la data para las compañías; ISO/IEC 27002, guía de recomendaciones de gestión de la seguridad de la data; ISO/IEC 27003, Guía de cómo realizar la implementación de un SGSI.; ISO/IEC 27004, corresponde a medidas de gestión de la seguridad de la data (quién, cuándo y cómo realizar medidas de seguridad de la data); ISO/IEC 27005, reglas

diseñadas exclusivamente para gestionar los riesgos de seguridad de la data. Incorpora mejores prácticas y orientación sobre procedimientos y métodos de monitoreo de riesgos de seguridad de la data para respaldar las operaciones de administración de riesgos del estándar ISO/IEC 27001; ISO/IEC 27006, contempla requerimientos de consagración de las compañías que certifican los sistemas de gestión de la seguridad de la data. Este estándar establece los requerimientos para la certificación ISMS y se utiliza junto con el estándar de acreditación general 17021-1; ISO/IEC 27007, sirve como medio de elaboración de la guía de control del SGSI (Intedya, 2015).

Data, representa el recurso más relevante para la compañía y, por ende, le corresponde la mejor protección posible. La data segura implica tener protección frente a diversas intimidaciones minimizando el perjuicio causado por estas intimidaciones (IRAM, 2010).

Seguridad, representa el factor crítico para el mantenimiento informático en buenas condiciones. La seguridad garantiza que cada componente de un ordenador o dispositivo informático se utilicen como se espera y que los usuarios autorizados ingresen a la data que les corresponde únicamente (Pérez, 2018).

Seguridad de la data, la data involucrada es un componente comercial que posee valor para la compañía; en tal sentido, requiere un cuidado especial. La seguridad lo protege contra muchas intimidaciones para garantizar el funcionamiento de la compañía, reducir el daño a la misma, ampliar el regreso de la inversión y las proyecciones comerciales (SGSI, 2015)**.** El propósito de la seguridad de la data es proteger los datos y los programas gestionando adecuadamente su ingreso, empleo, propaganda, dificultad o pérdida no autorizada. Entre sus funciones se tiene: Reserva, esta función que evita la propaganda de data a usuarios o programas no admitidos; Probidad, es una característica diseñada para proteger la data libre de cambios no admitidos; Disposición, es la propiedad, calidad o estado de la data disponible para cualquier persona, ya sean usuarios, operaciones o programas (ISO Tools, 2010).

Respecto a **marcos de trabajo y estándares mundiales** candidatos para la propuesta de la solución tecnológica, se tuvo:

Estándar mundial ISO/IEC 27002:2013 es una norma mundial que se emplea como base de control en la implementación de un sistema de administración de seguridad de la data incluyendo control de ingreso a la data, monitoreo de cifrado de data confidencial y administración de anagramas. Las recomendaciones requeridas por ISO/IEC 27002 son: gestión de ingreso a la data; Cifrado de data confidencial; Administración y cuidado de anagramas de encriptación; Registrar y archivar "todas las transacciones importantes relacionadas con el uso y la gestión de las credenciales de usuario y la información de autenticación secreta" y proteger esos registros "contra la alteración y el acceso no autorizado" (THALES, 2020).

Estándar mundial ISO/IEC 17799, es una norma de seguridad de la data publicada por la Organización Internacional de Estándares y la Comisión Electrotécnica Mundial bajo el título Tecnología informática - Tecnologías de seguridad - Manual de prácticas de gestión de la seguridad de la data. La seguridad de la data se sostiene en el estándar ISO 17799, que puede definirla de tal manera que se conserven las siguientes características: Confidencialidad, se asegura que los datos solo están en manos de quienes tienen acceso a ellos; Se garantiza la integridad, precisión y probidad de la data y técnicas de operacionalización; Disposición, logrando que los consumidores acreditados tengan ingreso a la data y los activos relacionados siempre que los necesiten (ENIACAUDITORIAS, 2015).

Marco de trabajo COBIT 2019, representa un marco de dirección y administración de la data y know-how organizacional para la compañía entera. Identifica elementos y componentes de diseño para desarrollar y soportar el sistema de control más apropiado. Este marco permite garantizar una administración de la data y know-how organizacional eficaz facilitando un desarrollo más simple y tipificada reforzando el rol permanente de COBIT como motivador clave de la creatividad e innovación empresarial (Otake, 2019).

De los tres estándares / marcos de trabajo presentados, se recurrió al **método de juicio experto** para elegir la más conveniente, siendo ésta la Norma internacional ISO/IEC 27002:2013 - ver Anexo 3.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

- Tipo de investigación:

  Aplicada porque parte de experiencias y conocimientos generados ya aprobados y que busca la solución de problemas puntuales en las organizaciones.

- Diseño de investigación:

  Preexperimental porque no se presenta un control y monitoreo exhaustivo con la muestra poblacional.

3.2 Variables y operacionalización

- Variables:
  - Independiente:

    Norma internacional ISO/IEC 27002:2013.

    - Definición conceptual:

      "Norma mundial empleada como base de control en la implementación de un sistema de administración de seguridad de la data incluyendo control de ingreso a la data, monitoreo de cifrado de data confidencial y administración de claves" (THALES, 2020).

    - Definición operacional:

      Se puede medir a través de la aplicación de sus dominios, objetivos y controles de seguridad.

  - Dependiente:

    Seguridad informática.

- Definición Conceptual:

  "Garantiza el uso adecuado de todos los recursos del sistema informático de la compañía y el registro del acceso a los datos, así como verificar que los cambios solo sean posibles para las personas autorizadas, siempre dentro de la autoridad" (ISO Tools, 2010).

- Definición operacional:

  Se puede medir por el grado de confidencialidad, integridad y disponibilidad de la data.

- Operacionalización:

  Las variables operacionalizadas se exhiben en la matriz correspondiente indicada en el Anexo 2.

3.3 Población, muestra y muestreo

- Población (N):

  Constituida por el personal empleado que labora actualmente en la institución en la modalidad administrativa y directiva, pues son ellos quienes son los tomadores de decisiones.

Tabla 1. *Población*

Cargo / Puesto	Cantidad
Director	1
Jefe de oficina	5
Administrativo	10
Total	18

Fuente: (Elaboración propia, 2022)

$$N = 18\, personas$$

- Muestra (n):

  Puesto que la población en estudio no fue mayor que 30; en consecuencia, la muestra resulto siendo la misma que la población.

  Se tiene entonces:

$$n = N = 18\ personas$$

- Muestreo:

  El muestreo fue no probabilístico, lo cual mostró que existió una deliberada manipulación de los elementos muestrales.

3.4 Técnicas e instrumentos de recolección de datos

- Técnicas:
  - Entrevista.
  - Encuesta.

- Instrumentos:
  - Guía de entrevista.
  - Cuestionario.

- Validez y confiabilidad:

  Los cuestionarios de esta investigación se validaron a través de la colaboración de tres jueces expertos con reconocido prestigio profesional, tal y como se exhibe en el Anexo 5.

  Los cuestionarios de esta investigación determinaron su confiabilidad empleando el estadístico de *Alfa de Cronbach*, tal y como se exhibe en el Anexo 6.

3.5 Procedimientos

Todos los pasos que se siguieron para la consecución de los objetivos concretos se detallan a continuación:

- Oe_1: Acrecentar el grado de confidencialidad de la data institucional

  Para el desarrollo de este objetivo concreto, se recurrió a la técnica de la Encuesta empleando como herramienta el Cuestionario a fin de recolectar la data institucional y procesar su grado de confidencialidad como parte de la opinión de sus colaboradores según se exhibe en el Anexo 4.

- Oe_2: Acrecentar el grado de integridad de la data institucional

  Para el desarrollo de este objetivo concreto, se recurrió a la técnica de la Encuesta empleando como herramienta el Cuestionario a fin de recolectar la data institucional y procesar su grado de integridad como parte de la opinión de sus colaboradores según se exhibe en el Anexo 4.

- Oe_3: Acrecentar el grado de disponibilidad de la data institucional

  Para el desarrollo de este objetivo concreto, se recurrió a la técnica de la Encuesta empleando como herramienta el Cuestionario a fin de recolectar la data institucional y procesar su grado de disponibilidad como parte de la opinión de sus colaboradores según se exhibe en el Anexo 4.

3.6 Método de análisis de datos

Se empleó los métodos estadísticos en el procesamiento y análisis de la data institucional recopilada.

En el caso de la estadística descriptiva condescendió en la realización de una comparativa visual y tabular de los estados en preprueba y posprueba.

En el caso de la estadística inferencial condescendió en la realización de la prueba de normalidad para cada indicador vinculado a cada objetivo concreto.

3.7 Aspectos éticos

La actual investigación consideró la declaratoria de originalidad del informe por parte de los autores, la declaratoria de autenticidad del informe avalado por el asesor y la autorización de publicación en repositorio institucional.

Se consideró el empleo del manual de ética de la Universidad y, que tenía como objetivo establecer el marco de conducta en la que se desenvuelven los procesos de investigación científica de la Universidad, normando la investigación científica, tipificando la categorización de faltas y determinado los pasos que se siguen para sancionar las faltas en sus diferentes niveles, las cuales van en contra de los valores morales y principios éticos, así como las normas a cumplir en lo relacionado a investigación con seres humanos y otros.

De otra parte, se empleó el sistema anti plagio Turnitin para la generación del índice de similitud y ser coherente con la declaratoria de originalidad.

Por último, se empleó el sistema de norma bibliográfica ISO-690 para la generación de referencias bibliográficas estipuladas por la UCV.

IV. RESULTADOS

- **Análisis descriptivo**
  - Indicador “Grado de confidencialidad de la data”

Tabla 2. *Análisis descriptivo del indicador “Grado de confidencialidad de la data”*

	N	Mínimo	Máximo	Media	Desv. Desviación
GCD-Preprueba	9	1,58	2,00	1,8300	,18603
GCD-Posprueba	9	4,05	5,00	4,7829	,43767
N válido (por lista)	9				

Fuente: (Elaboración propia, 2022)

Tomando los valores tabulados de la tabla precedente, el grado de confidencialidad de la data antes de la aplicación de la solución ofrecida arrojaba un valor promedio de 1.83 puntos y posterior a la aplicación de la solución ofrecida arrojaba un valor promedio de 4.78 puntos, lo cual se deriva en un acrecentamiento de 2.95 puntos (Δ 59.00%), como se exhibe en la figura adjunta:

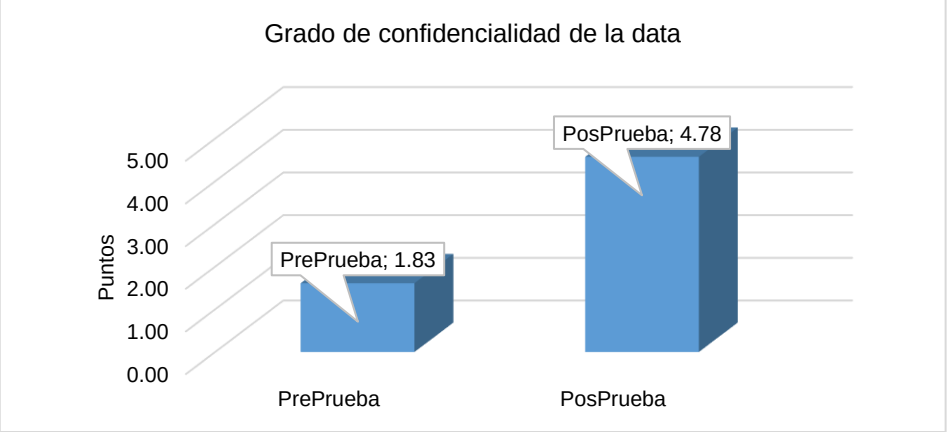

Figura 1. Promedios de preprueba y posprueba del indicador “Grado de confidencialidad de la data”.

- Indicador “Grado de integridad de la data”

Tabla 3. Análisis descriptivo del indicador “Grado de integridad de la data”

	N	Mínimo	Máximo	Media	Desv. Desviación
GID-Preprueba	9	1,58	1,85	1,7650	,16777
GID-Posprueba	9	4,48	5,00	4,8600	,25652
N válido (por lista)	9				

Fuente: (Elaboración propia, 2022)

Tomando los valores tabulados de la tabla precedente, el grado de integridad de la data antes de la aplicación de la solución ofrecida arrojaba un valor promedio de 1.77 puntos y posterior a la aplicación de la solución ofrecida arrojaba un valor promedio de 4.86 puntos, lo cual se deriva en un acrecentamiento de 3.09 puntos (Δ 61.80%), como se exhibe en la figura adjunta:

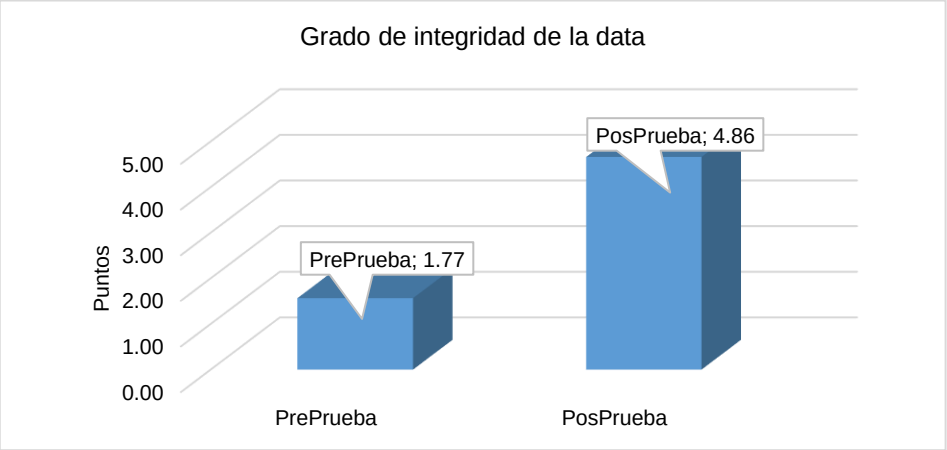

Figura 2. Promedios de preprueba y posprueba del indicador “Grado de integridad de la data”.

- Indicador “Grado de disponibilidad de la data”

Tabla 4. Análisis descriptivo del indicador “Grado de disponibilidad de la data”

	N	Mínimo	Máximo	Media	Desv. Desviación
GDD-PrePrueba	9	1,45	1,98	1,6030	,23520
GDD-PosPrueba	9	4,73	5,00	4,8520	,16069
N válido (por lista)	9				

Fuente: (Elaboración propia, 2022)

Tomando los valores tabulados de la tabla precedente, el grado de confidencialidad de la data antes de la aplicación de la solución ofrecida arrojaba un valor promedio de 1.60 puntos y posterior a la aplicación de la solución ofrecida arrojaba un valor promedio de 4.85 puntos, lo cual se deriva en un acrecentamiento de 3.25 puntos (Δ 65.00%), como se exhibe en la figura adjunta:

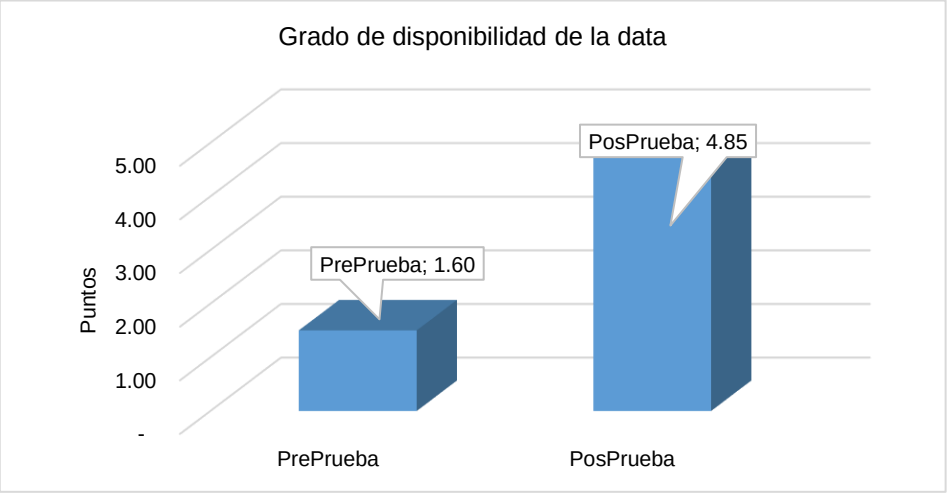

Figura 3. Promedios de preprueba y posprueba del indicador “Grado de disponibilidad de la data”.

- **Análisis inferencial**

  - Test de normalidad para el indicador “Grado de confidencialidad de la data”

    El test de normalidad del indicador examinó los efectos generados con el grado de significancia en la etapa de preprueba y en la etapa de posprueba.

    Se formularon las hipótesis de normalidad:

    H_0: “El grado de confidencialidad de la data” (sin la aplicación de la solución ofrecida) si tiene distribución normalizada”.

    H_1: “El grado de confidencialidad de la data” (sin la aplicación de la solución ofrecida) no tiene distribución normalizada”.

    H_0: “El grado de confidencialidad de la data” (con la aplicación de la solución ofrecida) no tiene distribución normalizada”.

    H_1: “El grado de confidencialidad de la data” (con la aplicación de la solución ofrecida) si tiene distribución normalizada”.

    Se expresa el grado de significancia: $\alpha = 0.05$

    Grado de significancia > 0.05, se consiente la hipótesis negativa (H_0).

    Grado de significancia <= 0.05, se consiente la hipótesis positiva (H_1).

Tabla 5. *Prueba de normalidad del indicador “Grado de confidencialidad de la data”*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
GCD-PrePrueba	,736	9	,024
GCD-PosPrueba	,831	9	,076

Fuente: (Elaboración Propia, 2022)

De lo exhibido en la tabla precedente**,** el grado de significancia en la etapa de preprueba fue de 0.027, siendo inferior a 0.05; en tal sentido, se consiente la primera hipótesis positiva que establece que el indicador tiene una distribución no normalizada. Por otra parte, el grado de significancia en la etapa de posprueba fue de 0.076, siendo superior a 0.05; en tal sentido, se consiente la segunda hipótesis negativa que establece que el indicador tiene una distribución no normalizada. La prueba que se aplicó en esta ocasión fue la prueba de Wilcoxon.

- Test de normalidad para el indicador “Grado de integridad de la data”

El test de normalidad del indicador examinó los efectos generados con el grado de significancia en la etapa de preprueba y en la etapa de posprueba.

Se formularon las hipótesis de normalidad:

H_0: “El grado de integridad de la data” (sin la aplicación de la solución ofrecida) si tiene distribución normalizada”.

H_1: “El grado de integridad de la data” (sin la aplicación de la solución ofrecida) no tiene distribución normalizada”.

H_0: “El grado de integridad de la data” (con la aplicación de la solución ofrecida) no tiene distribución normalizada”.

H_1: “El grado de integridad de la data” (con la aplicación de la solución ofrecida) si tiene distribución normalizada”.

Se expresa el grado de significancia: $\alpha = 0.05$

Grado de significancia > 0.05, se consiente la hipótesis negativa (H_0).

Valor de significancia <= 0.05, se consiente la hipótesis positiva (H_1).

Tabla 6. *Prueba de normalidad del indicador “Grado de integridad de la data”*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
GID-PrePrueba	,764	9	,021
GID-PosPrueba	,914	9	,067

Fuente: (Elaboración Propia, 2022)

De lo exhibido en la tabla precedente**,** el grado de significancia en la etapa de preprueba fue de 0.021, siendo inferior a 0.05; en tal sentido, se consiente la primera hipótesis positiva que establece que el indicador tiene una distribución no normalizada. Por otra parte, el grado de significancia en la etapa de posprueba fue de 0.067, siendo superior a 0.05; en tal sentido, se consiente la segunda hipótesis negativa que establece que el indicador tiene una distribución no normalizada. La prueba que se aplicó en esta ocasión fue la prueba de Wilcoxon.

- Test de normalidad para el indicador “Grado de disponibilidad de la data”

El test de normalidad del indicador examinó los efectos generados con el grado de significancia en la etapa de preprueba y en la etapa de posprueba.

Se formularon las hipótesis de normalidad:

H_0: “El grado de disponibilidad de la data” (sin la aplicación de la solución ofrecida) si tiene distribución normalizada”.

H_1: “El grado de disponibilidad de la data” (sin la aplicación de la solución ofrecida) no tiene distribución normalizada”.

H_0: “El grado de disponibilidad de la data” (con la aplicación de la solución ofrecida) no tiene distribución normalizada”.

H_1: “El grado de disponibilidad de la data” (con la aplicación de la solución ofrecida) si tiene distribución normalizada”.

Se expresa el grado de significancia: $\alpha = 0.05$

Grado de significancia > 0.05, se consiente la hipótesis negativa (H_0).

Grado de significancia <= 0.05, se consiente la hipótesis positiva (H_1).

Tabla 7. *Prueba de normalidad del indicador “Grado de disponibilidad de la data”*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
GDD-PrePrueba	,856	9	,032
GDD-PosPrueba	,832	9	,071

Fuente: (Elaboración Propia, 2022)

De lo exhibido en la tabla precedente**,** el grado de significancia en la etapa de preprueba fue de 0.032, siendo inferior a 0.05; en tal sentido, se consiente la primera hipótesis positiva que establece que el indicador tiene una distribución no normalizada. Por otra parte, el grado de significancia en la etapa de posprueba fue de 0.071, siendo superior a 0.05; en tal sentido, se consiente la segunda hipótesis negativa que establece que el indicador tiene una distribución no normalizada. La prueba que se aplicó en esta ocasión fue la prueba de Wilcoxon.

- **Contrastación de hipótesis**

Los test de normalidad aplicados a todos los indicadores anteriores, mantienen una distribución no normalizada; en consecuencia, se aplicó la prueba no paramétrica de Wilcoxon. Se tuvo:

- Hipótesis específica 1:

"La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

Supuestos estadísticos:

H_0: "La aplicación de la norma internacional ISO/IEC 27002:2013 no acrecienta de manera significativa el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

$$H_0: GCDa >= GCDp$$

Se establece que no existe acrecentamiento del indicador.

H_1: "La aplicación de la norma internacional ISO/IEC 27002:2013 si acrecienta de manera significativa el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

$$H_1: GCDa < GCDp$$

Se establece que si existe acrecentamiento del indicador.

Grado de significancia: $\alpha = 0.05$.

Grado de significancia > 0.05, se consiente la hipótesis negativa (H_0).

Grado de significancia <= 0.05, se consiente la hipótesis positiva (H_1).

Tabla 8. *Prueba Wilcoxon para el indicador "Grado de confidencialidad de la data"*

Estadísticos de prueba[a]

	GCD-Posprueba - GCD-Preprueba
Z	-2,359[b]
Sig. asintótica(bilateral)	,015

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El grado de significancia obtenido fue 0.015 (< 0.05); en consecuencia, se desestima la hipótesis negativa admitiéndose la hipótesis positiva.

Se pudo concluir: "Existe amplia evidencia estadística del 95% de valor de significación para afirmar que la aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

- Hipótesis específica 2:

“La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de integridad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.

Supuestos estadísticos:

H_0: “La aplicación de la norma internacional ISO/IEC 27002:2013 no acrecienta de manera significativa el grado de integridad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.

$$H_0: GIDa >= GIDp$$

Se establece que no existe acrecentamiento del indicador.

H_1: “La aplicación de la norma internacional ISO/IEC 27002:2013 si acrecienta de manera significativa el grado de integridad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.

$$H_1: GIDa < GIDp$$

Se establece que si existe acrecentamiento del indicador.

Grado de significancia: $\alpha = 0.05$.

Grado de significancia > 0.05, se consiente la hipótesis negativa (H_0).

Grado de significancia <= 0.05, se consiente la hipótesis positiva (H_1).

Tabla 9. *Prueba de Wilcoxon para el indicador "Grado de integridad de la data"*

Estadísticos de prueba[a]

	GID-PosPrueba - GID-PrePrueba
Z	-2,134[b]
Sig. asintótica(bilateral)	,025

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El grado de significancia obtenido fue 0.025 (< 0.05); en consecuencia, se desestimó la hipótesis negativa admitiéndose la hipótesis positiva.

Se pudo concluir: "Existe amplia evidencia estadística del 95% de valor de significación para afirmar que la aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de integridad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

- Hipótesis específica 3:

  “La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.

  Supuestos estadísticos:

  H_0: “La aplicación de la norma internacional ISO/IEC 27002:2013 no acrecienta de manera significativa el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.

  $$H_0: GDDa >= GDDp$$

  Se establece que no existe acrecentamiento del indicador.

  H_1: “La aplicación de la norma internacional ISO/IEC 27002:2013 si acrecienta de manera significativa el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.

  $$H_1: GDDa < GDDp$$

  Se establece que si existe acrecentamiento del indicador.

  Grado de significancia: $\alpha = 0.05$.

  Grado de significancia > 0.05, se consiente la hipótesis negativa (H_0).

  Grado de significancia <= 0.05, se consiente la hipótesis positiva (H_1).

Tabla 10. *Prueba de Wilcoxon para el indicador "Grado de disponibilidad de la data"*

Estadísticos de prueba[a]

	GDD-PosPrueba - GDD-PrePrueba
Z	-2,165[b]
Sig. asintótica(bilateral)	,035

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: (Elaboración propia, 2022)

El grado de significancia obtenido fue 0.035 (< 0.05); en consecuencia, se desestimó la hipótesis negativa admitiéndose la hipótesis positiva.

Se pudo concluir: "Existe amplia evidencia estadística del 95% de valor de significación para afirmar que la aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".

V. DISCUSIÓN

En referencia al primer indicador “Grado de confidencialidad de la data”, antes de la aplicación de la solución ofrecida arrojaba un valor promedio de 1.83 puntos y posterior a la aplicación de la solución ofrecida arrojaba un valor promedio de 4.78 puntos, lo cual se deriva en un acrecentamiento de 2.95 puntos (Δ 59.00%). Estos resultados son comparables a los obtenidos por (Flores, 2018), quien en su investigación tuvo como finalidad demostrar que, el estudio de las normas y estándares en la educación peruana, especialmente en el campo educativo superior, se difunde de manera destacada. Del mismo modo, son comparables por (Basaldúa, 2017), quien en su investigación tuvo como finalidad demostrar que, la auditoría crea una directiva de seguridad que garantiza que se conozca las responsabilidades de todos los involucrados para garantizar la seguridad. La base teórica que sustenta estos resultados corresponde a la norma internacional ISO/IEC 27002:2013, específicamente referido al monitoreo de acceso, control que puede tener acceso a la data. Después de todo, en una compañía no todos requerirán manejar la data para llevar a cabo sus tareas cotidianas, aun así, existen roles que necesitan un acceso mayor y también aquellos que requieren un acceso más restringido (ISO Tools Excellence, 2016).

En referencia al segundo indicador “Grado de integridad de la data”, antes de la aplicación de la solución ofrecida arrojaba un valor promedio de 1.77 puntos y posterior a la aplicación de la solución ofrecida arrojaba un valor promedio de 4.86 puntos, lo cual se deriva en un acrecentamiento de 3.09 puntos (Δ 61.80%). Estos resultados son comparables a los obtenidos por (Novoa, 2016), quien en su investigación tuvo como finalidad analizar diferentes enfoques de estándares para proponer una metodología para implementar, gestionar y mejorar el SGSI en un patronato universitario, destacando también diversas opciones vitales y discutiendo su pertinencia o no. Del mismo modo, son comparables por (Corcho, 2016), quien en su investigación tuvo como finalidad demostrar que, el origen de los sistemas de administración de seguridad de la data tiene cuatro componentes principales: la entidad, recursos humanos, tecnología y el lado jurídico, que explican el empleo del estándar ISO/IEC 27001:2013. La base teórica que sustenta estos

resultados corresponde a la norma internacional ISO/IEC 27002:2013, específicamente referido al Cifrado, para información delicada, pudiera ser interesante emplear diversas estrategias de cifrado a fin de cuidar y asegurar su naturalidad, reserva y probidad (ISO Tools Excellence, 2016).

En referencia al tercer indicador “Grado de disponibilidad de la data”, antes de la aplicación de la solución ofrecida arrojaba un valor promedio de 1.60 puntos y posterior a la aplicación de la solución ofrecida arrojaba un valor promedio de 4.85 puntos, lo cual se deriva en un acrecentamiento de 3.25 puntos (Δ 65.00%). Estos resultados son comparables a los obtenidos por (Guerrero, 2015), quien en su investigación tuvo como finalidad demostrar que, es frecuente tener un factor primordial de la competitividad de las compañías. La administración de riesgos y la garantía de datos están respaldadas por la presencia de estándares mundiales como la ISO/IEC 27002. Del mismo modo, son comparables por (Pallas, 2019), quien en su investigación tuvo como finalidad demostrar que, propuesta de un método para implementar, administrar y mejorar el SGSI en un grupo empresarial jerárquico, así como presentar diversas opciones estratégicas y discutir su pertinencia o no. La base teórica que sustenta estos resultados corresponde a la norma internacional ISO/IEC 27002:2013, específicamente referido a la protección real y ambiental, la seguridad va más allá de lo tecnológico, debiera ser real, esto significa la simple tarea de evitar dejar pantallas y dispositivos de impresión en lugares donde los trabajadores externos puedan acceder fácilmente a los documentos en los que están trabajando, además de una adecuada gestión segura (ISO Tools Excellence, 2016).

VI. CONCLUSIONES

1. Se consiguió acrecentar la seguridad informática de la entidad pública en estudio con respecto al grado de confidencialidad de la data, obteniéndose específicamente puntuaciones de 1.83 a 4.78 puntos, representando un acrecentamiento de 2.95 puntos (Δ 59.00%).
2. Se consiguió acrecentar la seguridad informática de la entidad pública en estudio con respecto al grado de integridad de la data, obteniéndose específicamente puntuaciones de 1.77 a 4.86 puntos, representando un acrecentamiento de 3.09 puntos (Δ 61.80%).
3. Se consiguió acrecentar la seguridad informática de la entidad pública en estudio con respecto al grado de disponibilidad de la data, obteniéndose específicamente puntuaciones de 1.60 a 4.85 puntos, representando un acrecentamiento de 3.25 puntos (Δ 65.00%).
4. En conclusión, se logró acrecentar la seguridad informática de la entidad pública en estudio a través del acrecentamiento del valor obtenido en cada uno de sus indicadores estadísticos procesados.

VII. RECOMENDACIONES

Al Director general:

Se sugiere realizar la implementación de la solución ofrecida en este estudio sobre la base de un adecuado empleo de soporte tecnológico conveniente para el sostenimiento de la misma en la UGEL.

Al Jefe de Informática:

Se sugiere optimizar la seguridad informática de la UGEL tomando como punto de partida el ciclo de mejora continua, toda vez que también debe contemplarse el campo de la ciberseguridad.

Al Jefe de Recursos humanos:

Se sugiere organizar eventos de capacitación tecnológica sobre seguridad informática invitando a la participación de los colaboradores de la UGEL, toda vez que se requiere su compromiso laboral en el buen empleo de la data.

A los Usuarios:

Se sugiere sensibilizar la importancia de la seguridad informáticas a través de un proceso de sensibilización en buenas prácticas de seguridad de los activos informáticos como resultado de la aplicación del estándar mundial ISO/IEC 27002.

REFERENCIAS

Alemán, Isabel. 2016. *“Metodología de Implementación de un SGSI en un grupo empresarial educativo”.* Tunja : UILR, 2016.

Aliaga, Luis. 2018. *"Diseño de un sistema de gestión de seguridad de información para un instituto educativo".* Lima : PUCP, 2018.

Álvarez, Luis. 2017. *"Seguridad en informática (auditoria de sistemas)".* México DF : UI, 2017.

Basaldúa, Daniel. 2017. *"Seguridad en informática (auditoria de sistemas)".* México DF : UI, 2017.

CGR. 2020. *Manual de Auditoría Informática.* Lima : CGR, 2020.

Corcho, Felipe. 2016. *"Diseño de un Sistema de Gestión de Seguridad de la Información mediante la Aplicación de la Norma Internacional ISO/IEC 27001:2013 en la Oficina de Sistemas de Información y Telecomunicaciones de la Universidad de Córdoba".* Córdoba : UC, 2016.

CSS. 2017. Seguridad Informática. [En línea] 29 de Marzo de 2017. https://www.css.pe/que-es-la-seguridad-informatica/.

Doria, Andrés. 2016. *"Diseño de un Sistema de Gestión de Seguridad de la Información mediante la Aplicación de la Norma Internacional ISO/IEC 27001:2013 en la Oficina de Sistemas de Información y Telecomunicaciones de la Universidad de Córdoba".* Córdoba : UC, 2016.

ENIACAUDITORIAS. 2015. Norma ISO/IEC 17799. [En línea] 1 de Enero de 2015. https://eniacauditorias.wordpress.com/norma-isoiec-17799/.

Flores, Carlos. 2018. *"Diseño de un sistema de gestión de seguridad de información para un instituto educativo".* Lima : PUCP, 2018.

Guerrero, César. 2015. *"Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002".* Cancun : LACCEI, 2015.

Hefner, Kim, Peterson, Stacey y Crocetti, Paul. 2020. Protección de datos. [En línea] 1 de Enero de 2020. https://www.computerweekly.com/es/definicion/Proteccion-de-datos#:~:text=La%20protecci%C3%B3n%20de%20datos%20es,a%20un%20ritmo%20sin%20precedentes..

Intedya. 2015. ISO 27000 y el conjunto de estándares de Seguridad de la Información. [En línea] 1 de Septiembre de 2015. https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html#:~:text=La%20familia%20ISO%2027000%20contiene,las%20normas%2027001%20y%2027002..

IRAM. 2010. Instituto Argentino de Normalización y Certificación. [En línea] 01 de 01 de 2010. [Citado el: 15 de 04 de 2018.] http://www.iram.org.ar/index.php?IDM=28.

ISO Tools Excellence. 2016. Norma ISO 27002. [En línea] 01 de 01 de 2016. [Citado el: 15 de 03 de 2018.] https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/.

—. 2016. Norma ISO 27002. [En línea] 1 de Enero de 2016. [Citado el: 15 de 03 de 2018.] https://www.isotools.cl/normas/nch-iso-27001/.

ISO Tools. 2017. Plataforma Tecnológica para la Gestión de la Excelencia. [En línea] 01 de 12 de 2017. [Citado el: 15 de 03 de 2018.] https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/.

—. 2010. Seguridad de la Información. [En línea] 01 de 01 de 2010. [Citado el: 18 de 03 de 2018.] http://www.iram.org.ar/index.php?IDM=28.

Novoa, Helena. 2016. *“Metodología de Implementación de un SGSI en un grupo empresarial educativo”.* Tunja : UILR, 2016.

OSTEC. 2016. ISO 27002: Buenas prácticas para gestión de la seguridad de la información. [En línea] 30 de Diciembre de 2016. [Citado el: 22 de Junio de 2022.] https://ostec.blog/es/aprendizaje-descubrimiento/iso-27002-buenas-practicas-gsi/.

Otake, Luis. 2019. COBIT 2019. [En línea] 21 de Octubre de 2019. https://www.audiconsulti.com/glosario/que-es-cobit-2019/#:~:text=El%20marco%20de%20COBIT%202019,%2C%20DSS%2C%20y%20MEA)..

Pallas, Gustavo. 2019. *"Metodología de implantación de un SGSI en un grupo empresarial jerárquico".* Montevideo : UDELAR, 2019.

Pereira, José. 2016. *Análisis de riesgos para el proceso administrativo: Departamento de informática en la empresa de Acueducto y Alcantarillado de Pereira S.A E.S.P., basados en la Norma ISO 27005.* Lima : UTP, 2016.

Pérez, Carlos. 2018. Definiciones de Seguridad. [En línea] 20 de 01 de 2018. [Citado el: 12 de 04 de 2018.] https://definicion.de/seguridad/.

PMG-SSI. 2016. Seguridad de la Información. [En línea] 14 de Junio de 2016. https://www.pmg-ssi.com/2016/06/la-norma-iso-27002-complemento-para-la-iso-27001/.

Porto, Carlos Pérez. 2018. Definiciones de Seguridad. [En línea] 20 de 01 de 2018. [Citado el: 12 de 04 de 2018.] https://definicion.de/seguridad/.

Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera. **Apaza, Wilmer. 2021.** 2021, Innovación y Software, págs. 27-43.

SGSI. 2015. Sistemas de Gestión de Seguridad de la Información. [En línea] 01 de 01 de 2015. [Citado el: 15 de 02 de 2018.] https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/.

THALES. 2020. ISO/IEC 27002:2013. [En línea] 1 de Enero1 de 2020. https://cpl.thalesgroup.com/es/compliance/isoiec-270022013-compliance#:~:text=ISO%2FIEC%2027002%20es%20un,confidenciales%20y%20administraci%C3%B3n%20de%20claves..

UGEL UTCUBAMBA. 2018. Sitio web oficial. [En línea] 1 de Enero de 2018. https://ugelutcubamba.gob.pe/.

VIU. 2018. Importancia de la Seguridad Informática. [En línea] 21 de Marzo de 2018. https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme#:~:text=Hay%20tambi%C3%A9n%20ciberdelincuentes%20que%20intentar%C3%A1n,propiciar%20la%20p%C3%A9rdida%20de%20datos..

XULETAS. 2016. Seguridad activa y pasiva informática. [En línea] 23 de Junio de 2016. https://www.xuletas.es/ficha/seguridad-activa-pasiva-informatica-3/.

ANEXOS

Anexo 1 - Matriz de consistencia de la investigación

Título: Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’, 2022

Autora: Abad Chávez, Manuel / Cruz Calderón, Franklyn

Problema	Objetivo	Hipótesis	Variable	Dimensión	Indicador	Instrumento
General: ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en la seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022?	General: Acrecentar la seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022 mediante la aplicación de la norma internacional ISO/IEC 27002:2013.	General: “La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa la seguridad informática de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”.	Independiente: Norma internacional ISO/IEC 27002:2013			
Específicos: 1. ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022? 2. ¿En qué medida la norma internacional ISO/IEC	Específicos: 1. Acrecentar el grado de confidencialidad de la data institucional. 2. Acrecentar el grado de integridad de la data institucional. 3. Acrecentar el grado de disponibilidad de la data institucional.	Específicas: 1. “La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de confidencialidad de la data de la Unidad de Gestión Educativa Local ‘Utcubamba’ en el año 2022”. 2. “La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de integridad de la data de la Unidad de	Dependiente: Seguridad informática	Confidencialidad	Grado de confidencialidad de la data	Cuestionario
				Integridad	Grado de integridad de la data	Cuestionario

27002:2013 influye en el grado de integridad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022? 3. ¿En qué medida la norma internacional ISO/IEC 27002:2013 influye en el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022?		Gestión Educativa Local 'Utcubamba' en el año 2022". 3. "La aplicación de la norma internacional ISO/IEC 27002:2013 acrecienta de manera significativa el grado de disponibilidad de la data de la Unidad de Gestión Educativa Local 'Utcubamba' en el año 2022".		Disponibilidad	Grado de disponibilidad de la data	Cuestionario

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Norma internacional ISO/IEC 27002:2013	“Conjunto de métricas adecuadas respecto a protección de activos informáticos a fin de evaluar la confidencialidad, integridad y usabilidad de la información” (Cano, 2018).	Se puede medir a través de aspectos de directivas y actividades de seguridad informática en las organizaciones.			
Dependiente: Seguridad informática	“Proceso por el cual se generan mecanismos para el cuidado y atención de la data importante a fin de evitar la corrupción, fuga, pérdida o compromiso del mismo” (Hefner, y otros, 2020)	Se puede medir por el grado de prevención de la divulgación no autorizada, grado de prevención de la modificación no autorizada y grado de prevención de la interrupción no autorizada.	Confidencialidad	Prevención de la divulgación no autorizada	Ordinal
			Integridad	Prevención de la modificación no autorizada	Ordinal
			Disponibilidad	Prevención de la interrupción no autorizada	Ordinal

Anexo 3 - Método de juicio experto

Apellidos y nombres del experto: Agreda Gamboa, Everson David

Título profesional y/o Grado académico: Ingeniero de Sistemas / Doctor

Fecha: 04/05/2022

Título del proyecto de investigación: "Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba', 2022".

Autores: Abad Chávez, Manuel / Cruz Calderón, Franklyn

Evaluación de la norma / marco de trabajo para la seguridad informática

Mediante el método de juicio experto, Usted tiene la facultad de calificar las normas / marcos de trabajo involucrados, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la norma / marco de trabajo para la seguridad informática en la presente investigación y, también si hubiese algunas sugerencias:

Ítem	Criterios	Norma / Marco de trabajo		
		ISO 27002:2013	NTP-ISO 17799	COBIT 2019
1	Tiempo de implementación	2	2	2
2	Información	3	2	2
3	Requerimientos	3	3	2
4	Complejidad	3	3	2
5	Conocimiento	3	2	2
Total		14	12	10

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

Ítem	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Apellidos y nombres del experto: Mendoza Rivera, Ricardo Darío

Título profesional y/o Grado académico: Ingeniero Industrial / Doctor

Fecha: 04/05/2022

Título del proyecto de investigación: "Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba', 2022".

Autores: Abad Chávez, Manuel / Cruz Calderón, Franklyn

Evaluación de la norma / marco de trabajo para la seguridad informática

Mediante el método de juicio experto, Usted tiene la facultad de calificar las normas / marcos de trabajo involucrados, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la norma / marco de trabajo para la seguridad informática en la presente investigación y, también si hubiese algunas sugerencias:

Ítem	Criterios	Norma / Marco de trabajo		
		ISO 27002:2013	NTP-ISO 17799	COBIT 2019
1	Tiempo de implementación	2	2	1
2	Información	3	2	2
3	Requerimientos	3	2	2
4	Complejidad	2	2	1
5	Conocimiento	2	2	2
Total		12	10	8

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

Ítem	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Apellidos y nombres del experto: Córdova Otero, Juan Luis

Título profesional y/o Grado académico: Ingeniero de Computación y Sistemas / Maestro

Fecha: 04/05/2022

Título del proyecto de investigación: "Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba', 2022".

Autores: Abad Chávez, Manuel / Cruz Calderón, Franklyn

Evaluación de la norma / marco de trabajo para la seguridad informática

Mediante el método de juicio experto, Usted tiene la facultad de calificar las normas / marcos de trabajo involucrados, mediante unas series de criterios con puntuaciones especificadas al final de la tabla. Así mismo le exhortamos en la correcta determinación de la norma / marco de trabajo para la seguridad informática en la presente investigación y, también si hubiese algunas sugerencias:

Ítem	Criterios	Norma / Marco de trabajo		
		ISO 27002:2013	NTP-ISO 17799	COBIT 2019
1	Tiempo de implementación	3	3	2
2	Información	3	2	2
3	Requerimientos	3	3	3
4	Complejidad	3	2	2
5	Conocimiento	3	3	2
Total		15	13	11

La escala a evaluar es de: **1** - Malo, **2** - Regular, **3** - Bueno

Sugerencias: Ninguna.

Firma del experto

Criterios de evaluación de las metodologías/marcos de trabajo propuestas

Ítem	Criterio	Descripción
1	Tiempo de implementación	Es el tiempo que toma la implementación de la solución.
2	Información	Es la cantidad de información disponible sobre la metodología/marco de trabajo.
3	Requerimientos	Es la cantidad de requerimientos que exige la metodología/marco de trabajo.
4	Complejidad	Es el nivel de abstracción del estudio de la metodología/marco de trabajo.
5	Conocimiento	Es la cantidad de conocimiento que el investigador debe tener sobre la metodología/marco de trabajo.

Anexo 4 - Instrumentos de recolección de datos

Cuestionario aplicado al Personal administrativo de la UGEL ‘Utcubamba’

A continuación, se presenta una lista de preguntas contenidas en nueve (9) ítems que corresponden a su percepción sobre la seguridad informática en la UGEL. Por favor, indique su apreciación objetiva marcando con una “X” sobre cualquier de los números 1, 2, 3, 4 o 5, dónde:

1	2	3	4	5
Deficiente	Malo	Regular	Bueno	Excelente

Variable	Dimensión	Ítems	Opción de respuesta				
			1	2	3	4	5
Seguridad informática	Confidencialidad	1. ¿Cómo considera Usted los requerimientos establecidos para el monitoreo de acceso de usuarios a los activos informáticos?					
		2. ¿Cómo considera Usted el procedimiento establecido para el monitoreo del acceso de usuarios a los activos informáticos?					
		3. ¿Cómo considera Usted el uso de indicadores para el monitoreo del acceso de los usuarios a los activos informáticos?					
	Integridad	4. ¿Cómo considera Usted los requerimientos establecidos para la protección del contenido de la data institucional?					
		5. ¿Cómo considera Usted el procedimiento establecido para la protección del contenido de la data institucional?					
		6. ¿Cómo considera Usted el uso de indicadores para la protección del contenido de la data institucional?					
	Disponibilidad	7. ¿Cómo considera Usted los requerimientos establecidos para la disposición del contenido de la data institucional?					
		8. ¿Cómo considera Usted el procedimiento establecido para la disposición del contenido de la data institucional?					
		9. ¿Cómo considera Usted el uso de indicadores para la disposición del contenido de la data institucional?					

Anexo 5 - Validación de los instrumentos de recolección de datos

I. Datos generales:

Cuestionario

II. II. Instrucciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Cómo considera Usted los requerimientos establecidos para el monitoreo de acceso de usuarios a los activos informáticos?	x		x		x		
2. ¿Cómo considera Usted el procedimiento establecido para el monitoreo del acceso de usuarios a los activos informáticos?	x		x		x		
3. ¿Cómo considera Usted el uso de indicadores para el monitoreo del acceso de los usuarios a los activos informáticos?	x		x		x		
Dimensión 2: Integridad							
4. ¿Cómo considera Usted los requerimientos establecidos para la protección del contenido de la data institucional?	x		x		x		
5. ¿Cómo considera Usted el procedimiento establecido para la protección del contenido de la data institucional?	x		x		x		
6. ¿Cómo considera Usted el uso de indicadores para la protección del contenido de la data institucional?							
Dimensión 3: Disponibilidad							
7. ¿Cómo considera Usted los requerimientos establecidos para la disposición del contenido de la data institucional?	x		x		x		
8. ¿Cómo considera Usted el procedimiento establecido para la disposición del contenido de la data institucional?	x		x		x		
9. ¿Cómo considera Usted el uso de indicadores para la disposición del contenido de la data institucional?	x		x		x		

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

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

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

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

Observaciones: Es suficiente	
Opinión de aplicabilidad Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]	
Apellidos y nombres del juez evaluador	Dr. Agreda Gamboa, Everson David
Especialidad del evaluador	Redes y Comunicaciones
 **DNI:** 18161457	Trujillo, 18 de mayo del 2022

I. Datos generales:

Cuestionario

II. II. Instrucciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Cómo considera Usted los requerimientos establecidos para el monitoreo de acceso de usuarios a los activos informáticos?	x		x		x		
2. ¿Cómo considera Usted el procedimiento establecido para el monitoreo del acceso de usuarios a los activos informáticos?	x		x		x		
3. ¿Cómo considera Usted el uso de indicadores para el monitoreo del acceso de los usuarios a los activos informáticos?	x		x		x		
Dimensión 2: Integridad							
4. ¿Cómo considera Usted los requerimientos establecidos para la protección del contenido de la data institucional?	x		x		x		
5. ¿Cómo considera Usted el procedimiento establecido para la protección del contenido de la data institucional?	x		x		x		
6. ¿Cómo considera Usted el uso de indicadores para la protección del contenido de la data institucional?							
Dimensión 3: Disponibilidad							
7. ¿Cómo considera Usted los requerimientos establecidos para la disposición del contenido de la data institucional?	x		x		x		
8. ¿Cómo considera Usted el procedimiento establecido para la disposición del contenido de la data institucional?	x		x		x		
9. ¿Cómo considera Usted el uso de indicadores para la disposición del contenido de la data institucional?	x		x		x		

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

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

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

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

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

I. Datos generales:

Cuestionario

II. II. Instrucciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Cómo considera Usted los requerimientos establecidos para el monitoreo de acceso de usuarios a los activos informáticos?	x		x		x		
2. ¿Cómo considera Usted el procedimiento establecido para el monitoreo del acceso de usuarios a los activos informáticos?	x		x		x		
3. ¿Cómo considera Usted el uso de indicadores para el monitoreo del acceso de los usuarios a los activos informáticos?	x		x		x		
Dimensión 2: Integridad							
4. ¿Cómo considera Usted los requerimientos establecidos para la protección del contenido de la data institucional?	x		x		x		
5. ¿Cómo considera Usted el procedimiento establecido para la protección del contenido de la data institucional?	x		x		x		
6. ¿Cómo considera Usted el uso de indicadores para la protección del contenido de la data institucional?							
Dimensión 3: Disponibilidad							
7. ¿Cómo considera Usted los requerimientos establecidos para la disposición del contenido de la data institucional?	x		x		x		
8. ¿Cómo considera Usted el procedimiento establecido para la disposición del contenido de la data institucional?	x		x		x		
9. ¿Cómo considera Usted el uso de indicadores para la disposición del contenido de la data institucional?	x		x		x		

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

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

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

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

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

Anexo 6 - Tabla de datos

Data recolectada (Preprueba)

	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9
Persona 1	1	2	1	2	2	1	2	1	1
Persona 2	2	2	1	2	2	1	1	2	2
Persona 3	2	1	2	1	1	2	1	2	1
Persona 4	1	2	2	2	2	1	2	2	2
Persona 5	1	2	1	2	2	1	1	2	1
Persona 6	2	2	1	2	2	1	2	2	2
Persona 7	2	2	1	2	2	2	1	1	2
Persona 8	2	1	2	1	1	2	1	2	1
Persona 9	2	2	1	2	2	1	1	2	2
Persona 10	2	1	2	1	1	2	1	2	1
Persona 11	1	2	2	2	2	1	2	2	2
Persona 12	1	2	1	2	2	1	1	2	1
Persona 13	2	2	1	2	2	1	2	2	2
Persona 14	2	2	1	2	2	2	1	1	2
Persona 15	2	1	2	1	1	2	1	2	1
Persona 16	1	2	1	2	2	1	2	1	1
Persona 17	2	2	1	2	2	1	1	2	2
Persona 18	2	1	2	1	1	2	1	2	1
Promedio	1.63	1.75	1.38	1.75	1.75	1.38	1.38	1.75	1.50

Data recolectada (Posprueba)

	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9
Persona 1	4	5	5	4	5	5	5	5	5
Persona 2	5	5	5	4	4	4	4	5	4
Persona 3	4	4	5	5	4	5	5	5	4
Persona 4	4	4	5	4	5	4	5	5	5
Persona 5	4	5	5	4	4	5	4	5	4
Persona 6	4	5	5	4	5	5	5	5	5
Persona 7	4	4	5	5	4	5	5	5	5
Persona 8	5	5	5	4	4	4	4	5	5
Persona 9	4	5	5	4	5	5	5	5	5
Persona 10	5	5	5	4	4	4	4	5	4
Persona 11	4	4	5	5	4	5	5	5	4
Persona 12	4	4	5	4	5	4	5	5	5
Persona 13	4	5	5	4	4	5	4	5	4
Persona 14	4	5	5	4	5	5	5	5	5
Persona 15	4	4	5	5	4	5	5	5	5
Persona 16	5	5	5	4	4	4	4	5	5
Persona 17	4	5	5	4	5	5	5	5	5
Persona 18	5	5	5	4	4	4	4	5	4
Promedio	4.25	4.63	5.00	4.25	4.38	4.63	4.63	5.00	4.63

Anexo 7 - Confiabilidad de los instrumentos de recolección de datos

Resumen de procesamiento de casos

		N	%
Casos	Válido	18	100,0
	Excluido[a]	0	,0
	Total	18	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,786	9

Anexo 8 - Solución tecnológica propuesta

APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27002:2013 PARA LA SEGURIDAD INFORMÁTICA DE LA UGEL 'UTCUBAMBA' – 2022

Según OSTEC (2016), la seguridad de la información es un tema que ha ganado cuerpo en los últimos años, obteniendo espacio en los medios y convirtiéndose en «commodity», en empresas de los más variados portes y segmentos. En contrapartida es importante subrayar que la popularización del término SI (Seguridad de la Información) fue motivada por la elevación en el número de incidentes de seguridad, ocurridos a nivel mundial. Los trastornos generados por esos incidentes son variados, generando daños a la imagen del negocio o fuga de informaciones críticas, lo que puede resultar en pérdidas financieras sustanciales.

El aumento del número de ocurrencias influye en la percepción de valor sobre inversiones en seguridad informática y hacen que las empresas busquen la estructuración de procesos para garantizar que sus negocios estén protegidos contra los más variados tipos de amenazas virtuales.

En medio de este escenario surgió la norma internacional ISO/IEC 27002, que se centra en las buenas prácticas para gestión de la seguridad de la información. En los días de hoy esa es fundamental para la consolidación de la seguridad informática de una institución o entidad (privada o pública), garantizando la continuidad y el mantenimiento de los procesos de seguridad, alineados a los objetivos estratégicos de la organización.

El principal objetivo de la ISO 27002 es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

Algunos de los beneficios asociados a la aplicación de la norma son:

- Mejor concienciación sobre la seguridad de la información;
- Mayor control de activos e información sensible;
- Adecuado enfoque para la implementación de políticas de control;
- Oportunidad de identificar y corregir puntos débiles;
- Promueve la reducción de costos con la prevención de incidentes de seguridad de la información.
- Organización por procesos y mecanismos bien diseñados y gestionados.

La parte principal de la norma se encuentra distribuida en dominios, que corresponden a un conjunto de objetivos y controles que contempla la seguridad informática.

A continuación, se presentará la solución tecnológica propuesta para la UGEL 'Utcubamba' basado en el empleo de este estándar internacional.

- Dominio 8: Gestión de activos

Activo, según la norma, es cualquier cosa que tenga valor para la UGEL y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos.

Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

- Objetivo 8.1: Responsabilidad sobre los activos
  - ✓ No existe un inventario de activos asociados con información e instalaciones de procesamiento de información.
  - ✓ Al no contar con un inventario de activos, no existe mantenimiento de éstos.
  - ✓ Hace falta de un inventario de activos que permita establecer normas para un uso aceptable de los activos.
  - ✓ Debido a la coyuntura se ha establecido acuerdos que permiten a los empleados sacar activos de la organización, que posteriormente deben ser devueltos.

  Estado: Se debe aplicar los Controles de seguridad 8.1.1, 8.1.2 y 8.1.3.

- Objetivo 8.2: Clasificación de la información
  - ✓ Hace falta clasificar la información en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.
  - ✓ Se debe etiquetar los procedimientos desarrollados e implementados en concordancia con el esquema de clasificación de la información a adoptar.
  - ✓ Se debe establecer un esquema de clasificación de la información a fin de desarrollar y establecer los procedimientos para el manejo de activos.

  Estado: Se debe aplicar los Controles de seguridad 8.2.1, 8.2.2 y 8.2.3.

- Objetivo 8.3: Manejo de los soportes de almacenamiento
  - ✓ Hace falta procedimientos que permita gestionar los medios.
  - ✓ No existe procedimientos formales para poner a disposición los medios de manera segura.
  - ✓ Hace falta proteger los medios del acceso no autorizado durante su transporte.

  Estado: Se debe aplicar los Controles de seguridad 8.3.1, 8.3.2 y 8.3.3.

- Dominio 9: Control de accesos

El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios en la UGEL, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

- Objetivo 9.1: Requerimiento de negocio para el control de accesos
  - ✓ Hace falta políticas documentadas y revisadas que establezcan el control de acceso a instalaciones de procesamiento de información.
  - ✓ Existen restricciones a servicios de red, pero hace falta especificar más los servicios autorizados a usar.

  Estado: Se debe aplicar los Controles de seguridad 9.1.1 y 9.1.2.

- Objetivo 9.2: Gestión de acceso de usuario
  - ✓ Hace falta establecer procesos formales para el registro y baja de usuarios, lo que permite una correcta asignación de derechos de acceso.
  - ✓ Hace falta formalidad en la asignación de acceso a los usuarios, así también al revocar estos.
  - ✓ Los derechos de acceso privilegiados se encuentran controlados por la unidad de sistemas de la organización.
  - ✓ La asignación de información de autentificación se controla a través del correo y teléfono personal.
  - ✓ No existe revisión de derechos de acceso por parte de los propietarios de activos.
  - ✓ Hace falta formalizar la remoción de derechos de acceso a información de los empleados al concluir su empleo.

  Estado: Se debe aplicar los Controles de seguridad 9.2.1, 9.2.2, 9.2.5 y 9.2.6.

- Objetivo 9.3: Responsabilidades del usuario
  - ✓ No existen prácticas establecidas por la organización para el uso de información de autenticación secreta por parte de los usuarios.

  Estado: Se debe aplicar los Controles de seguridad 9.3.1.

- Objetivo 9.4: Control de acceso a sistemas y aplicaciones
  - ✓ Hay un control establecido mediante roles para restringir el acceso a la información y funciones del sistema.
  - ✓ Hace falta una política de control de acceso, para formalizar el procedimiento de ingreso seguro.
  - ✓ Si existe un sistema de gestión de contraseñas, lo cual asegura la calidad de estas.
  - ✓ Hace falta establecer un control estricto de programas que sean capaces pasar por alto los controles del sistema.
  - ✓ El acceso al código fuente está restringido por parte de la unidad de sistemas de la organización.

    Estado: Se debe aplicar los Controles de seguridad 9.4.2 y 9.4.4.

- Dominio 10: Cifrado

Se debe proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas. La UGEL debería utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

- Objetivo 10.1: Controles criptográficos
  - ✓ Se debe de desarrollar e implementar un método criptográfico a fin de proteger la información sensible.
  - ✓ Se debe implementar una política que indique tiempo de vida de las claves criptográficas.

Estado: Se debe aplicar los Controles de seguridad 10.1.1 y 10.1.2.

- Dominio 11: Seguridad física y ambiental

  Los equipos e instalaciones de procesamiento de información crítica o sensible en la UGEL deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales.

  Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

  - Objetivo 11.1: Áreas seguras
    - ✓ Los perímetros de seguridad están definidos con pegatinas, avisos, carteles, etc.
    - ✓ El acceso a las áreas restringidas es sólo a personal autorizado, que son debidamente custodiadas.
    - ✓ Ambientes seguros y acondicionados. Personal de seguridad encargado de resguardar los ambientes.
    - ✓ Ambientes acondicionados contra amenazas naturales, externas y accidentes.
    - ✓ No existen procedimientos para realizar trabajos en áreas seguras.
    - ✓ No existen áreas de despacho y carga.

      Estado: Se debe aplicar los Controles de seguridad 11.1.5 y 11.1.6.

  - Objetivo 11.2: Seguridad de los equipos
    - ✓ Los equipos están asegurados contra robo (términos de referencia en contrato de vigilancia) y desastres naturales.
    - ✓ El área cuenta con pozo a tierra que protege a los equipos, así también con reguladores de voltaje en cada uno de éstos.
    - ✓ Los equipos de telecomunicaciones están protegidos y debidamente identificados y señalados.
    - ✓ Existe un personal asignado para las tareas de servicio y asistencia de equipos.
    - ✓ No se puede proceder al retiro de equipos sin autorización de los encargados.
    - ✓ Los equipos están identificados por la oficina de control patrimonial.
    - ✓ Cuando se da de baja un equipo, no se asegura que la información sea totalmente eliminada.
    - ✓ Debería de establecerse un protocolo desatendido.
    - ✓ Implementar una política de procedimientos de limpieza de escritorio.

      Estado: Se debe aplicar los Controles de seguridad 11.2.7, 11.2.8 y 11.2.9.

- Dominio 12: Seguridad en la operativa

  Se debe controlar en la UGEL la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada. Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento. Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad que posee la organización. El control de la realización de las copias de resguardo de información, así como la prueba periódica de su restauración permiten garantizar la restauración de las operaciones en los tiempos de recuperación establecidos y acotar el periodo máximo de pérdida de información asumible para cada organización. Se deberían definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados a las redes de la organización.

  Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

  - Objetivo 12.1: Procedimientos operacionales y responsabilidades

    - ✓ Es importante disponer de la información a todos los usuarios que necesiten saber sobre los procedimientos operativos.
    - ✓ Debe establecerse un control de los cambios en los procesos, instalaciones y sistemas relacionados a la información.
    - ✓ Debe realizarse un monitoreo a las proyecciones de las capacidades del desempeño requerido del sistema.
    - ✓ A fin de reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

      Estado: Se debe aplicar los Controles de seguridad 12.1.1, 12.1.2, 12.1.3 y 12.1.4.

  - Objetivo 12.2: Protección de software malicioso

    - ✓ Se debe llevar un control de las incidencias sobre la detección, prevención y recuperación contra código malicioso.

      Estado: Se debe aplicar el Control de seguridad 12.2.1.

- Objetivo 12.3: Respaldo
  - ✓ Se hace uso de herramientas en la nube como respaldo.

    Estado: No es necesario aplicar el Control de seguridad 12.3.1.

- Objetivo 12.4: Bitácoras y monitoreo
  - ✓ Hace falta el registro de los eventos realizados por el personal, así también como fallas presentadas en los sistemas
  - ✓ Hace falta mantener la privacidad de la información generada por los eventos
  - ✓ No existe la necesidad de registrar los eventos realizados por el personal administrativo
  - ✓ Los relojes están sincronizados de acuerdo a la zona horaria que brinda internet.

    Estado: Se debe aplicar los Controles de seguridad 12.4.1 y 12.4.2.

- Objetivo 12.5: Control de software operacional
  - ✓ Se debería de tener los procedimientos documentados para la instalación de software en sistemas operacionales.

    Estado: Se debe aplicar el Control de seguridad 12.5.1.

- Objetivo 12.6: Gestión de vulnerabilidades técnicas
  - ✓ Se debería tener documentada aquellas vulnerabilidades técnicas que pueden afectar a los sistemas de información.
  - ✓ Se tienen explícitas las reglas para que los usuarios no realicen alguna instalación.

    Estado: Se debe aplicar el Control de seguridad 12.6.1.

- Objetivo 12.7: Consideraciones de auditoría de sistemas de información
  - ✓ Se debería auditar de las actividades que involucran al sistema de información y los procesos del negocio.

    Estado: Se debe aplicar el Control de seguridad 12.7.1.

- Dominio 13: Seguridad en las telecomunicaciones

Se debe asegurar la protección de la información en la UGEL que se comunica por redes telemáticas y la protección de la infraestructura de soporte. La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección. La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección. Los intercambios de información por parte de las organizaciones se deberían basar en una política formal de intercambio y en línea con los acuerdos de intercambio, y debiera cumplir con cualquier legislación relevante.

Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

- Objetivo 13.1: Gestión de seguridad en red
  - ✓ Debe gestionarse el control de las redes, mediante la configuración correcta de los equipos, aplicaciones e información que comprometen.
  - ✓ Se debe tener mecanismos de seguridad, niveles de servicio y requisitos de gestión.
  - ✓ Se debe segregar la información para los usuarios.

  Estado: Se debe aplicar los Controles de seguridad 13.1.1, 13.1.2 y 13.1.3.

- Objetivo 13.2: Transferencia de información
  - ✓ Hace falta políticas y/o directivas establecidas para la transferencia formal de información
  - ✓ No existe un acuerdo que dirija la transferencia segura de la información con las partes externas
  - ✓ Los correos utilizados para mensajería son institucionales, lo cual reduce el riesgo de alteraciones.
  - ✓ Al contratar personal para la unidad, se indican los acuerdos de confidencialidad.

  Estado: Se debe aplicar el Control de seguridad 13.2.1.

- Dominio 14: Adquisición, desarrollo y mantenimiento de sistemas

  Los requisitos de seguridad de los sistemas de información en la UGEL deben ser identificados y acordados antes de su desarrollo y/o de su implementación para ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por criptografía.

  Con respecto a la aplicación de la norma internacional ISO/IEC 27002:2013 correspondiente a este dominio, se tuvo lo siguiente:

  - Objetivo 14.1: Requerimientos de seguridad en sistemas de información
    - ✓ Hace falta establecer requisitos relacionados a la seguridad cuando se realiza la planificación de un sistema de información.
    - ✓ Se cuenta con el firewall FORTINET.
    - ✓ Se debe tener directivas o protocolos para proteger las transacciones de servicios de aplicaciones.

      Estado: Se debe aplicar los Controles de seguridad 14.1.1 y 14.1.3.

  - Objetivo 14.2: Seguridad en el proceso de desarrollo y soporte
    - ✓ Existen reglas para un desarrollo que software están establecidas por el área de tecnologías de la información.
    - ✓ Hace falta una revisión exhaustiva de los módulos de sistemas desarrollados antes de su despliegue.
    - ✓ Se debe control en las actualizaciones o modificaciones en paquetes software.
    - ✓ Existe un ambiente designado para el área de TI donde se da atención a los sistemas de comunicación y los sistemas de información
    - ✓ Los encargados del área de TI, se mantienen monitoreando las actividades de desarrollo de los sistemas contratados.
    - ✓ Se debería llevar a cabo pruebas de seguridad durante el desarrollo.
    - ✓ Se debe tener un esquema donde se tenga mapeado los requerimientos de los sistemas, a fin de tener un Checklist de las implementaciones.

      Estado: Se debe aplicar los Controles de seguridad 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.8 y 14.2.9.

  - Objetivo 14.3: Datos de prueba
    - ✓ Hace falta usar información para el desarrollo y pruebas de los sistemas.

      Estado: Se debe aplicar el Control de seguridad 14.3.1.

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, AGREDA GAMBOA EVERSON DAVID, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - TRUJILLO, asesor de Tesis titulada: "Aplicación de la Norma internacional ISO/IEC 27002:2013 para la Seguridad informática de la Unidad de Gestión Educativa Local 'Utcubamba', 2022", cuyos autores son CRUZ CALDERON FRANKLYN, ABAD CHAVEZ MANUEL, constato que la investigación tiene un índice de similitud de 23.00%, 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.

TRUJILLO, 22 de Agosto del 2022

Apellidos y Nombres del Asesor:	**Firma**
AGREDA GAMBOA EVERSON DAVID **DNI:** 18161457 **ORCID:** 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 22-08-2022 15:52:29

Código documento Trilce: TRI - 0422901

INVESTIGA UCV