UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Propuesta de un Modelo de seguridad informática para la Protección de datos en la Municipalidad Distrital de Pinra, Huánuco 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

AUTORA:

Sanchez Campos, Krystel Elena (orcid.org/0000-0002-2497-1413)

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

LIMA - PERÚ

2022

Dedicatoria

A Dios todo poderoso por cuidarme en todo este tiempo.

A mis Padres por su infinito amor y cuidado.

A mis hermanos por su aliento constante para seguir adelante.

Krystel

Agradecimiento

A la Universidad César Vallejo por su apoyo.

A la Municipalidad Distrital de Pinra que brindó y compartió la información solicitada.

A mi asesor de tesis por su orientación y constante apoyo en el desarrollo de la investigación.

La autora

Índice de contenidos

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

Esta investigación tuvo como objetivo mejorar la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022 mediante la propuesta de un modelo de seguridad informática; el tipo es investigación fue aplicada y de diseño preexperimental. Se utilizó una muestra poblacional de 18 personas, además de la aplicación de la norma internacional ISO/IEC 27002:2013 para la propuesta de la solución tecnológica. Como resultados se tuvo que, para el primer indicador “Prevención de la divulgación no autorizada” hubo un incremento de 69.40% de satisfacción, para el segundo indicador “Prevención de la modificación no autorizada” hubo un incremento de 65.20% de satisfacción y para el tercer indicador “Prevención de la interrupción no autorizada” hubo un incremento de 67.30% de satisfacción, lo cual permitió un resultado favorable al elaborar la solución propuesta. Como conclusión general se tuvo que, la propuesta de un modelo de seguridad informática mejoró significativamente la protección de datos de la municipalidad en estudio.

Palabras clave: modelo, seguridad informática, protección de datos, municipalidad distrital.

Abstract

The objective of this research was to improve data protection in the District Municipality of Pinra in the city of Huánuco in the year 2022 by proposing an information security model; the type of research was applied and of pre-experimental design. A population sample of 18 people was used, in addition to the application of the international standard ISO/IEC 27002:2013 for the proposal of the technological solution. As results it was had that, for the first indicator "Prevention of unauthorized disclosure" there was an increase of 69.40% satisfaction, for the second indicator "Prevention of unauthorized modification" there was an increase of 65.20% satisfaction and for the third indicator "Prevention of unauthorized interruption" there was an increase of 67.30% satisfaction, which allowed a favorable result when elaborating the proposed solution. As a general conclusion, the proposal of an information security model significantly improved the data protection of the municipality under study.

Keywords: model, information security, data protection, district municipality.

I. INTRODUCCIÓN

ESIC (2018) sostiene que, hoy en día, se vive en la época de la sociedad informática, donde el desarrollo de los negocios en escenarios digitales avanza creciendo cada vez más rápido, cada vez en un periodo de tiempo más corto. En este escenario, el peligro de pérdida de datos aumenta y se vuelve más costoso. Por lo tanto, las entidades deben mapear sus medidas de control de mitigación con un *modelo de seguridad informática*.

CEPAL (2020) manifiesta que, la *protección de datos* hace referencia a los derechos de los interesados cuya data se recopila, almacena y procesa teniendo en cuenta la finalidad de los mismos. Si se incluyen personas en el estudio, es importante tomar en cuenta aspectos legales y de carácter moral relacionados con el intercambio de información.

A nivel internacional, PowerData (2020) afirma que, actualmente, las organizaciones globales realizan grandes inversiones en tecnologías informáticas sobre todo en estableces mecanismos de defensa para ataques por Internet y, de esta forma cuidad de sus activos críticos: marca, talento humano y datos de los consumidores finales. En tal sentido, todos los retos respecto a seguridad informática presentan aspectos comunes para toda organización como es la implementación de medidas de protección en los colaboradores, las operaciones y la tecnología.

A nivel nacional, Alvarado (2016) sostiene que, Las organizaciones de hoy en el Perú son más dependientes de la información, de las tecnologías que la procesan y transmiten, y de los sistemas informáticos, estos últimos que soportan su gestión. Los sistemas informáticos consisten en una colección de elementos: personal, datos, programas y equipos orientados a la provisión, proceso y transferencia de información para realizar tareas específicas. Existen cuatro tipos de medidas de seguridad para proteger dichos sistemas: lógicas, físicas, administrativas y legales.

A nivel local, se tiene a la Municipalidad Distrital de Pinra, la cual es una entidad pública ubicada en la provincia de Huacaybamba, Departamento de Huánuco. Es un órgano administrativo con personalidad jurídica pública promotor del desarrollo local, que está en plena capacidad para el

cumplimiento de su objeto (Ley N° 27972 - Ley Orgánica de Municipalidades). Esta comunidad provee y controla la provisión de los servicios estatales básicos necesarios en pro del beneficio comunitario y del progreso local del área elegida (MDP, 2018).

La municipalidad en estudio, actualmente no cuenta con una propuesta tecnológica como solución en la protección de datos, encontrándose la data vulnerable a cualquier ataque externo o incluso interno habiéndose identificado los siguientes **problemas específicos**: Poca regulación para restringir el uso de la data; Poca regulación para restringir la manipulación de la data; Poca regulación para restringir la disponibilidad de la data.

Para hacer frente a los problemas descritos anteriormente, fue necesario proponer un **Modelo de Seguridad Informática (MSI)**, que permitiera proponer un esquema para especificar y forzar políticas de seguridad en la entidad municipal.

Se contempló la **formulación del problema**: *General:* ¿De qué modo la propuesta de un modelo de seguridad informática influye en la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022?; *Específicos:* Inconveniente específico 1 - ¿De qué modo la propuesta de un modelo de seguridad informática influye en la prevención de la divulgación no autorizada de la información de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022? Inconveniente específico 2 - ¿De qué modo la propuesta de un modelo de seguridad informática influye en la prevención de la modificación no autorizada de la información de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022? Inconveniente específico 3 - ¿De qué modo la propuesta de un modelo de seguridad informática influye en la prevención de la interrupción no autorizada de la información de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022?

Se contempló la **justificación de la investigación**: *Conveniencia*, porque logró fortalecer la credibilidad de la información institucional exhibiendo ser una institución más segura; *Relevancia social*, porque incluyó un beneficio para la comunidad dado que se contará con datos mejor protegidos para la realización de sus operaciones cotidianas; *Utilidad*

metodológica, porque se convirtió en el punto de parte de próximas investigaciones sobre modelos de seguridad informática; *Implicancias prácticas*, porque permitió mejorar la protección de los datos; *Valor teórico*, porque hizo posible comprender las teorías respecto al modelo de seguridad informática y la protección de datos.

Se contempló los **objetivos**: *General*: Mejorar la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022 mediante la propuesta de un modelo de seguridad informática; *Específicos*: Objetivo específico 1 - Mejorar la prevención de la divulgación no autorizada de la información; Objetivo específico 2 - Mejorar la prevención de la modificación no autorizada de la información; Objetivo específico 3 - Mejorar la prevención de la interrupción no autorizada de la información.

Se contempló la **hipótesis:** *General:* "La propuesta de un modelo de seguridad informática mejora significativamente la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022"; *Específicas:* Supuesto específico 1 - *"*La propuesta de un modelo de seguridad informática mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022"; Supuesto específico 2 - "La propuesta de un modelo de seguridad informática mejora la prevención de la modificación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022"; Supuesto específico 3 - "La propuesta de un modelo de seguridad informática mejora prevención de la interrupción no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

II. MARCO TEÓRICO

Se examinó un conjunto de **antecedentes** (artículos de investigación científica e investigaciones) como sigue:

Antecedentes internacionales, se tuvo:

Arias y Botero (2019) en su investigación tuvo como objetivo informar y orientar al lector según buenas prácticas de seguridad para una información veraz; las mismas necesidades surgieron con el tiempo, y de esto surgió un conjunto de instrucciones que bien soportan el sistema de administración de seguridad informática. También, se observó una pequeña, pero importante introducción, donde se señaló la necesidad de emplear recomendaciones de seguridad informática y sus beneficios, así como el análisis del problema, donde se plantea el problema o la pregunta a resolver que, en este estudio fue revelado de una manera sencilla. Luego, se profundizó en el tema, creando definiciones que llevaron a por qué un lienzo paralelo con los empleados es tan importante para una empresa y, finalmente una forma de fortalecer los procesos de seguridad informática, lo que requiere que los participantes comprendan la relevancia de la correcta aplicación de la gestión informática.

Hidalgo (2017) en su investigación tuvo como objetivo generar un modelo de administración de seguridad informática para proteger y certificar la data técnica de las instituciones. Para ello, se realizó un juicio y examen de vulnerabilidades informáticas en el Consejo de Justicia, que a través de sus unidades brindaba servicios jurídicos a nivel nacional a toda la población; por lo tanto, el contenido de este trabajo fue el desarrollo de un modelo de gestión dirigida, que logró articular la estrategia institucional, las autorizaciones y productos vinculados con la seguridad informática de acuerdo con el estatuto de gestión organizacional integral de la entidad en estudio.

Yañez (2017) en su investigación tuvo como objetivo gestionar, supervisar, compilar y favorecer continuamente la seguridad informática. El método utilizado en esta investigación se basa en ciclos aprobatorios de consenso y mediación de puntos de vista soportados por un riguroso trabajo grupal orientado a flexibilizar la puesta en práctica de directivas y

procedimientos de seguridad informática. En esta investigación, se dispone del empleo de un método de creación de un SGSI tomando adicionalmente, la gestión de riesgos siguiendo los lineamientos y las recomendaciones de la norma internacional ISO 31000. Las operaciones estratégicas de la alta dirección se priorizan aquí en función de la exposición al riesgo y el impacto. Se optimizó la disposición de planes de seguridad informática, promoviendo el aprendizaje y la conformación de equipos de trabajo centrados en metas prioritarias, sin perder el visionamiento global y la meta final. Hubo dos procesos de auditoria a nivel interno y externo, todo con la finalidad de examinar el funcionamiento del SGSI y sus componentes. Los procesos de auditoria se dieron por separado con respecto a los equipos encargados de la aplicación del SGSI junto con directivas y procedimientos de seguridad informática. Al final, se concluyó que, el diagnóstico presente de la seguridad informática está a un nivel medianamente aceptable siendo un paso importante porque al comienzo de la investigación no se contaba con un SGSI o directivas y pasos efectivos encaminados al resguardo de la seguridad informática.

Romo y Valarezo (2016) en su investigación intentaron informar y orientar al interesado en las mejores recomendaciones de seguridad informática; la misma que ha surgido con el tiempo, y todos los fraudes derivados de filtraciones, impresas o no. En el primer capítulo se pudo ver una pequeña introducción, la cual esboza la necesidad y desarrollo de buenas prácticas de seguridad y los objetivos en forma general y en forma específica considerados para el desarrollo de este proyecto. los problemas más comunes que surgieron por la falta de estándares y/o directivas de seguridad informática. En el segundo capítulo, se abordó el tema con más profundidad, se introdujo la terminología básica y cada parte de esta tesis se apoyó en buenas prácticas de seguridad. En el tercer capítulo se presentó una guía de ejecución de directivas de seguridad informática, en la cual se dieron a conocer las buenas prácticas que la Universidad debía seguir y seguir paso a paso para obtener la información necesaria, lo que le permitió crear controles de seguridad basados en políticas y, a su vez, reducir el riesgo.

Pérez (2015) en su investigación tuvo como objetivo dar soporte a la no modificación, disponibilidad y reserva de los activos informáticos de la organización que almacenan data relevante, toda vez que, se realizó un estudio de los controles necesarios contenidos en la norma internacional ISO/ICE 27002 a fin de cumplir con el campo de la administración de activos.

Antecedentes nacionales, se tuvo:

Ticona (2022) en su investigación tuvo como objetivo establecer la consecuencia relevante de un modelo de seguridad informática empleando el estándar mundial ISO/IEC 27001:2013 orientado a disminuir los inconvenientes que presentaban los activos informáticos de una empresa particular. El estudio realizado consideró que 32 empleados de la empresa, cuyo supuesto de investigación fue crear un modelo de seguridad informática para la reducción de peligros de los activos informáticos. Se logró demostrar que la solución propuesta tuvo un resultado positivo en los objetivos planteados.

Aguinaga (2021) en su investigación tuvo como objetivo establecer un método de administración basado en el estándar mundial ISO/IEC 27001:2013 para establecer el impacto en la protección informática de la entidad financiera. Se empleó un método cuantitativo en una investigación preexperimental. Se tuvo una muestra de la población de 24 actividades por indicador. Como resultado se logró mejorar la confidencialidad de 75,52% a 87,36%, para la integridad de datos se observó una mejora de 50,83% a 76,32% y para la disponibilidad de datos se observó un aumento significativo a 96,81. 99,93%.

Chavarry (2021) en su investigación tuvo como objetivo examinar las consecuencias de implementar las normas internacionales ISO 27001 y 27002 con respecto a la seguridad informática de una entidad policial. El diseño de investigación fue cuasiexperimental y se realizó con la disposición de dos (2) grupos para la preprueba y posprueba.

Cahuana y Cahuana (2021) en su investigación tuvo como objetivo conocer la consecuencia de utilizar un sistema de comunicación basado en la norma de administración de seguridad informática ISO/IEC 27001 en una

empresa. Se tuvo una investigación de tipo aplicada y con diseño preexperimental. La encuesta contempló un procedimiento de selección de datos y como ayuda se utilizó un formulario de registro. Como resultados se confirma que la aplicación del sistema de red dio un resultado real en la administración de la seguridad informática; respectivamente, los indicadores de los informes presentados durante el período establecido, los informes integrados formados y los informes reservados presentados de forma intangible. Se coincide en que ha aumentado la “proporción de mensajes confidenciales entregados con amabilidad”, con una media del 71,89% sin sistema y del 96,89% con sistema, un aumento de 25,00 en la satisfacción. informes confidenciales. Se encontró que la "Proporción de informes generados" sin el software web promedia 69,11%, pero con el software la cifra promedio es de 96%, mostrando una mejora de 27,33% en la satisfacción del usuario con informes completos. Se encontró que la “Proporción de informes entregados en el período especificado” aumentó, con un promedio de 79% sin el sistema y 96,00% con el sistema, logrando una mejora satisfactoria de solo 16,56. usuarios con informes enviados.

Risco (2021) en su investigación tuvo como objetivo examinar la consecuencia de contar con un método de administración de protección informática de una entidad empleando el estándar mundial ISO/IEC 27001:2013, puesto que presentaba muchas debilidades en las operaciones de las unidades de negocio que lo conforman. Se empleó el método cuantitativo con una investigación de diseño preexperimental. La muestra poblacional empleada fue de veinte (20) operaciones por indicador obteniendo los siguientes resultados: 68.85% de vulnerabilidad; 75.40% de confidencialidad y 63.50% de integridad logrando mejorar en todos los aspectos la seguridad informática con una eficiencia media de 80%.

Zapata (2021) en su investigación tuvo como objetivo examinar los puntos clave de éxito en la aplicación de un método de administración de protección informática en una entidad particular. Se empleó el método descriptivo. Con respecto a los puntos clave de éxito, se entrevistó a cada gerente regional y se entregó una lista de verificación a un grupo de trabajo integrado por el supervisor y la gerencia involucrada en la decisión. Como

resultados se tuvo: se estableció que en la entidad identificó cinco (5) elementos: disposición de la dirección, paradigma institucional, grado de seguridad informática, examinación del desempeño, reflexión. Se concluyó que cada punto clave debe fomentar acciones para lograr la implementación del método de administración de protección informática en la entidad, toda vez que, se concluyó que el punto clave más relevante fue la reflexión, la cual tuvo un impacto de 77.8%, porque se debían medir otros puntos clave para que se determine primero y, así crear una buena actitud hacia la implementación del SGSI dentro de la empresa.

Alarcón y otros (2020) en su artículo de investigación sostuvieron que, el desarrollo de la tecnología global requiere, entre otras cosas, de la gestión de información relevante para poder ser considerada indispensable desde el la perspectiva estratégica de las empresas involucradas. El motivo del presente trabajo fue inspeccionar la consecuencia de la implementación del estándar mundial ISO 27001 en la seguridad informática de una entidad privada en la ciudad de Lima - Perú. La consecuencia de la aplicabilidad del estándar mundial ISO 27001 sobre la implementación del método cuantitativo se determinó mediante un estudio piloto, por lo cual se consideró una muestra poblacional de 30 empleados. Como conclusión se logró tener un impacto positivo en la seguridad informática y en las dimensiones del acceso, modificación y recursos.

Poicon y Ramírez (2020) en su investigación tuvo como objetivo proponer la generación del método de administración de protección informática de un distrito a través de la NTP-ISO/IEC 27001:2014 empleando un esbozo preexperimental y estudio aplicativo, adaptando el método PDCA para crear una propuesta de sistema, considerando peligros, debilidades y efectos de riesgo en los activos informáticos, y así proponer la formulación de directivas e indicadores de monitoreo. Durante la encuesta, los activos de información de varios municipios identificados y evaluados según categorías, la mayoría de los cuales eran equipos de data procesada con un grado de riesgo elevado (57,50%), siendo los más significativos el deteriorado funcionamiento de los equipos, falla de comunicación conexiones y ausencia de servicios de soporte. El grado de debilidades se consideró elevado (49%),

siendo la vulnerabilidad más importante la protección física insuficiente y el impacto adverso de los potenciales problemas en un 15% y 30% respectivamente. Se concluyó que, las grietas de seguridad informática presentes se podían identificar con base en una investigación básica para disponer de directivas, variables de supervisión para la exploración y valoración de la seguridad informática del municipio.

Cruz y Huamaní (2019) en su investigación tuvo como objetivo la implementación e integración de la protección informática empleando la NTP ISO 27001 en una organización empresarial. Se buscó examinar los efectos de la solución propuesta en la empresa, porque con la aplicación de esta norma y sus controles, fue posible mejorar debilidades y administrar adecuadamente cada riesgo informático. El resultado fue que, a través de la implementación de la seguridad informática con la norma señalada tuvo un impacto positivo.

Rojas (2019) en su investigación tuvo como objetivo implementar la NTP ISO/IEC 27001:2014 mejorando la seguridad informática sobre la base de datos de una entidad pública. Los sistemas informáticos de la entidad soportan las operaciones fundamentales de la entidad pública creando amplios volúmenes de información en el desarrollo de las operaciones del día a día. Existe un reto permanente en la administración de la data, más aún si se trata de seguridad, pues se debe proteger la posición clave que soporta la data de millones de personas; es decir, la data administrada. Los controles de seguridad establecidos por la NTP ISO/IEC 27001:2014 ha permitido la administración confiable, integra y disponible para la aplicabilidad de las mejores sugerencias basadas en el direccionamiento estratégico de la organización. El enfoque empleado fue cuantitativo, aplicado con diseño experimental. Las reuniones con los expertos de las áreas orgánicas y la subdirección de administración de la data tuvieron como consecuencia la elaboración de documentos normativos con la selección, indicadores y previsiones de normas técnicas de control necesarias para garantizar la protección informática de la certificación ISO/IEC 27001:2013 posterior.

Chuna (2018) en su investigación tuvo como objetivo ofrecer un sistema de administración de protección informática empleando directrices de la NTP

vigente. Realizó un análisis de los activos informáticos identificando debilidades y potenciales problemas. Se empleó la metodología MAGERIT y se obtuvo como resultado que el 50% de los activos evaluados poseen alto riesgo, el 40% de éstos poseen riesgo alto, el 5% de éstos poseen riesgo medio y el 5% final riesgo bajo. Se dispuso de 75 controles de seguridad para el manejo de estos potenciales problemas. Luego, se recomendaron inspecciones y directivas seguras para la entidad estableciendo formas de protección de los datos mediante la administración de los potenciales problemas para el aprovechamiento adecuado de eventos no deseados, definir funciones y garantes para la rápida atención de inconvenientes de seguridad y pasos reglamentarios adaptando el formato aprobado por ONGEI para la documentación del SGSI.

Maquera y otros (2017) en su artículo sostuvieron que, una amplia cantidad de organizaciones no presentan controles seguros con respecto a la protección de sus datos. El desarrollo tecnológico y la administración de la data se vuelve cada vez más compleja trayendo consigo una diversidad de amenazas que tienden a bajar el nivel de servicio en los activos en el espacio de los planes de digitalización. El propósito de este trabajo fue el desarrollo de formas de monitoreo y administración de activos basados en el estándar mundial ISO/IEC 27002 empleando indicadores planteados en la guía de medición. Con la ayuda del análisis de riesgo se pudo afirmar que el nivel de riesgo se redujo mediante mecanismos basados en el control administrativo-técnico-físico.

Ayala (2017) en su investigación tuvo como objetivo examinar el desarrollo del método de administración de seguridad informática con respecto al proceso de administración de riesgos de la entidad. El trabajo de investigación fue aplicado y con diseño pre experimental, se tomó como muestra poblacional todos los recursos de datos complejos relacionados con el método de administración de peligros potenciales de la entidad. La recopilación de la data se realizó mediante la herramienta ficha observable. Al final. Se concluyó que, el desarrollo del método de administración de seguridad informática mejora el proceso de administración del riesgo en la entidad citada.

Salsavilca (2017) en su investigación tuvo como objetivo la aplicación del estándar mundial ISO 27001 en la administración de la seguridad informática de una empresa empleando la metodología PDCA como herramienta de mejora continua para la calidad adaptada al estándar mundial ISO 27001:2014, siendo la información un recurso importante para la continuidad del negocio en sus diversas presentaciones como herramientas de software, equipamiento en hardware u otros métodos de transferencia y distribución en la entidad, existiendo amenazas a la seguridad de los datos. Las frecuentes agresiones que puede darse, el trabajo generado para promover una adecuada gestión de riesgos que ha permitido a los sistemas evitar o reducir las fallas de las redes y todos los posibles ataques o desastres. En general, los resultados luego de la solución propuesta fueron buenos en términos de acceso, probidad y usabilidad, debido a que sus indicadores, como el nivel de información divulgada sin permiso, incluyen información publicable. Las tasas de datos falsificados y frecuentemente inaccesibles fueron del 92,23%, 97,42% y 90,95% respectivamente, lo que indica un mayor control y una mayor seguridad. En resumen, la implementación del estándar mundial ISO 27001 redujo significativamente los potenciales problemas de información y logró un grado de confianza para sus activos informáticos.

Maldonado (2016) en su investigación tuvo como objetivo establecer el impacto de la aplicación del estándar mundial ISO 27001 en la seguridad de los archivos de carácter académico en la entidad en estudio. La investigación fue aplicada y con un diseño preexperimental. El conjunto completo estuvo conformado por 26 registros de indicadores de riesgo. La técnica de recopilación de data utilizada fue la observación, la cual se realizó como herramienta a la ficha de observación. Como resultado, existió una consecuencia positiva en la documentación del colegio en estudio: según cambios permitidos, bajó a 80.8% en la etapa de prueba y siendo la administración de riesgos una reducción del 19% en la posprueba.

También, se recurrió a la examinación de un grupo de **bases teóricas** como soporte para un mejor entendimiento de las variables de estudio presentes en esta investigación como sigue:

Modelo de seguridad informática, Conjunto de métricas adecuadas respecto a protección de activos informáticos a fin de evaluar la reserva, probidad y disposición de la información, porque este es el modelo de gestión que toda organización desea implementar (Cano, 2018). En cuanto a la usabilidad es resulta relevante, pues no debería haber limitaciones a los usuarios (internos y/o externos) que deseen utilizar la data adecuadamente, solo de una entidad preautorizada, puesto que un ciberataque puede interrumpir los servicios afectando sus procesos. Según el mismo autor, lo más importante es que las organizaciones autorizadas tengan acceso a los datos, porque el mal uso de los datos puede revelar y crear problemas legales por su uso no autorizado. Resulta relevante tomar acciones para protegerse contra el acceso de personal no admitido y en cuanto a la dimensión integridad se encarga de garantizar que los datos no se modifiquen de cualquier manera mientras un usuario tenga acceso permitido y debe ser autentificado permanentemente. Todos los estudios presentados tienen como objetivo el SGSI, sobre el cual se basa la necesidad de la privacidad, medio y probidad de la información, donde estas tres dimensiones son el fundamento de la arquitectura de seguridad informática (Solano, 2020).

Protección de datos: 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. Su importancia radica en el hecho de que conforme el volumen de la data generada aumenta se hace muy necesario protegerla constantemente. Por lo tanto, como estrategia del cuidado de la data se deben asegurar que sea posible recuperarla en caso haya algún daño o pérdida, de tal manera que, éstos se encuentren disponibles todo el tiempo. Como se sabe, con la pandemia del coronavirus, muchos empleados hicieron teletrabajo o trabajo remoto, por lo cual, la necesidad de cuidar la data se hace imperante. En tal sentido, las organizaciones empresariales deben alinearse a las necesidades de proteger la información de sus colaboradores sin importar el lugar físico o residencia de los mismos, tampoco sin tomar en cuenta el dispositivo usado (móvil, portátil, de escritorio, etc.). El término “protección” se emplea para el uso de los respaldos de datos operativos, así como para garantizar el continuo funcionamiento del negocio y la puesta en

recuperación frente a desastres producidos. Las estrategias de cuidado de la data evolucionan de dos maneras: uso de data y administración de data. El uso de data permite que los usuarios cuenten con la misma data de negocio todo el tiempo, aun cuando éstos puedan dañarse o perderse (Hefner, y otros, 2020).

Norma internacional ISO 27002:2013: Estándar mundial que define pautas y directivas genéricas para dar inicio, crear, soportar y aplicar mejora continua a la seguridad informática de una empresa. Como objetivos se debe proveer pautas generales para la aceptación de los mismos. Con respecto a los objetivos de control de la norma, se tiene que se debe realizar un análisis de peligros potenciales. De esta manera, este estándar internacional puede ser una guía práctica de directrices seguras orientadas al desarrollo de políticas de seguridad organizacional y buenas prácticas de administración de la data fomentando libertad para la realización de acciones transparentes. Esta norma emplea dominios de seguridad, controles de seguridad y objetivos de control de forma anidad y jerárquica (ISO, 2013).

También, se tuvo un grupo de **enfoques conceptuales** para complementar la investigación como sigue:

Activo informático, se refiere a los recursos tecnológicos del entorno de la información de comunicación, que forman parte de las empresas y cuyo objeto es difundir información; son parte integral de la empresa y aseguran su continuidad o competitividad; protegerlos es crucial para que las claves y los datos de varios proyectos comerciales o personales permanezcan seguros; protéjase de posibles daños y cambios de datos (PJGROUP, 2020).

Control de seguridad, Conjunto de objetivos que garantizan el manejo seguro de los activos, métodos, bases, data y archivos vinculados a la aplicación de tecnologías informáticas a fin de estar cubiertos contra usos no admitidos, posibles peligros y usos inapropiados o ilegales y sean siempre funcionales, seguros y protegidos (AUDITOOL, 2022).

Datos sensibles: Se trata de datos personales que consisten en datos personales, como: datos biométricos que pueden identificar a una persona, como huellas dactilares, retina, iris, datos relacionados con la raza y el origen

étnico, ingresos financieros, opiniones o creencias políticas, religiosas, filosóficas o. datos morales; Membresía de la unión.

Delitos informáticos: Es toda actividad ofensiva e ilegal a través de canales informáticos que tenga como objetivo captar información privada, dañar equipos de cómputo, contaminar las redes de Internet, modificar sistemas, negar acceso, divulgar información personal, etc. (Condori, h. 2012).

En cuanto a la **metodología, marco de trabajo o norma internacional** para el desarrollo del modelo de seguridad informática, se eligió a la *norma internacional ISO/IEC 27002:2013.*

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

- **Tipo de investigación**

  Aplicada porque se fundamenta en el uso de métodos y técnicas ya probadas y estandarizadas aplicadas a la solución de una problemática empresarial.

- **Diseño de investigación**

  Preexperimental porque existe el manejo indirecto de la data muestral para fines de conveniencia práctica.

3.2. Variables y operacionalización

- **Variables**

  - **Variable independiente:** Modelo de seguridad informática

    - **Definición Conceptual:**

      "Conjunto de métricas adecuadas respecto a protección de activos informáticos a fin de evaluar la confidencialidad, integridad y usabilidad de la información" (Cano, 2018).

    - **Definición operacional:**

      Se puede medir a través de aspectos de directivas y actividades de seguridad informática en las organizaciones.

  - **Variable dependiente:** Protección de datos

    - **Definición Conceptual:**

      "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).

- **Definición operacional:**

  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.

- **Operacionalización**

Se ha elaborar una matriz de operacionalización en el Anexo 2 con la finalidad de mostrar detalladamente el uso de las dos variables de estudio, sus dimensiones e indicadores respectivos.

3.3. Población, muestra y muestreo:

- **Población (N)**

Conformada por el personal que presta servicios en la municipalidad. Se tiene:

Tabla 1. *Población*

Cargo / Puesto	Cantidad
Gerente municipal	1
Subgerente de área	7
Operario	10
Total	18

Fuente: (Elaboración propia, 2022)

$$N = 18\, personas$$

- **Muestra (n)**

En vista que la población no es superior a 30, se puede concluir que, la muestra posee la misma cantidad de elementos que la población como sigue:

$$n = N = 18\, personas$$

- **Muestreo**

No probabilístico puesto que no se recurrió a la aleatoriedad en el manejo de la muestra obtenida de la población.

3.4. Técnicas e instrumentos de recolección de datos:

- **Técnicas:**
  - Encuesta.
  - Análisis documentario.

- **Instrumentos:**
  - Cuestionario (Encuesta).
  - Tarjeta de datos (Análisis documentario).

- **Validez y confiabilidad:**

Para determinar la validez del cuestionario se recurrió a la evaluación de tres expertos de amplia trayectoria como se puede constatar en el Anexo 4.

Para determinar la confiabilidad, se aplicó el coeficiente Alfa de Cronbach en el programa aplicativo SPSS v26 como se puede constatar en el Anexo 6.

Tabla 2. *Confiabilidad del instrumento "Cuestionario"*

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,714	12

Fuente: (Elaboración propia, 2022)

3.5. Procedimientos

Este estudio incorpora la realización de tres (3) objetivos específicos, cuyo desarrollo y ejecución implicó las siguientes actividades como sigue:

- Objetivo específico 1: Mejorar la prevención de la divulgación no autorizada de la información

  Se hizo necesario realizar la recopilación de la data que correspondía al manejo de la confidencialidad de la información de la municipalidad solicitando el permiso respectivo y aplicando la técnica de la Encuesta, específicamente empleando como instrumento de recolección a un Cuestionario personalizado conteniendo cuatro (4) preguntas o ítems, el cual se puede observar detalladamente en el Anexo 3.

- Objetivo específico 2: Mejorar la prevención de la modificación no autorizada de la información

  Se hizo necesario realizar la recopilación de la data que correspondía al manejo de la integridad de la información de la municipalidad solicitando el permiso respectivo y aplicando la técnica de la Encuesta, específicamente empleando como instrumento de recolección a un Cuestionario personalizado conteniendo cuatro (4) preguntas o ítems, el cual se puede observar detalladamente en el Anexo 3.

- Objetivo específico 3: Mejorar la prevención de la interrupción no autorizada de la información

  Se hizo necesario realizar la recopilación de la data que correspondía al manejo de la confidencialidad de la información de la municipalidad solicitando el permiso respectivo y aplicando la técnica de la Encuesta, específicamente empleando como instrumento de recolección a un Cuestionario personalizado conteniendo cuatro (4) preguntas o ítems, el cual se puede observar detalladamente en el Anexo 3.

3.6. Método de análisis de datos

Para el procesamiento estadístico de la data recopilada, se recurrió a métodos basados en la aplicación de la estadística descriptiva y de la estadística inferencial.

La estadística descriptiva estuvo orientada a mostrar gráfica y tubularmente la situación anterior y posterior luego de la aplicación de la solución propuesta.

La estadística inferencial estuvo orientada a mostrar gráfica y tubularmente la prueba de normalidad para cada indicador empleado según los objetivos específicos trazados.

Finalmente, se empleó el método deductivo porque es lo más común cuando se realiza una investigación cuantitativa, dado que se origina de generalidades y termina en particularidades.

3.7. Aspectos éticos:

La parte ética en la presente investigación estuvo dada por los siguientes elementos:

La generación de la declaración de autoría, que evidencia que los autores reconocen el desarrollo de la investigación como una creación suya o propia.

La generación de la declaración de originalidad, que evidencia que el asesor refrenda la aceptación de que la investigación es original y pertenece a los autores.

La generación del reporte de similitud mediante el uso del sistema Turnitin, que evidencia el empleo de un software anti plagio para garantizar la originalidad del mismo.

El correcto uso del estándar internacional ISO-690 que permita el registro de las fuentes bibliográficas siguiendo un estándar mundialmente aceptado sobre todo a nivel de ingeniería.

IV. RESULTADOS

- **Análisis descriptivo**
  - Indicador 1: “Prevención de la divulgación no autorizada”

Tabla 3. *Análisis descriptivo - Indicador “Prevención de la divulgación no autorizada”*

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
PDNA-Preprueba	4	1,38	1,75	1,5100	,16603
PDNA-Posprueba	4	4,25	5,00	4,7729	,33767
N válido (por lista)	4				

Fuente: (Elaboración propia, 2022)

Al examinar la Tabla 3, se evidencia que la prevención de la divulgación no autorizada en la preprueba a la propuesta de un modelo de seguridad informática tenía un promedio de 1.51 puntos y en la posprueba a la propuesta de un modelo de seguridad informática tiene un promedio de 4.77 puntos, dando lugar a un incremento de 3.26 puntos (aumento de 69.40%). Existe una mejora de la prevención de la divulgación no autorizada después de la propuesta de un modelo de seguridad informática, así como lo ilustra la siguiente imagen.

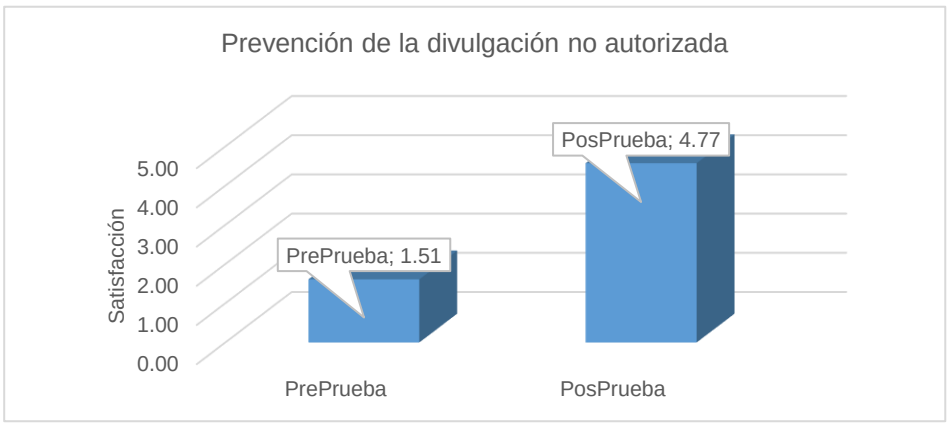

Figura 1. Medias de preprueba y posprueba del indicador 1.

- Indicador 2: “Prevención de la modificación no autorizada”

Tabla 4. Análisis descriptivo - Indicador “Prevención de la modificación no autorizada”

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
PMNA-Preprueba	4	1,38	1,75	1,6650	,19777
PMNA-Posprueba	4	4,38	5,00	4,8600	,23652
N válido (por lista)	4				

Fuente: (Elaboración propia, 2022)

Al examinar la Tabla 4, se evidencia que la prevención de la modificación no autorizada en la preprueba a la propuesta de un modelo de seguridad informática tenía un promedio de 1.67 puntos y en la posprueba a la propuesta de un modelo de seguridad informática tiene un promedio de 4.86 puntos, dando lugar a un incremento de 3.19 puntos (aumento de 65.20%). Existe una mejora de la prevención de la modificación no autorizada después de la propuesta de un modelo de seguridad informática, así como lo ilustra la siguiente imagen.

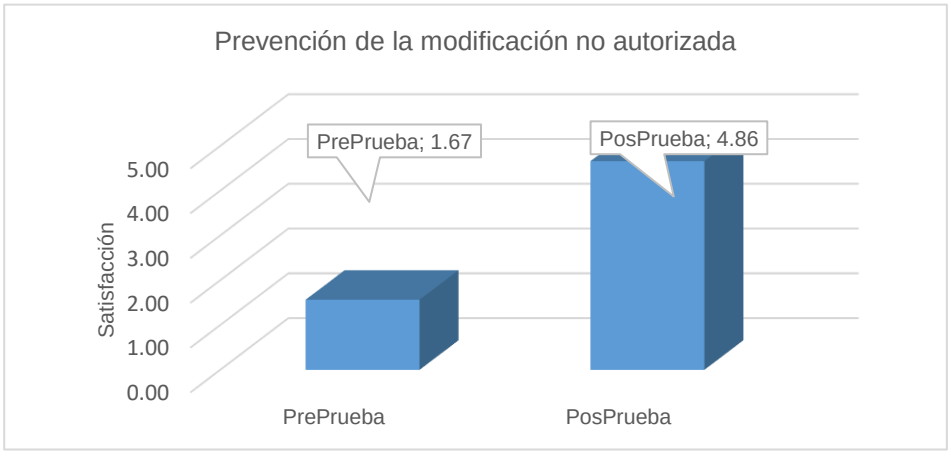

Figura 2. Medias de preprueba y posprueba del indicador 2.

- Indicador 3: “Prevención de la interrupción no autorizada”

Tabla 5. Análisis descriptivo - Indicador “Prevención de la interrupción no autorizada”

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desv. Desviación
PINA-Preprueba	4	1,25	1,88	1,6020	,23520
PINA-Posprueba	4	4,63	5,00	4,9280	,16069
N válido (por lista)	4				

Fuente: (Elaboración propia, 2022)

Al examinar la Tabla 5, se evidencia que la prevención de la interrupción no autorizada en la preprueba a la propuesta de un modelo de seguridad informática tenía un promedio de 1.60 puntos y en la posprueba a la propuesta de un modelo de seguridad informática tiene un promedio de 4.93 puntos, dando lugar a un incremento de 3.23 puntos (aumento de 67.30%). Existe una mejora de la prevención de la interrupción no autorizada después de la propuesta de un modelo de seguridad informática, así como lo ilustra la siguiente imagen.

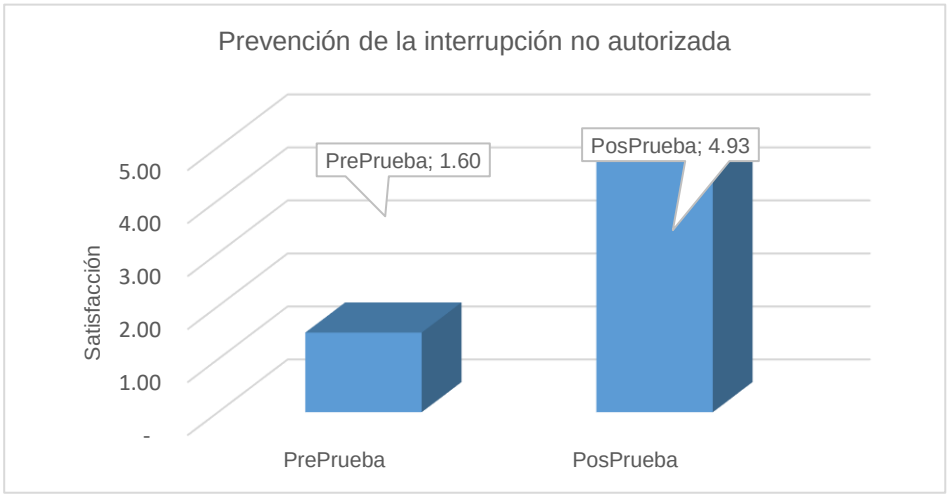

Figura 3. Medias de preprueba y posprueba del indicador 3.

- **Análisis inferencial**

Debido a que la muestra poblacional de los tres (3) indicadores fueron menores que cincuenta (50), entonces se optó por la aplicación de la prueba estadística de Shapiro-Wilk para establecer la normalización de cada indicador y su respectiva muestra.

- Indicador 1: “Prevención de la divulgación no autorizada”

Se genera las hipótesis de normalización y se establece el valor de significancia a 0.05.

H_0: “La prevención de la divulgación no autorizada (sin la propuesta del modelo de seguridad informática) si tiene distribución normal”.

H_1: “La prevención de la divulgación no autorizada (sin la propuesta del modelo de seguridad informática) no tiene distribución normal”.

H_0: “La prevención de la divulgación no autorizada (con la propuesta del modelo de seguridad informática) no tiene distribución normal”.

H_1: “La prevención de la divulgación no autorizada (con la propuesta del modelo de seguridad informática) si tiene distribución normal”.

Para todos los casos anteriormente expuestos, se establece el valor de significancia: $\alpha = 0.05$

Sig. > 0.05, se admite la hipótesis nula (H_0)

Sig. <= 0.05, se admite la hipótesis alterna (H_1)

Tabla 6. *Prueba de normalidad del indicador "Prevención de la divulgación no autorizada"*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PDNA-Preprueba	,866	12	,202
PDNA-Posprueba	,866	12	,200

Fuente: (Elaboración Propia, 2022)

En la Tabla 6**,** se observa que el nivel de significancia para la Preprueba es de 0.202, el cual es mayor a 0.05; por lo tanto, se acepta la primera hipótesis nula que determina que se tiene una distribución normal; por otro lado, se observa que el nivel de significancia en Posprueba es de 0.200, el cual es mayor a 0.05; por lo tanto, se acepta la segunda hipótesis alterna que determina que se tiene una distribución normal. De este modo, se aplicará la prueba T-Student.

- Indicador 2: “Prevención de la modificación no autorizada”

Se genera las hipótesis de normalización y se establece el valor de significancia a 0.05.

H_0: “La prevención de la modificación no autorizada (sin la propuesta del modelo de seguridad informática) si tiene distribución normal”.

H_1: “La prevención de la modificación no autorizada (sin la propuesta del modelo de seguridad informática) no tiene distribución normal”.

H_0: “La prevención de la modificación no autorizada (con la propuesta del modelo de seguridad informática) no tiene distribución normal”.

H_1: “La prevención de la modificación no autorizada (con la propuesta del modelo de seguridad informática) si tiene distribución normal”.

Para todos los casos anteriormente expuestos, se establece el valor de significancia: $\alpha = 0.05$

Sig. > 0.05, se admite la hipótesis nula (H_0)

Sig. <= 0.05, se admite la hipótesis alterna (H_1)

Tabla 7. *Prueba de normalidad del indicador “Prevención de la modificación no autorizada”*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PMNA-Preprueba	,846	12	,203
PMNA-Posprueba	,846	12	,201

Fuente: (Elaboración Propia, 2022)

En la Tabla 7**,** se observa que el nivel de significancia para la Preprueba es de 0.203, el cual es mayor a 0.05; por lo tanto, se acepta la primera hipótesis nula que determina que se tiene una distribución normal; por otro lado, se observa que el nivel de significancia en Posprueba es de 0.201, el cual es mayor a 0.05; por lo tanto, se acepta la segunda hipótesis alterna que determina que se tiene una distribución normal. De este modo, se aplicará la prueba T-Student.

- Indicador 3: “Prevención de la interrupción no autorizada”

Se genera las hipótesis de normalización y se establece el valor de significancia a 0.05.

H_0: “La prevención de la interrupción no autorizada (sin la propuesta del modelo de seguridad informática) si tiene distribución normal”.

H_1: “La prevención de la interrupción no autorizada (sin la propuesta del modelo de seguridad informática) no tiene distribución normal”.

H_0: “La prevención de la interrupción no autorizada (con la propuesta del modelo de seguridad informática) no tiene distribución normal”.

H_1: “La prevención de la interrupción no autorizada (con la propuesta del modelo de seguridad informática) si tiene distribución normal”.

Para todos los casos anteriormente expuestos, se establece el valor de significancia: $\alpha = 0.05$

Sig. > 0.05, se admite la hipótesis nula (H_0)

Sig. <= 0.05, se admite la hipótesis alterna (H_1)

Tabla 8. *Prueba de normalidad del indicador “Prevención de la interrupción no autorizada”*

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PINA-Preprueba	,856	12	,204
PINA-Posprueba	,856	12	,210

Fuente: (Elaboración Propia, 2022)

En la Tabla 8**,** se observa que el nivel de significancia para la Preprueba es de 0.204, el cual es mayor a 0.05; por lo tanto, se acepta la primera hipótesis nula que determina que se tiene una distribución normal; por otro lado, se observa que el nivel de significancia en Posprueba es de 0.210, el cual es mayor a 0.05; por lo tanto, se acepta la segunda hipótesis alterna que determina que se tiene una distribución normal. De este modo, se aplicará la prueba T-Student.

- **Contrastación de hipótesis**

Para las muestras que siguen una distribución normalizada, se aplica la prueba paramétrica T-Student.

A continuación, se presenta el contraste de las hipótesis específicas:

- Hipótesis específica 1:

"La propuesta de un modelo de seguridad informática mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

Se generan las hipótesis nula y alternativa, estableciendo el valor de significancia a 0.05.

Hipótesis estadísticas:

H_0: "La propuesta de un modelo de seguridad informática no mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

H_0: PDNAa >= PDNAp

H_1: "La propuesta de un modelo de seguridad informática si mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

H_1: PDNAa < PDNAp

Valor de significancia: $\alpha = 0.05$.

Sig. > 0.05, se admite la hipótesis nula (H_0)

Sig. <= 0.05, se admite la hipótesis alterna (H_1)

Tabla 9. Prueba t-Student para la prevención de la divulgación no autorizada

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
PDNA_Preprueba PDNA_Posprueba	-3,2966	,23888	,09544	-3,54686	-3,08647	-35,087	12	,000

Fuente: (Elaboración propia, 2022)

El T calculado está ubicado en la zona de rechazo, por lo que, se concluye que: “La propuesta de un modelo de seguridad informática mejora de forma significativa la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022”.

- Hipótesis específica 2:

  "La propuesta de un modelo de seguridad informática mejora la prevención de la modificación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

  Se generan las hipótesis nula y alternativa, estableciendo el valor de significancia a 0.05.

  Hipótesis estadísticas:

  H_0: "La propuesta de un modelo de seguridad informática no mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

  H_0: PMNAa >= PMNAp

  H_1: "La propuesta de un modelo de seguridad informática si mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

  H_1: PMNAa < PMNAp

  Valor de significancia: α = 0.05.

  Sig. > 0.05, se admite la hipótesis nula (H_0)

  Sig. <= 0.05, se admite la hipótesis alterna (H_1)

Tabla 10. *Prueba t-Student para la prevención de la modificación no autorizada*

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
PMNA_Preprueba PMNA_Posprueba	-3,1966	,22888	,08544	-3,44686	-3,01647	-33,287	12	,000

Fuente: (Elaboración propia, 2022)

El T calculado está ubicado en la zona de rechazo, por lo que, se concluye que: “La propuesta de un modelo de seguridad informática mejora de forma significativa la prevención de la modificación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022”

- Hipótesis específica 3:

"La propuesta de un modelo de seguridad informática mejora la prevención de la interrupción no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

Se generan las hipótesis nula y alternativa, estableciendo el valor de significancia a 0.05.

Hipótesis estadísticas:

H_0: "La propuesta de un modelo de seguridad informática no mejora la prevención de la interrupción no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

H_0: PINAa >= PINAp

H_1: "La propuesta de un modelo de seguridad informática no mejora la prevención de la interrupción no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".

H_1: PINAa < PINAp

Valor de significancia: α = 0.05.

Sig. > 0.05, se admite la hipótesis nula (H_0)

Sig. <= 0.05, se admite la hipótesis alterna (H_1)

Tabla 11. *Prueba t-Student para la prevención de la interrupción no autorizada*

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia				
				Inferior	Superior			
PINA_Preprueba PINA_Posprueba	-3,2766	,24666	,08355	-3,62586	-3,06597	-31,547	12	,000

Fuente: (Elaboración propia, 2022)

El T calculado está ubicado en la zona de rechazo, por lo que, se concluye que: “La propuesta de un modelo de seguridad informática mejora de forma significativa la prevención de la interrupción no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022”.

V. DISCUSIÓN

Para el indicador 1 “Prevención de la divulgación no autorizada”, se obtuvo antes y después de la propuesta de un modelo de seguridad informática valores de 1.51 a 4.77 puntos, lo cual significó un incremento de 3.26 puntos (aumento de 69.40%). Estos resultados son equiparables a los obtenidos por (Arias, y otros, 2019) quienes en su investigación tuvo como objetivo informar y orientar al lector según buenas prácticas de seguridad para una información veraz; las mismas necesidades surgieron con el tiempo, y de esto surgió un conjunto de instrucciones que bien soportan el sistema de administración de seguridad informática. Del mismo modo, son equiparables por Hidalgo (2017) quien en su investigación tuvo como objetivo generar un modelo de administración de seguridad informática para proteger y certificar la data técnica de las instituciones. Lo anterior, se sustenta en la teoría del modelo de seguridad informática, que establece un conjunto de métricas adecuadas respecto a protección de activos informáticos a fin de evaluar la confidencialidad, integridad y usabilidad de la información, porque este es el modelo de gestión que toda organización desea implementar (Cano, 2018).

Para el indicador 2 “Prevención de la modificación no autorizada”, se obtuvo antes y después de la propuesta de un modelo de seguridad informática valores de 1.67 a 4.86 puntos, lo cual significó un incremento de 3.19 puntos (aumento de 65.20%). Estos resultados son equiparables a los obtenidos por (Yañez, 2017) quien en su investigación tuvo como objetivo gestionar, supervisar, compilar y favorecer continuamente la seguridad informática. Del mismo modo, son equiparables por con los resultados por Romo y Valarezo (2016) quienes en su investigación intentaron informar y orientar al interesado en las mejores recomendaciones de seguridad informática; la misma que ha surgido con el tiempo, y todos los fraudes derivados de filtraciones, impresas o no. Lo anterior, se sustenta en la teoría del modelo de seguridad informática que establece que, en cuanto a la usabilidad es resulta relevante, pues no debería haber limitaciones a los usuarios (internos y/o externos) que deseen utilizar la data adecuadamente, solo de una entidad preautorizada, puesto que un ciberataque puede interrumpir los servicios afectando sus procesos (Solano, 2020).

Para el indicador 3 “Prevención de la interrupción no autorizada”, se obtuvo antes y después de la propuesta de un modelo de seguridad informática valores de 1.60 a 4.93 puntos, lo cual significó un incremento de 3.23 puntos (aumento de 67.30%). Estos resultados son equiparables a los obtenidos por (Ticona, 2022) quien en su investigación tuvo como objetivo establecer el impacto de un modelo de seguridad informática empleando el estándar mundial ISO/IEC 27001:2013 orientado a disminuir los inconvenientes que presentaban los activos informáticos de una empresa particular. Del mismo modo, son equiparables por (Aguinaga, 2021) en su investigación tuvo como objetivo establecer un método de administración basado en el estándar mundial ISO/IEC 27001:2013 para establecer el impacto en la protección informática de la entidad financiera. Lo anterior, se sustenta en la teoría del modelo de seguridad informática, cuyo principio de disponibilidad sostiene que el acceso a la información debería estar a la orden del día en un horario 24 x 7 (Hefner, y otros, 2020).

VI. CONCLUSIONES

1. Se logró mejorar la prevención de la divulgación no autorizada de la información en la municipalidad, obteniéndose un incremento de 3.26 puntos (aumento de 69.40%). Se inicia con una preprueba promedio de 1.51 puntos y finaliza con una posprueba promedio de 4.77 puntos luego de la propuesta de un modelo de seguridad informática en la municipalidad.

2. Se logró mejorar la prevención de la modificación no autorizada de la información en la municipalidad, obteniéndose un incremento de 3.19 puntos (aumento de 65.20%). Se inicia con una preprueba promedio de 1.67 puntos y se finaliza con una posprueba promedio de 4.86 puntos luego de la propuesta de un modelo de seguridad informática en la municipalidad.

3. Se logró mejorar la prevención de la interrupción no autorizada de la información en la municipalidad, obteniéndose un incremento de 3.23 puntos (aumento de 67.30%). Se inicia con una preprueba promedio de 1.60 puntos y se finaliza con una posprueba promedio de 4.93 puntos luego de la propuesta de un modelo de seguridad informática en la municipalidad.

VII. RECOMENDACIONES

Al Gerente municipal:

Se recomienda la aplicación y ejecución de la solución planteada en esta investigación (modelo de seguridad informática) mediante el uso de una plataforma tecnológica adecuada para la protección de datos de la municipalidad.

Al Jefe de Informática:

Se recomienda implementar un sistema de monitoreo de red para la municipalidad a fin de proteger los activos informáticos.

Al Jefe de recursos humanos:

Se recomienda desarrollar capacitaciones técnicas sobre seguridad informática al personal administrativo de la municipalidad.

A los trabajadores:

Se recomienda tomar en cuenta los consejos de expertos profesionales que brindan buenas prácticas basadas en la norma internacional ISO/IEC 27002:2013 para cuidar y asegurar la protección de sus datos e información.

REFERENCIAS

Alarcón, Mitchell, y otros. 2020. "*Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana".* 2020, Propósitos y Representaciones, págs. 1-11.

Aguinaga, William. 2021. *"Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021".* Lima : UCV, 2021.

Alvarado, Francisco. 2016. *La gestión de la Seguridad de la Información en el régimen peruano de Protección de Datos Personales.* Lima : PUCP, 2016.

Arias, Mauricio y Botero, Ricardo. 2019. *Estado de la norma técnica de seguridad ISO27002 como soporte para la norma ISO27001 en una empresa de telecomunicaciones de la ciudad de Medellín.* Medellín : TDEA, 2019.

AUDITOOL. 2022. [En línea] 10 de Febrero de 2022. [Citado el: 16 de Mayo de 2022.] https://www.auditool.org/blog/auditoria-de-ti/8317-que-son-los-controles-de-seguridad-de-ti.

Ayala, Ángel. 2017. *"Sistema de gestión de seguridad de información para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017".* Lima : UCV, 2017.

Cahuana, César y Cahuana, Elin. 2021. *"Sistema web basado en la ISO/IEC 27001 para la gestión de la información en la Empresa P.A Perú S.A.C.".* Lima : UCV, 2021.

CEPAL. 2020. Gestión de datos de investigación. [En línea] 18 de Diciembre de 2020. [Citado el: 15 de Mayo de 2022.] https://biblioguias.cepal.org/c.php?g=495473&p=4398118.

Chavarry, Francisco. 2021. *"Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en Secretaría Ejecutiva de Policía Nacional del Perú".* Lima : UCV, 2021.

Chuna, Luciano. 2018. *"Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - Piura".* Piura : UCV, 2018.

Cruz, Jesús y Huamaní, Miguel. 2019. *"Automatización de la seguridad de la información basado en la norma técnica peruana ISO 27001 en la empresa ZEPPELIN INVERSIONES GENERALES S.R.L".* Lima : UCV, 2019.

ESIC. 2018. Tipos de seguridad informática, ¿cuáles existen? [En línea] 1 de Septiembre de 2018. [Citado el: 15 de Mayo de 2022.] https://www.esic.edu/rethink/tecnologia/tipos-de-seguridad-informatica-cuales-existen.

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..

Hidalgo, Vinicio. 2017. *"Diseño de modelo de gestión para el gerenciamiento de la seguridad de la información tecnológica en el Consejo de la Judicatura" – planta central Quito".* Quito : EPG-UQ, 2017.

ISO. 2013. ISO/IEC 27002:2013. *Information technology - Security techniques - Code of practice for information security controls.* [En línea] 1 de Octubre de 2013. [Citado el: 28 de Mayo de 2022.] https://www.iso.org/standard/54533.html.

Maldonado, Efraín. 2016. *"Norma ISO 27001 para la seguridad de información del área de Registros Académicos del colegio Nuestra Señora del Carmen".* Lima : UCV, 2016.

Maquera, Henry y Serpa, Paola. 2017. *Gestión de Activos basados en ISO/IEC 27002 para garantizar Seguridad de la información.* Tacna : UNJBG, 2017.

MDP. 2018. *Plan Estratégico 2018-2022.* Huanúco : MDP, 2018.

MINTIC. 2016. "Modelo de Seguridad y Privacidad de la Información". [En línea] 29 de Julio de 2016. [Citado el: 20 de Mayo de 2022.] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf.

Pérez, Andrea. 2015. *"Diseño de un modelo de los controles necesarios asociados a la gestión de activos, bajo el cumplimiento de la norma ISO/IEC 27002 anexo A, en una entidad bancaria".* Bogotá : UCC, 2015.

PJGROUP. 2020. [En línea] 1 de Enero de 2020. [Citado el: 16 de Mayo de 2022.] https://peritojudicial.com/activos-informaticos/#:~:text=1.-,Qu%C3%A9%20son%20los%20activos%20inform%C3%A1ticos,ejemplo%20de%20hardware%20y%20software..

Poicon, Ángel y Ramírez, Óscar. 2020. *"Propuesta de un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Marcavelica, mediante la NTP- ISO/IEC 27001:2014".* Piura : UCV, 2020.

PowerData. 2020. Seguridad de datos: En qué consiste y qué es importante en tu empresa. [En línea] 1 de Enero1 de 2020. [Citado el: 15 de Mayo de 2022.] https://www.powerdata.es/seguridad-de-datos.

Risco, Giap. 2021. *"Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín,2021".* Lima : UCV, 2021.

Rojas, Clemente. 2019. *"Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC".* Lima : UCV, 2019.

Romo, Daniel y Valarezo, Joffre. 2016. *Analisis e Implementación de la Norma ISO 27002 para el Departamento de Sistemas de la Universidad Politécnica Salesiana de la ciudad de Guayaquil.* Guayaquil : UPS, 2016.

Salsavilca, Carlos. 2017. *"Implementación de la norma ISO 27001 en la Gestión de la Seguridad de la Información en la empresa Atento del Perú 2017".* Lima : UCV, 2017.

Ticona, Raúl. 2022. *"Modelo de seguridad de la información basado en la normativa ISO/IEC 27001:2013 para mitigar los riesgos de los activos de la información en la entidad privada Severox Perú SAC, Arequipa, 2021".* Arequipa : UCV, 2022.

Yañez, Alejandro. 2017. *"Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño".* Santiago de Chile : UCH, 2017.

Zapata, Stefany. 2021. *"Análisis de factores críticos de éxito para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la empresa Inversiones Prisco S.A.C – Sechura".* Piura : UCV, 2021.

ANEXOS

Anexo 1 - Matriz de consistencia de la investigación

Título: Propuesta de un modelo de seguridad informática para la Protección de datos en la Municipalidad Distrital de Pinra, Huánuco 2022

Autora: Sánchez Campos, Krystel Elena

Problema	Objetivo	Hipótesis	Variable	Dimensión	Indicador	Instrumento
General: ¿De qué modo la propuesta de un modelo de seguridad informática influye en la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022?	General: Mejorar la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022 mediante la propuesta de un modelo de seguridad informática.	General: "La propuesta de un modelo de seguridad informática mejora significativamente la protección de datos de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".	Independiente: Modelo de seguridad informática			
Específicos: 1. ¿De qué modo la propuesta de un modelo de seguridad informática influye en la prevención de la divulgación no autorizada de la información de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022? 2. ¿De qué modo la propuesta de un	Específicos: 1. Mejorar la prevención de la divulgación no autorizada de la información. 2. Mejorar la prevención de la modificación no autorizada de la información. 3. Mejorar la prevención de la interrupción no autorizada de la información.	Específicas: 1. "La propuesta de un modelo de seguridad informática mejora la prevención de la divulgación no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022". 2. "La propuesta de un modelo de seguridad informática mejora la prevención de la modificación no autorizada de la	Dependiente: Protección de datos	Confidencialidad	Prevención de la divulgación no autorizada	Cuestionario
				Integridad	Prevención de la modificación no autorizada	Cuestionario

modelo de seguridad informática influye en la prevención de la modificación no autorizada de la información de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022? 3. ¿De qué modo la propuesta de un modelo de seguridad informática influye en la prevención de la interrupción no autorizada de la información de la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022?		información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022". 3. "La propuesta de un modelo de seguridad informática mejora prevención de la interrupción no autorizada de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el año 2022".		Disponibilidad	Prevención de la interrupción no autorizada	Cuestionario

Anexo 2 - Matriz de operacionalización de variables

Variable	Definición Conceptual	Definición Operacional	Dimensión (Sub variable)	Indicador	Escala de medición
Independiente: Modelo de seguridad informática	“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: Protección de datos	“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 - Instrumentos de recolección de datos

Cuestionario aplicado a los operarios de la Municipalidad Distrital de Pinra

A continuación, se presenta una lista de preguntas contenidas en doce (12) ítems que corresponden a su percepción sobre la protección de datos en la municipalidad. 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. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?					
		2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?					
		3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?					
		4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?					
	Integridad	5. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?					
		6. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?					
		7. ¿Qué opina Usted sobre el manejo de copias de seguridad?					
		8. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?					
	Disponibilidad	9. ¿Qué opina Usted sobre la gestión de seguridad en redes?					
		10. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?					
		11. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?					
		12. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?					

Anexo 4 - Validación de los instrumentos de recolección de datos

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
Dimensión 2: Integridad							
5. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
6. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
8. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
Dimensión 3: Disponibilidad							
9. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
10. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
11. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
12. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	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	Tecnologías de la información

DNI: 18161457 Trujillo, 18 de mayo del 2022

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
Dimensión 2: Integridad							
5. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
6. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
8. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
Dimensión 3: Disponibilidad							
9. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
10. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
11. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
12. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	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

Hoja de validación del instrumento

I. Instrumento:

Cuestionario

II. Indicaciones:

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

Dimensiones	Claridad[1]		Pertinencia[2]		Relevancia[3]		Sugerencias
	Sí	No	Sí	No	Sí	No	
Dimensión 1: Confidencialidad							
1. ¿Qué opina Usted sobre el cumplimiento de los requisitos de negocio para el control de accesos?	x		x		x		
2. ¿Qué opina Usted sobre la gestión adecuada de acceso de los usuarios?	x		x		x		
3. ¿Qué opina Usted sobre el manejo responsable de la información de los usuarios?	x		x		x		
4. ¿Qué opina Usted sobre el control de acceso conveniente a los sistemas y aplicaciones?	x		x		x		
Dimensión 2: Integridad							
5. ¿Qué opina Usted sobre las responsabilidades y procedimientos de operación?	x		x		x		
6. ¿Qué opina Usted sobre la protección conveniente contra código malicioso?	x		x		x		
7. ¿Qué opina Usted sobre el manejo de copias de seguridad?	x		x		x		
8. ¿Qué opina Usted sobre el registro adecuado de actividad y supervisión de los sucesos?	x		x		x		
Dimensión 3: Disponibilidad							
9. ¿Qué opina Usted sobre la gestión de seguridad en redes?	x		x		x		
10. ¿Qué opina Usted sobre el intercambio seguro de información con partes externas?	x		x		x		
11. ¿Qué opina Usted sobre los requisitos de seguridad de los sistemas de información?	x		x		x		
12. ¿Qué opina Usted sobre la seguridad en los procesos de desarrollo y soporte?	x		x		x		

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

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

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

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

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

Anexo 5 - Tabla de datos

Data preprueba

	Confidencialidad				Integridad				Disponibilidad			
	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9	Ítem 10	Ítem 11	Ítem 12
Persona 1	1	2	1	2	2	1	2	1	1	2	1	1
Persona 2	2	2	1	2	2	1	1	2	2	2	1	1
Persona 3	2	1	2	1	1	2	1	2	1	2	2	2
Persona 4	1	2	2	2	2	1	2	2	2	2	2	1
Persona 5	1	2	1	2	2	1	1	2	1	2	1	1
Persona 6	2	2	1	2	2	1	2	2	2	2	1	1
Persona 7	2	2	1	2	2	2	1	1	2	2	1	1
Persona 8	2	1	2	1	1	2	1	2	1	1	2	2
Persona 9	2	2	1	2	2	1	1	2	2	2	1	1
Persona 10	2	1	2	1	1	2	1	2	1	2	2	2
Persona 11	1	2	2	2	2	1	2	2	2	2	2	1
Persona 12	1	2	1	2	2	1	1	2	1	2	1	1
Persona 13	2	2	1	2	2	1	2	2	2	2	1	1
Persona 14	2	2	1	2	2	2	1	1	2	2	1	1
Persona 15	2	1	2	1	1	2	1	2	1	1	2	2
Persona 16	1	2	1	2	2	1	2	1	1	2	1	1
Persona 17	2	2	1	2	2	1	1	2	2	2	1	1
Persona 18	2	1	2	1	1	2	1	2	1	2	2	2
Promedio	1.63	1.75	1.38	1.75	1.75	1.38	1.38	1.75	1.50	1.88	1.38	1.25

Data posprueba

	Confidencialidad				Integridad				Disponibilidad			
	Ítem 1	Ítem 2	Ítem 3	Ítem 4	Ítem 5	Ítem 6	Ítem 7	Ítem 8	Ítem 9	Ítem 10	Ítem 11	Ítem 12
Persona 1	4	5	5	4	5	5	5	5	5	5	5	5
Persona 2	5	5	5	4	4	4	4	5	4	5	5	4
Persona 3	4	4	5	5	4	5	5	5	4	4	5	4
Persona 4	4	4	5	4	5	4	5	5	5	4	5	5
Persona 5	4	5	5	4	4	5	4	5	4	5	5	4
Persona 6	4	5	5	4	5	5	5	5	5	5	5	5
Persona 7	4	4	5	5	4	5	5	5	5	5	5	5
Persona 8	5	5	5	4	4	4	4	5	5	5	5	5
Persona 9	4	5	5	4	5	5	5	5	5	5	5	5
Persona 10	5	5	5	4	4	4	4	5	4	5	5	4
Persona 11	4	4	5	5	4	5	5	5	4	4	5	4
Persona 12	4	4	5	4	5	4	5	5	5	4	5	5
Persona 13	4	5	5	4	4	5	4	5	4	5	5	4
Persona 14	4	5	5	4	5	5	5	5	5	5	5	5
Persona 15	4	4	5	5	4	5	5	5	5	5	5	5
Persona 16	5	5	5	4	4	4	4	5	5	5	5	5
Persona 17	4	5	5	4	5	5	5	5	5	5	5	5
Persona 18	5	5	5	4	4	4	4	5	4	5	5	4
Promedio	4.25	4.63	5.00	4.25	4.38	4.63	4.63	5.00	4.63	4.75	5.00	4.63

Anexo 6 - 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
,714	12

Anexo 7 - Solución tecnológica propuesta

MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA INTERNACIONAL ISO/IEC 27002:2013

Hoy en día la seguridad informática se ha convertido en el activo más importante para las empresas y, por ende, hay que tener en cuenta que las vulnerabilidades aumentan y los ciberataques son más frecuentes debido a ello es que en la actualidad existen varias formas de salvaguardar la información.

Una característica importante en las organizaciones actuales es mejorar el nivel de seguridad de la información que manejan; por lo tanto, toda organización hace uso de elementos como hardware, software y personas que son los activos de la información. Una característica deseable es contar con un modelo de seguridad informática para lograr la seguridad de la información.

Asimismo, un modelo de seguridad informática representa un esquema para especificar y hacer cumplir las políticas de seguridad. Un modelo de seguridad puede basarse en un modelo formal de derechos de acceso, un modelo de computación, un modelo de computación distribuida o ninguna base teórica particular. Un modelo de seguridad informática se implementa a través de una política de seguridad informática.

De esta forma, los activos de cada organización o empresa están vulnerables a cualquier ataque informático, modificaciones, fraudes y robos de información. Por ello, se propuso realizar un Modelo seguridad informática aplicando la Norma internacional ISO/IEC 27002:2013 para proteger los activos de la información en la Municipalidad Distrital de Pinra de la ciudad de Huánuco en el presente año 2022, con la finalidad de garantizar una mejor protección a la entidad municipal asegurando la integridad, confidencialidad y disponibilidad de la misma.

El modelo de seguridad informática se basa en el modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información (MINTIC, 2016).

Se tiene:

Figura. Fase del modelo de seguridad informática

- Fase 1: Diagnóstico

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del modelo de seguridad informática.

En la fase, se pretende alcanzar las siguientes metas:

- ✓ Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad municipal.
- ✓ Identificar el nivel de cumplimiento con la normatividad de seguridad vigente relacionada con protección de datos.
- ✓ Identificación del uso de buenas prácticas en seguridad informática.

Para ello se recomienda utilizar los siguientes instrumentos:

- ✓ Herramienta de diagnóstico.
- ✓ Pruebas de seguridad de la información.

Para realizar esta fase la entidad municipal debe efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y las pruebas de seguridad de la información. Una vez se tenga el resultado del diagnóstico se procede al desarrollo de la fase de Planificación.

- Fase 2: Planificación

Para el desarrollo de esta fase, la entidad municipal debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad de seguridad informática alineado con el objetivo misional de la entidad municipal, con el propósito de definir las acciones a implementar a nivel de seguridad informática.

El alcance del modelo de seguridad informática permite a la entidad municipal definir los límites sobre los cuales se implementará la seguridad y privacidad en la misma. Este enfoque es por procesos y debe extenderse a toda la organización.

Para desarrollar el alcance y los límites del modelo se debe tener en cuenta las siguientes recomendaciones:

- ✓ Procesos que impactan directamente la consecución de objetivos misionales.
- ✓ Servicios y sistemas de información
- ✓ Ubicaciones físicas y terceros relacionados
- ✓ Interrelaciones del modelo con otros procesos.

A continuación, se explica de manera general la fase de planificación del modelo de seguridad informática tomando como base los objetivos de control de la norma internacional ISO 27002:2013 en cuanto a su aplicabilidad en la entidad municipal:

- ✓ Dimensión: Confidencialidad de la información
  - ▪ Dominio: Control de accesos
    - o Objetivo de control 9.1: Requerimientos de negocio para el control de acceso
      - ❖ Control 9.1.1: Política de control de acceso

        Hace falta políticas documentadas y revisadas que establezcan el control de acceso a instalaciones de procesamiento de información.
      - ❖ Control 9.1.2: Acceso a redes y servicios de red

        Existen restricciones a servicios de red, pero hace falta especificar más los servicios autorizados a usar.

    - o Objetivo de control 9.2: Gestión de accesos de usuario
      - ❖ Control 9.2.1: Registro y baja del usuario

        Hace falta establecer procesos formales para el registro y baja de usuarios, lo que permite una correcta asignación de derechos de acceso.
      - ❖ Control 9.2.2: Provisión de acceso a usuarios

        Hace falta formalidad en la asignación de acceso a los usuarios, así también al revocar estos.
      - ❖ Control 9.2.3: Gestión de derechos de acceso privilegiados

        Los derechos de acceso privilegiados se encuentran controlados por la unidad de sistemas de la organización.
      - ❖ Control 9.2.4: Gestión de información de autenticación secreta de usuarios

        La asignación de información de autentificación se controla a través del correo y teléfono personal.
      - ❖ Control 9.2.5: Revisión de derechos de acceso de usuarios

        No existe revisión de derechos de acceso por parte de los propietarios de activos.
      - ❖ Control 9.2.6: Eliminación o ajuste de derechos de acceso

        Hace falta formalizar la remoción de derechos de acceso a información de los empleados al concluir su empleo.

- Objetivo de control 9.3: Responsabilidades del usuario
  - Control 9.3.1: Uso de información de autenticación secreta

    No existen prácticas establecidas por la organización para el uso de información de autenticación secreta por parte de los usuarios.

- Objetivo de control 9.4: Control de acceso de sistemas y aplicaciones
  - Control 9.4.1: Restricción de acceso a la información

    Hay un control establecido mediante roles para restringir el acceso a la información y funciones del sistema.
  - Control 9.4.2: Procedimientos de inicio de sesión seguro

    Hace falta una política de control de acceso, para formalizar el procedimiento de ingreso seguro.
  - Control 9.4.3: Sistema de gestión de contraseñas

    Si existe un sistema de gestión de contraseñas, lo cual asegura la calidad de éstas.
  - Control 9.4.4: Uso de programas y utilidades privilegiadas

    Hace falta establecer un control estricto de programas que sean capaces pasar por alto los controles del sistema.
  - Control 9.4.5: Control de acceso al código fuente del programa

    El acceso al código fuente está restringido por parte de la unidad de sistemas de la organización.

✓ Dimensión: Integridad de la información

- Dominio: Seguridad en las operaciones
  - Objetivo de control 12.1: Procedimientos operacionales y responsabilidades
    - Control 12.1.1: Documentación de procedimientos operacionales

      Es importante disponer de la información a todos los usuarios que requieren conocer los procedimientos operativos.
    - Control 12.1.2: Gestión de cambios

      Debe establecerse un control de los cambios en los procesos, instalaciones y sistemas relacionados a la información

- ❖ Control 12.1.3: Gestión de la capacidad

  Debe realizarse un monitoreo a las proyecciones de las capacidades del desempeño requerido del sistema.

- ❖ Control 12.1.4: Separación de los ambientes de desarrollo, pruebas y operación

  A fin de reducir los riesgos de acceso no autorizado o cambios al entorno operativo.

- Objetivos de control 12.2: Protección de software malicioso
  - ❖ Control 12.2.1: Controles contra software malicioso

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

- Objetivos de control 12.3: Respaldo
  - ❖ Control 12.3.1: Respaldo de información

    Se hace uso de herramientas en la nube como respaldo.

- Objetivos de control 12.4: Bitácoras y monitoreo
  - ❖ Control 12.4.1: Bitácoras de eventos

    Hace falta el registro de los eventos realizados por el personal, así también como fallas presentadas en los sistemas

  - ❖ Control 12.4.2: Protección de información en bitácoras

    Hace falta mantener la privacidad de la información generada por los eventos

  - ❖ Control 12.4.3: Bitácoras de administrador y operador

    No existe la necesidad de registrar los eventos realizados por el personal administrativo

  - ❖ Control 12.4.4: Sincronización de relojes

    Los relojes están sincronizados de acuerdo a la zona horaria que brinda internet.

- Objetivo de control 12.5: Control de software operacional
  - ❖ Control 12.5.1: Instalación de software operacional

Se debería de tener los procedimientos documentados para la instalación de software en sistemas operacionales.

- Objetivo de control 12.6: Gestión de vulnerabilidades técnicas
  - ❖ Control 12.6.1: Gestión de vulnerabilidades técnicas

    Se debería tener documentada aquellas vulnerabilidades técnicas que pueden afectar a los sistemas de información.
  - ❖ Control 12.6.2: Restricciones en la instalación de software

    Se tienen explícitas las reglas para que los usuarios no realicen alguna instalación.

- Objetivo de control 12.7: Consideraciones de auditoría de sistemas de información
  - ❖ Control 12.7.1: Controles de auditoría de sistemas de información

    Se debería auditar de las actividades que involucran al sistema de información y los procesos del negocio.

✓ Dimensión: Disponibilidad de la información

- Dominio: Seguridad en las comunicaciones
  - Objetivo de control 13.1: Gestión de seguridad en red
    - ❖ Control 13.1.1: Controles de red

      Debe gestionarse el control de las redes, mediante la configuración correcta de los equipos, aplicaciones e información que comprometen.
    - ❖ Control 13.1.2: Seguridad en los servicios en red

      Se debe tener mecanismos de seguridad, niveles de servicio y requisitos de gestión.
    - ❖ Control 13.1.3: Segregación en redes

      Se debe segregar la información para los usuarios.

  - Objetivo de control 13.2: Transferencia de información
    - ❖ Control 13.2.1: Políticas y procedimientos para transferir datos

Hace falta políticas y/o directivas establecidas para la transferencia formal de información.

❖ Control 13.2.2: Acuerdos en la transferencia de información

No existe un acuerdo que dirija la transferencia segura de la información con las partes externas.

❖ Control 13.2.3: Mensajería electrónica

Los correos utilizados para mensajería son institucionales, lo cual reduce el riesgo de alteraciones.

❖ Control 13.2.4: Acuerdos de confidencialidad o no-revelación

Al contratar personal para la unidad, se indican los acuerdos de confidencialidad.

- Fase 3: Implementación

Esta fase le permitirá a la entidad municipal, llevar a cabo la implementación de la planificación realizada en la fase anterior del modelo de seguridad informática.

Con base a los resultados de la fase de planeación, en la fase de implementación deberá ejecutarse las siguientes actividades:

✓ Dimensión: Confidencialidad de la información

▪ Dominio: Control de accesos

o Objetivo de control 9.1: Requerimientos de negocio para el control de acceso

❖ Control 9.1.1: Política de control de acceso

Se ha creado la política de usuarios y grupos con definición de una serie de grupos que tendrán determinados accesos para cada tipo de información establecido y asignación de permisos, así como tener un procedimiento que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios y las cuentas de administración.

❖ Control 9.1.2: Acceso a redes y servicios de red

Se ha creado perfiles de seguridad para todos los usuarios; se ha pedido a todos los usuarios que firmen un acuerdo de uso apropiado antes de que tengan acceso a los equipos; se ha definido procedimientos donde se registren las altas, las bajas y los cambios de usuarios.

- Objetivo de control 9.2: Gestión de accesos de usuario
  - Control 9.2.1: Registro y baja del usuario

    Se ha determinado procedimientos para cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas.

  - Control 9.2.2: Provisión de acceso a usuarios

    Se ha establecido mecanismos de control de acceso físico y lógico para los usuarios, con el fin de asegurar que los activos de información se mantengan protegidos de una manera consistente.

  - Control 9.2.5: Revisión de derechos de acceso de usuarios

    Se ha creado registros de la actividad realizada, que pueden ser revisados periódicamente o en una investigación, con el objetivo de detectar abusos y amenazas.

  - Control 9.2.6: Eliminación o ajuste de derechos de acceso

    Se ha dispuesto de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal, la cual puede ser modificada cuando se presente un cambio de funciones del empleado o se retire definitivamente.

- Objetivo de control 9.3: Responsabilidades del usuario
  - Control 9.3.1: Uso de información de autenticación secreta

    Se propone que la identidad de cada usuario que accedan a los recursos informáticos debe ser establecida y autenticada de una manera única.

- Objetivo de control 9.4: Control de acceso de sistemas y aplicaciones
  - Control 9.4.2: Procedimientos de inicio de sesión seguro

    Se ha propuesto buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas para la validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos de manera segura.

- ✓ Dimensión: Integridad de la información
  - ▪ Dominio: Seguridad en las operaciones
    - o Objetivo de control 12.1: Procedimientos operacionales y responsabilidades
      - ❖ Control 12.1.1: Documentación de procedimientos operacionales

        Se ha propuesto definir mediante un documento aquellos procedimientos operacionales, donde se detallen las actividades correspondientes y personal implicado. Además, distribuir esta información con los usuarios.

      - ❖ Control 12.1.2: Gestión de cambios

        Se ha propuesto tener documentos de control de todo cambio en la infraestructura informática además debe ser realizado de acuerdo con los procedimientos de gestión de cambios del área de TI de la entidad municipal.

      - ❖ Control 12.1.3: Gestión de la capacidad

        Se ha propuesto revisiones periódicas por parte del área de TI, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (Plan de capacidad) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica.

      - ❖ Control 12.1.4: Separación de los ambientes de desarrollo, pruebas y operación

        Se ha determinado que el área de TI debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- ✓ Dimensión: Disponibilidad de la información
  - ▪ Dominio: Seguridad en las comunicaciones
    - o Objetivo de control 13.1: Gestión de seguridad en red

- ❖ Control 13.1.1: Controles de red

  Se ha propuesto mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas y minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

- ❖ Control 13.1.2: Seguridad en los servicios en red

  Se ha propuesto identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

- ❖ Control 13.1.3: Segregación en redes

  Se ha propuesto mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la entidad municipal.

- Fase 4: Evaluación de desempeño

  El proceso de seguimiento y monitoreo del modelo de seguridad informática se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

  En esta actividad la entidad debe crear un plan que contemple las siguientes actividades:

  - ✓ Revisión de la efectividad de los controles establecidos y su apoyo al cumplimiento de los objetivos de seguridad.
  - ✓ Revisión de la evaluación de los niveles de riesgo después de la aplicación de controles y medidas administrativas.
  - ✓ Seguimiento al alcance y a la implementación del modelo de seguridad informática.
  - ✓ Seguimiento a los registros de acciones y eventos/incidentes que podrían tener impacto en el desempeño de la seguridad informática al interior de la entidad municipal.
  - ✓ Medición de los indicadores de gestión del modelo de seguridad informática.
  - ✓ Revisiones de acciones o planes de mejora.

  Este plan deberá permitir la consolidación de indicadores periódicamente y su evaluación frente a las metas esperadas.

- Fase 5: Mejora continua

  En esta fase la entidad municipal debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad informática, tomando las acciones oportunas para mitigar las debilidades identificadas.

  En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye:

  - ✓ Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el modelo de seguridad informática.
  - ✓ Resultados del plan de ejecución de auditorías y revisiones independientes al modelo de seguridad informática.

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 - LIMA NORTE, asesor de Tesis titulada: "Propuesta de un Modelo de seguridad informática para la Protección de datos en la Municipalidad Distrital de Pinra, Huánuco 2022", cuyo autor es SANCHEZ CAMPOS KRYSTEL ELENA, constato que la investigación tiene un índice de similitud de 20.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 24 de Junio del 2022

Apellidos y Nombres del Asesor:	**Firma**
AGREDA GAMBOA EVERSON DAVID **DNI:** 18161457 **ORCID:** 0000-0003-1252-9692	Firmado electrónicamente por: AGREDA el 02-08-2022 09:22:15

Código documento Trilce: TRI - 0310462

INVESTIGA UCV