UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Guizado Castillo, Jose Manuel (orcid.org/0000-0002-2666-816X)

ASESORES:

Dra. Alza Salvatierra, Silvia Del Pilar (orcid.org/0000-0002-7075-6167)

Dr. Vargas Huaman, Jhonatan Isaac (orcid.org/0000-0002-1433-7494)

LÍNEA DE INVESTIGACIÓN:

Sistemas de Información y Comunicaciones

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2024

DEDICATORIA

Dedico este trabajo a mi madre, por ser ella la razón y motivo de seguir adelante, por ser mi ejemplo constante de no rendirme y seguir adelante y cada día mostrarme que siempre hay algo nuevo que aprender.

AGRADECIMIENTO

Agradecer a Dios por darme la fuerza de seguir adelante y darme salud para continuar mis metas; a mis padres de corazón por siempre confiar en mí, a los docentes de la Universidad César Vallejo por guiarme en la elaboración de la presente tesis.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, ALZA SALVATIERRA SILVIA DEL PILAR, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis Completa titulada: "SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023", cuyo autor es GUIZADO CASTILLO JOSE MANUEL, constato que la investigación tiene un índice de similitud de 14.00%, 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 Completa 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, 17 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
ALZA SALVATIERRA SILVIA DEL PILAR **DNI:** 18110381 **ORCID:** 0000-0002-7075-6167	Firmado electrónicamente por: SALZAS el 20-01-2024 09:55:44

Código documento Trilce: TRI - 0733883

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Originalidad del Autor

Yo, GUIZADO CASTILLO JOSE MANUEL estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

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

Nombres y Apellidos	**Firma**
JOSE MANUEL GUIZADO CASTILLO **DNI:** 41642580 **ORCID:** 0000-0002-2666-816X	Firmado electrónicamente por: JGUIZADOCA el 17-01-2024 08:29:37

Código documento Trilce: TRI - 0733886

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

RESUMEN

En la presente investigación titulada “SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023” estableció como objetivo determinar la incidencia SGSI según ISO/IEC 27001:2022 en la protección de información de una Municipalidad distrital, Lima 2023. La metodología empleada fue tipo aplicada, enfoque cuantitativo, nivel correlacional causal y diseño no experimental, asimismo la población estuvo conformada por 200 trabajadores, el cual se realizó un cálculo muestral obteniendo 132 trabajadores especializados en el área de tecnologías, siendo muestreo no probabilístico por conveniencia, para la recolección de datos se aplicó la técnica de la encuesta y como instrumento dos cuestionarios que fueron evaluados por 3 juicios de expertos en la materia, además mediante el alfa de Cronbach se decretó la confiabilidad de los instrumentos, teniendo 0.842 para el cuestionario SGSI y el cuestionario de la protección fue 0.885. En los resultados, se precisó nivel óptimo en la variable SGSI y nivel medio en la variable protección de información, es más se tuvo una correlación 0.611 con significancia 0.032 < 0.05. En conclusión, el SGSI según ISO/IEC 27001:2022 incidió significativamente en la protección de información de una Municipalidad distrital, Lima 2023.

Palabras clave: Seguridad de información, confidencialidad, integridad, disponibilidad.

ABSTRACT

In the present research titled "ISMS according to ISO/IEC 27001:2022 and its impact on the protection of information in a district municipality, Lima 2023" the objective was to determine the incidence of ISMS according to ISO/IEC 27001:2022 on the protection of information of a district Municipality, Lima 2023. The methodology used was applied type, quantitative approach, causal correlational level and non-experimental design, also the population was made up of 200 workers, for which a sample calculation was carried out obtaining 132 workers specialized in the area of technologies, being non-probabilistic sampling for convenience, for data collection the survey technique was applied and as an instrument two questionnaires that were evaluated by 3 judgments of experts in the field, also through Cronbach's alpha the reliability of the instruments was decreed , having 0.842 for the SGSI questionnaire and the protection questionnaire was 0.885. In the results, an optimal level was specified in the SGSI variable and an average level in the information protection variable, in fact there was a rating of 0.611 with significance 0.032 < 0.05. In conclusion, the ISMS according to ISO/IEC 27001:2022 had a significant impact on the information protection of a district municipality, Lima 2023.

Keywords: Information security, confidentiality, integrity ,availability.

I. INTRODUCCIÓN

Actualmente, el manejo y protección de información se ha vuelto extremadamente problemático debido a los grandes avances tecnológicos que se han dado recientemente, lo que también trajo consigo grandes amenazas, esto se debe a que no existe un control sobre la protección de la información ni una estandarización de los procedimientos para gestionarla, dado que la información que manejan las diferentes organizaciones y empresas es considerada su activo más valioso (De la Rosa, 2021).

Al nivel internacional, el gobierno de Colombia en cuanto a la credibilidad con el público, presentó el riesgo de que la información sea vulnerada y amenazada llegando afectar la confidencialidad e integridad de los registros públicos, por tener sistemas y aplicaciones desactualizadas, como también contraseñas predeterminadas no modificadas, por tal motivo el gobierno viene ejecutando el ISO 27001 para la mitigación de los riesgos (Ramírez y Rincoc, 2022). Asimismo, en Colombia el SGSI de una biblioteca universitaria, la política de seguridad que había implementado para salvaguardar sus datos, generó debate porque, a pesar de la accesibilidad de estos datos, la protección de información fue violada por factores humanos como la eliminación del almacenamiento de los datos y para restaurar condujo a obtener grandes gastos (Guerra, Neira y Diaz, 2021).

Por otro lado, en Ecuador por la inexistencia de un sistema de seguridad debido al atraso tecnológico, el 49% de las Pymes tuvieron como consecuencia la exposición de información confidencial, a pesar que en los últimos cinco años ha aumentado empresarialmente, se encontró que en el área de la seguridad informática se están quedando asilados y están sufriendo pérdidas por ataques maliciosos de phishing o malware, debido a que creen que invertir en ciberseguridad es un gasto innecesario y no priorizan métodos de detección temprana, además no implementan métodos efectivos, ni capacitan a su personal o compran software de seguridad (Zuña et al., 2019).

Al nivel nacional, la protección de información en municipalidades peruanas se vio afectadas por amenazas contra sus activos como la pérdida, manipulación o no disponibilidad de la información, también está cada vez más vulnerable a cualquier ataque informático. Además, se informó que el 65% de las

organizaciones fueron víctimas de ataques en 2018, y el 10% de ellas perdieron más de $1 millón en el sector empresarial que sufrió la mayoría de los robos y pérdidas de datos, estos incidentes fueron el resultado de medidas de seguridad insuficientes, lo que disminuyó la productividad, la credibilidad, la competitividad y un daño financiero que puso en peligro la viabilidad, incluso cuando no invierten en software de seguridad (Bustamante et al., 2021).

También, en el Perú es crucial que las empresas implementen mecanismos o estrategias para salvaguardar no solo su propia información sino también la de sus clientes, colaboradores y socios estratégicos, debido a que un control y seguridad inadecuados puede conducir a problemas legales haciendo que las organizaciones estén vulnerables a riesgos de alto impacto, daños innecesarios y la pérdida de información confidencial como resultado de la falta de mecanismos de seguridad (Rodríguez et al., 2020).

A nivel local, en el presente caso de estudio se identificó una inadecuada gestión de SGSI en la protección de información en manejo de datos y procesos digitales, ya que en los procedimientos administrativos los controles de seguridad dejaban en bandeja abierta algunos datos, además se desarrollaba inapropiadamente la evaluación de los riesgos que se presentaba en las operaciones, dada por diversos factores como: Ineficiente comprensión y conciencia del personal sobre la importancia de seguridad de información, desfavorable uso de políticas y procedimientos de seguridad, poco capacitación de personal, falta de práctica en controles técnicos y físicos, trayendo consecuencia de un improcedente manejo de información confidencial en asociación al SGSI ISO/IEC 27001:2022 en una municipalidad distrital de Lima, por ende, dicho caso impulsó a indagar la relación entre las variables para analizar si se generó un aumento o disminución del fenómeno.

Ante lo establecido, el problema general fue: ¿Cómo el SGSI según ISO/IEC 27001:2022 incide en la protección de información de una Municipalidad distrital, Lima 2023? Del mismo modo, se generó las especificas: ¿Cómo la confidencialidad del SGSI incide en la protección de información de una Municipalidad Distrital, Lima 2023? ¿Cómo la integridad del SGSI incide en la protección de información de una Municipalidad Distrital, Lima 2023? ¿Cómo la disponibilidad del SGSI incide en la protección de información de una Municipalidad Distrital, Lima 2023?

Hernández y Mendoza (2018) la justificación se apoya en aspecto teórico, práctico y metodológico que se utilizan para explicar la importancia de la investigación y las motivaciones de la realización del estudio por parte de los investigadores. La investigación se justificó teóricamente porque se refutó teorías científicas acerca del sistema de gestión de seguridad de información para aumentar conocimientos científicos en la comunidad profesional presente y futura, además se desbordó la problemática investigativa (Fernández, 2020). Por justificación metodológica, debido a que con las fuentes recopiladas acerca de la variable se contextualizó un instrumento de investigación que permitirá la realización de nuevas investigaciones, además del proceso metodológico (Villela, 2019). Por justificación práctica, porque con los resultados obtenidos de asociación de variables se tomó en cuenta sugerencias para el cambio del ámbito del estudio en función a la municipalidad (Álvarez, 2020).

Dicho fundamento, estableció el objetivo general: Determinar la incidencia SGSI según ISO/IEC 27001:2022 en la protección de información de una Municipalidad distrital, Lima 2023. Asimismo, los específicos: Determinar la incidencia de la confidencialidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023. Determinar la incidencia de la integridad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023. Determinar la incidencia de la disponibilidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023

Por último, se propuso la hipótesis general: El SGSI según ISO/IEC 27001:2022 incide significativamente en la protección de información de una Municipalidad distrital, Lima 2023. Y los específicos: La confidencialidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023. La integridad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023. La disponibilidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023.

II. MARCO TEÓRICO

Se expuso trabajos previos que respaldaron la investigación sintetizando conceptualmente con el mismo enfoque y previa problemática de análisis.

En primer lugar, cono antecedente nacional, se tuvo a la investigación de Cuenca (2023) elaborada en Lima, con el propósito Determinar si existe relación entre sistema de gestión de seguridad de información en base al ISO/IEC 27001: 2013 y la protección de activos de información en empresas privadas outsourcing, de tal modo, el método de la presente fue no experimental, de nivel correlacional y aplicada cuantitativamente, se tomó a 150 trabajadores con un cuestionario bajo una validación de expertos y fiabilidad mayor a 0.70. En los resultados, se tuvo una correlación 0.713 con bilateral 0.000 (rechazó hipótesis nula), por lo tanto, el 45% de los trabajadores mencionaron que existe una protección de información moderado y el 55% alto. En conclusión, existe una relación significativa entre SGSI en base al ISO/IEC 27001: 2013 y protección de los activos de información en las empresas privadas outsourcing.

Seguidamente, Espinoza y Mendoza (2022) determinaron la relación de la seguridad de información basada en ISO 27001 con seguimiento y control de vulnerabilidades en las PYMES en Lima. El método destacó cuantitativamente, aplicado y no experimental, utilizando como muestra los 120 trabajadores especializados en el área de seguridad informática. Para realizar el diagnóstico se utilizó técnica de encuesta con 2 instrumentos. Según el análisis, hubo una tasa de seguimiento y control de vulnerabilidades del 71% siendo moderado, lo que significa que los 95% de usuarios mencionaron al SGSI en nivel alto con significancia 0.001 y correlación = 0.540. Se concluyó, que el seguimiento y la gestión de vulnerabilidades en PYMES se relacionan significativamente por sistema de gestión de seguridad de información.

También, Castro (2022) su trabajo planteó evaluar la relación de seguridad de información y gestión del riesgo en una entidad del sistema electoral, en dicho estudio se usó encuesta y cuestionario a una población de 65 trabajadores, asimismo fue no experimental de carácter correlativo, enfoque cuantitativo y aplicada. En los análisis encontrados, el 84.44% consideró en nivel

alto al sistema de seguridad de información y gestión de riesgo en nivel alto con la opinión del 80% de los trabajadores, además la correlación fue 0.495 con significancia 0.000. En resumen, seguridad de información se relacionó positivamente con gestión del riesgo en una entidad del sistema electoral.

Ticona (2022), en su estudio realizado en Arequipa, determinó la relación entre seguridad de información basado en ISO/IEC 27001:2013 y riesgos de activos de Severox Perú S.A.C. El método usado fue experimental, aplicada, explicativo y cuantitativo; se tomó a 32 trabajadores de la empresa que se les aplicó dos cuestionarios para almacenar datos. En los resultados, seguridad de gestión de información tuvo nivel alto por el 84% y el 74% de los colaboradores evaluaron a los riesgos de activos en nivel medio y en la confidencialidad el 83% evaluó en nivel alto con significancia 0.000 y correlación = 0.721. En conclusión, la seguridad de información basado en ISO/IEC 27001:2013 se relacionó significativamente con riesgos de activos de Severox Perú S.A.C.

Finalmente, Aguilar (2021) en su investigación determinó el impacto de un sistema web basado en teoría de colas para la seguridad del cliente en un municipio de Perú. El método fue aplicado, enfoque cuantitativo, explicativo y diseño pre experimental, como muestra fueron 338 usuarios mediante la técnica de la encuesta e instrumento del cuestionario. En resultados, se logró el incremento de eficiencia en la atención al usuario con 37.44% de mejora en la disponibilidad y en la protección de datos tuvo mejora de 14.14%. En conclusión, el sistema web dio un impacto positivo en la seguridad de los usuarios en un municipio de Perú.

Como antecedente internacional, se obtuvo a Correa (2023) investigación realizada en Ecuador, presentó el objetivo de evaluar como el sistema de gestión de seguridad de la información establece controles de ISO/IEC 27002:2022 mejorando la seguridad del gobierno Cantón Naranjal, dicho documentó aplicó el método cuantitativo y experimental, siendo alcance explicativo, la investigación examinó a 31 trabajadores a través del cuestionario. En los resultados, el 42% detalló que el SGSI antes era de nivel bajo y después de la mejora el 75% detalló que fue de nivel alto, de igual manera, la confidencialidad mejoró un 44%, la disponibilidad mejoró 58% y la integridad mejoró un 34%, de

cierto modo la significancia fue 0.003 < 0.50. En conclusión, los controles del SGSI influyeron en la seguridad de la información del gobierno Cantón Naranjal.

Asimismo, en la investigación de Guacanés y Vilatuña (2022) elaborada en Colombia, cuyo objetivo fue determinar como el sistema de gestión de seguridad de información se relaciona con toma de decisiones de la empresa Ultralink, dicho documento fue cuantitativo, no experimental del nivel correlacional, haciendo uso del cuestionario a 200 trabajadores. En los análisis, el nivel de cumplimiento de los controles fue el 33% en nivel moderado, el 45% de los trabajadores indicaron que nivel moderado fue la confiabilidad, el 81% nivel alto en la disponibilidad y el 69% de nivel moderado en la integridad, asimismo tuvo una correlación 0.640 y significancia 0.000. En conclusión, el sistema de gestión de seguridad de información se relacionó significativamente con la toma de decisiones en mención a la confidencial, disponibilidad e integridad.

Además, Torres y Chicaiza (2020) en su estudio realizado en Ambato-Ecuador, estableció como objetivo estimar la aplicación de un modelo de SGSI para un plan de seguridad informática en la empresa Megaprofer S.A, se generó una metodología numérica de nivel explicativa con diseño pre experimental en campo, la población fueron los 25 personales de dicha organización que se le aplicaron la técnica una encuesta. En la estadística, antes de la aplicación de mejora se tuvo el 67% de los trabajadores que evaluaron a la SI en nivel baja, después de la mejora, el 84% de los trabajadores evaluaron a la seguridad de información en nivel alto en relación a confidencialidad y disponibilidad con una significancia de 0.033 < 0.050. Se concluyó que, el plan de implementación ayudó a proteger la información de la organización.

Por último, Guevara (2019) en su estudio realizado en Ecuador, determinó los procesos de sistema de gestión de seguridad de la información ISO/IEC 27001 garantizando seguridad organizacional, en el proceso metodológico se utilizó el instrumento del cuestionario a 48 trabajadores, siendo cuantitativo y pre experimental. En los resultados, la confidencialidad antes era 22% después de emprender la mejora fue de 90% mostrando una seguridad confortable a la empresa, asimismo se dio una revisión independiente de la seguridad de

información de 20%, significancia obtenida fue 0.000 < 0.05. Por lo tanto, se concluyó que el SGSI ISO/IEC 27001 mediante los procesos de controles garantizó la protección de la información.

Continuamente, se presentó bases teóricas de variables estudiadas que constituyeron fundamento teórico, implicando teorías relacionadas en el conocimiento científico.

La teoría general de la gestión del sistema de seguridad fue puesta en marcha por Ludwing Von Bertalanffy en relación a las organizaciones fomentó que es el sistema colectivo para la toma de decisiones de manera concreta y fácil, cuyo enfoque es examinar los riesgos de una organización asociados a los datos que se manipulan para un bien común (Bustamante et al. 2021).

Según la teoría relacionada presentada por Bustamante et al. (2021), el SGSI debería poder evaluar los riesgos relacionados con los activos de información que se gestionan dentro de una organización a través de la norma ISO 27001 que requiere un SGSI como componente necesario con el respaldo de los tres pilares de disponibilidad, integridad y confidencialidad de la información.

El diagnóstico, la memoria, el mantenimiento, la toma de decisiones y la operación son algunas de la Teoría General de Sistemas y su perspectiva funcional con un nivel inicial que incluye: Política de Sistema de seguridad en la organización de los Recursos Humanos para la Gestión, también incluye elementos de planificación, asignación, comunicación, retroalimentación, evaluación y medición (López, 2019).

En cuanto al enfoque teórico, el SGSI según norma ISO 27000, para mantener seguridad de datos privados en empresas, se gestionan metódicamente, teniendo en cuenta los sistemas de TI, los procesos comerciales y las personas. Se utiliza un proceso de gestión para lograr esto. (Marlon, 2019).

La norma ISO 27001 es un patrón internacional de cláusulas para el mantenimiento y mejora continua de sistemas de gestión de seguridad de información (Baca et al., 2020). Dicho sistema tiene la función de salvaguardar

la confidencialidad, integridad y disponibilidad de toda información (Fong y Ballona, 2022).

La norma incluye definir políticas y procedimientos, identificar activos críticos y evaluar riesgos. Después de la implementación del SGSI, se realiza una auditoría interna y externa por parte de un organismo de certificación acreditado (Mahecha, et al., 2023). Este alcance del SGSI dispone conocer la aplicabilidad y límites de protección de datos con otros activos que tengan que haber con el municipio (Vásquez, 2018).

Según Peris (2023) Es una forma fundamental de abordar la ejecución en el trabajo y desarrollar aún más la seguridad de los datos de una asociación mediante el cumplimiento de sus objetivos comerciales y administrativos mediante series de estrategias, procedimientos y pautas, así como las actividades relacionadas que son administrados colectivamente por una organización en un esfuerzo por proteger sus activos de información críticos.

Asimismo, es fundamental para la toma de decisiones a nivel estratégico, táctico y operativo en diversas áreas funcionales del municipio, el cual actúa como herramienta poderosa para respaldar los procesos desarrollados y apoya todas las actividades que se realizan contribuyendo en el procesamiento de datos para generar información confidencial, integro y disponible en la utilidad de toma de decisiones de gestión (Vargas, et al., 2019)

El Sistema de Gestión de Seguridad de Información (SGSI) permite gestionar adecuadamente seguridad de datos institucionales para contrarrestar amenazas de ataque o intrusión, error y eventos inevitables, incluyendo otros (Abrego, Sánchez y Medina, 2018).

De acuerdo a De La Rosa (2021) un SGSI es un conjunto de directrices o procedimientos utilizados para identificar riesgos y especificar las acciones que se deben tomar para mitigarlos con la identificación de los activos de datos en base al análisis del conocimiento y la aplicación de los controles.

El objetivo del SGSI en las organizaciones es evaluar riesgos y determinar medidas de control adecuadas para eliminar por completo o reducir significativamente sus efectos negativos (Coronel y Quirumbay, 2022).

Específicamente, la capacidad de la organización para gestionar y salvaguardar su información se ve reforzada por certificación de un Sistema de Gestión de Seguridad de la Información (SGSI). La base de seguridad de la información es la preservación de disponibilidad, confidencialidad e integridad de los datos (Marlon, 2019).

De tal manera, según De La Rosa (2021) se definió las siguientes dimensiones del SGSI:

Dimensión confidencialidad, para salvaguardar la protección de los datos e información recabada, la confidencialidad garantiza que solo las personas u organizaciones autorizadas tengan acceso a la misma y que no se compartirá sin consentimiento, los esfuerzos de seguridad de datos deben garantizar que el secreto de la información se ponga en peligro (De La Rosa, 2021).

Asimismo, la confidencialidad de información garantiza el proceso y almacenamiento de datos a mantenerse lo más secreto posible para evitar la divulgación no autorizada (Tonysé, 2021).

Dimensión integridad, la información debe estar garantizada por los sistemas que la gestionan, lo que significa que debe mostrarse exactamente como fue diseñada, sin alteraciones o manipulaciones que no hayan sido expresamente autorizadas. El objetivo principal es garantizar que los datos se transmitan en un entorno seguro mientras se utilizan protocolos y técnicas seguros para reducir los riesgos (De La Rosa, 2021).

Además, respecto a la integridad de información, cuando los datos se transfieren o almacenan, su integridad garantiza que no hayan sido alterados, perdidos o destruidos, ya sea intencionalmente o no (Panaqué, Lizárraga y Mendoza, 2021).

Dimensión disponibilidad, esto garantiza que todas las personas u organizaciones con derechos de acceso siempre puedan acceder a la información. Para esto, debe haber medidas de soporte y seguridad que puedan acceder a los datos según sea necesario y que protejan contra las interrupciones del servicio (De La Rosa, 2021).

El principio esencial de seguridad de información, es disponibilidad de información o activos de información que garantiza acceso rápido y confiable a los datos y recursos por parte de personas o individuos autorizados que cuenten con credenciales requeridas (Duval, Delgado, Mendoza, 2022).

En cuanto a la teoría de la variable Protección de la información, también llamada seguridad de información se basa en el acceso, la utilización, divulgación o destrucción no autorizada del sistema de una empresa que ha evolucionado considerablemente y dispone de la planificación de la continuidad para mantener los controles, programas y políticas bajo una confidencialidad y disponibilidad de los datos (Meraz, 2018).

Según Castillo y Pérez (2018) la protección de la información se trata de asegurar o salvaguardar datos confidencial e importante de individuos y organizaciones de cualquier parte externa que pueda usarla sin su permiso contra corrupciones, pérdida o filtraciones.

De igual manera Parada, Gómez y Flores (2018) La seguridad de datos alude a la disposición de enfoques, métodos y dispositivos utilizados para cumplir, proteger y garantizar que ningún dato salga del sistema que la organización ha configurado. Es un componente crucial para que las empresas operen porque los datos que administran son cruciales para el trabajo que realizan (Arcos, Matute y Fernández, 2023).

Según ISO 27001 (2022), la seguridad de información se enfoca en confidencialidad, integridad y disponibilidad de datos e información cruciales para la organización, independientemente del formato en que se encuentren. escrito. vídeos y audios, etc.

La Protección de información se da por el buen manejo de SGSI, que mitiga los riesgos, reduciendo así la probabilidad de una violación de seguridad y mejorando la eficiencia (Mejía et al., 2023). Lo cual intervienen componentes como la dirección estratégica, gestión de mejora, innovación, procesos, proyectos y monitoreo constante (Jiménez y López, 2023).

La protección de información se refiere a un grupo de medidas preventivas y reactivas que aseguran la información con un manejo adecuado de los datos,

ya que es un activo intangible invaluable y, por lo tanto, su gestión y protección debe ser principal en cualquier organización (Guevara, Delgado y Mendoza, 2022)

El objetivo de la protección de información son las necesidades que una organización quiere que se satisfagan para garantizar disponibilidad, seguridad y confidencialidad de información y los datos, tanto propios como ajenos (Villalba y Donado, 2022).

La importancia de la protección de información radica en el propósito de prevenir el robo de información en cualquier área de la organización, donde la prevención es la clave de la importancia de la seguridad informática. También ayuda a determinar la presencia de amenazas y peligros de virus en los sistemas de información internos (Meraz, 2018).

De acuerdo a Guevara, Delgado y Mendoza (2022) la protección de información se distribuyó como dimensiones de la siguiente forma:

La primera dimensión son los controles de seguridad, que son medidas preventivas y mitigantes implementadas para minorizar riesgos de seguridad y garantizar confidencialidad, integridad y disponibilidad de activos físicos. Estos controles incluyen políticas, procedimientos, medidas técnicas para salvaguardar el sistema (Shojaie, 2018)

La aplicabilidad de controles de sistema de gestión de información asegura que el servicio cumpla consistentemente con las especificaciones para las cuales fue diseñado, brindando valor agregado, asimismo si se presenta una queja de los usuarios se resuelve con calidad funcional en la gestión respondiendo de manera oportuna a los servicios generados, utilizando tecnología para permitir la automatización y sincronización entre departamentos y funciones que integran la seguridad de los datos (Flores, et al., 2019).

Segunda dimensión, evaluación de riesgos, que es un proceso fundamental que se utiliza para identificar y luego evaluar los riesgos potenciales que pueden ocurrir. Este proceso identificará los activos de información clave de la empresa, identificará vulnerabilidades, determinando el efecto de posibles violaciones de seguridad organizacional (Shojaie, 2018).

Asimismo, es el proceso de análisis de riesgo de una organización que determina la probabilidad y ocurrencia de la operatividad con el impacto de contexto y responsabilidades, cuya finalidad es adoptar el conocimiento de todas las funcionalidades del sistema (ISO 27001, 2022).

La tercera dimensión es gestión de incidentes de seguridad, un esencial proceso del SGSI destinado a prevenir, detectar y recuperarse de incidentes que puedan impactar los datos. Esta gestión incluye planificar, implementar, monitorear y mejorar tareas y reglas de gestión de incidentes para mitigar impactos (Guevara, Delgado y Mendoza, 2022).

En mismo contexto, es el proceso de análisis de riesgo de una organización que determina la probabilidad y ocurrencia de la operatividad con el impacto de contexto y responsabilidades, cuya finalidad es adoptar el conocimiento de todas las funcionalidades del sistema (ISO 27001, 2022).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1 Tipo de investigación

Fue aplicada, en virtud a los análisis del SGSI en la variable protección de información donde los resultados obtenidos contribuyó como aporte para el cambio del fenómeno presentado. Según Delgado (2021) se origina con el aspecto teórico que busca la utilización de conocimientos para situaciones concretas.

El método fue hipotético-deductivo, pues las teorías se desarrollaron con base en las observaciones concluyentes de la investigación, y también se probaron las hipótesis. De acuerdo a De La Cruz (2020) mencionó que dicho método describe lo empírico en relación a la inducción- deducción.

Se trabajó con el enfoque cuantitativo porque tuvo como finalidad analizar el comportamiento de la muestra mediante medición numérica y la aprobación de las hipótesis de manera estadística. En base a Guerrero (2022) fundamentó que el enfoque cuantitativo es procesado y expresado en números.

La investigación fue de nivel correlacional porque midió la asociación del SGSI con la protección de la información en su contexto determinado. Según Ramos (2020) mide la relación estadística de las variables entre sí, analizando la relación si va en aumento o diminución.

3.1.2 Diseño de investigación

Se usó el diseño no experimental, corte transversal, porque las variables SGSI y protección de la información no tuvieron alteraciones y se midieron una sola vez en su estado actual sin influencia de una. De acuerdo a Arias (2021) definió que este diseño se evalúa en su forma más básica, dedicándose a la observar los fenómenos a medida entorno natural.

3.2. Variables y operacionalización

Variable 1: SGSI según ISO/IEC 27001:2022

Definición conceptual

El SGSI es un conjunto de directrices o procedimientos utilizados para identificar riesgos y especificar las acciones que se deben tomar para mitigarlos con identificación de activos de información en base al análisis del conocimiento y la aplicación de los controles (De La Rosa, 2021).

Definición operacional

La variable SGSI según ISO/IEC 27001:2022 se ha operacionalizado haciendo uso de tres dimensiones (confidencialidad, integridad y disponibilidad); asegurándose que la información recabada ha sido evaluada en los siguientes 3 niveles: No óptimo (1), Medio (2) y Óptimo (3)

Dimensiones:

Dimensión confidencialidad, para salvaguardar la protección de los datos e información recabada, la confidencialidad garantiza que solo las personas u organizaciones autorizadas tengan acceso a la misma y que no se compartirá sin consentimiento, los esfuerzos de seguridad de datos deben garantizar que el secreto de la información se ponga en peligro (De La Rosa, 2021).

Dimensión integridad, la información debe estar garantizada por los sistemas que la gestionan, lo que significa que debe mostrarse exactamente como fue diseñada, sin alteraciones o manipulaciones que no hayan sido expresamente autorizadas (De La Rosa, 2021).

Dimensión disponibilidad, esto garantiza que todas las personas u organizaciones con derechos de acceso siempre puedan acceder a la información. Para esto, debe haber medidas de soporte y seguridad que puedan acceder a los datos según sea necesario y que protejan contra las interrupciones del servicio (De La Rosa, 2021).

Indicadores

Protección de la información, Accesos, Redes, Información crítica, Claves y contraseñas, Protección de datos, Fiabilidad de los recursos, Ataques, Almacenamiento, Sistema de información, Acceso a la información, Sistemas de información, Aspectos técnicos, Causas humanas y naturales

Escala de medición ordinal:

Nunca (1), Casi nunca (2), A veces (3), Casi siempre (4), Siempre (5)

Variable 2: Protección de información

Definición conceptual

Se refiere a un grupo de medidas preventivas y reactivas que aseguran la información con un manejo adecuado de los datos, ya que es un activo intangible invaluable y, por lo tanto, su gestión y protección debe ser principal en cualquier organización (Guevara, Delgado y Mendoza, 2022).

Definición operacional

La variable protección de información se ha operacionalizado haciendo uso de tres dimensiones (controles de seguridad, evaluación de riesgos y gestión de incidentes de seguridad); asegurándose que la información recabada ha sido evaluada en los siguientes 3 niveles: No óptimo (1), Medio (2) y Óptimo (3)

Dimensiones:

La primera dimensión son controles de seguridad, que son medidas preventivas y mitigantes implementadas para minorizar riesgos de seguridad y garantizar confidencialidad, integridad y disponibilidad de activos físicos. Estos controles incluyen políticas, procedimientos, medidas técnicas para salvaguardar el sistema (Shojaie, 2018)

Segunda dimensión, evaluación de riesgos, que es un proceso fundamental que se utiliza para identificar y luego evaluar los riesgos potenciales que pueden ocurrir. Este proceso identificará los activos de

información clave de la empresa, identificará vulnerabilidades, determinando impacto de posibles violaciones de seguridad organizacional (Shojaie, 2018).

La tercera dimensión es la gestión de incidentes de seguridad, un importante proceso del SGSI destinado a prevenir, detectar y recuperarse de incidentes que puedan impactar a los datos. Esta gestión incluye planificar, implementar, monitorear y mejorar las tareas y reglas de gestión de incidentes para mitigar el impacto (Guevara, Delgado y Mendoza, 2022).

Indicadores

Revisión, Disponibilidad, Mejora, Confiabilidad y Verificación

Escala de medición:

Nunca (1), Casi nunca (2), A veces (3), Casi siempre (4), Siempre (5)

Matriz de operacionalización ver en anexo 2.

3.3. Población (criterios de selección), muestra, muestreo, unidad de análisis

3.3.1 Población

Grupo total de los miembros que serán medidos para el análisis del fenómeno (Romero, 2020). La población fueron los 200 trabajadores de una Municipalidad Distrital de Lima.

Criterios de inclusión: Colaboradores con experiencia más de 2 años.

Criterios de exclusión: A todos los trabajadores del área de planeamiento y Gerencial general de administración

3.3.2 Muestra.

Es una porción pequeña que contiene características particulares para ser examinadas (Cortés et al., 2020). De cierto modo, para la muestra se sacó la formula finita al conocer la población total, obteniendo una

muestra de 132 trabajadores especializados en el área de tecnologías de información, abastecimiento, presupuesto y rentas. (ver anexo 10)

3.3.3 Muestreo

Fue muestreo no probabilístico por conveniencia, teniendo en cuenta que no hay un criterio específico para elegir a los trabajadores del área de tecnologías de información, debido a la proximidad del investigador, según Quispe et al. (2020) es un método de muestra que se basa a selección del criterio del investigador.

3.3.4 Unidad de análisis

Trabajadores de una Municipalidad Distrital de Lima

3.4. Técnicas e instrumentos de recolección de datos

3.4.1 Técnica

Fue la encuesta, según Gonzáles et al. (2018) es un método estratégico recolector, asimismo la encuesta es el procedimiento de la técnica que busca la recolección de los fenómenos estudiados.

3.4.2 Instrumento

Se ejecutó el cuestionario, siendo 2 cuestionarios una para cada variable, donde el instrumento de SGSI contó con 18 ítems y el instrumento de protección de información 18 ítems, a través de una escala de Likert del 1 al 5: Nunca (1), casi nunca (2), a veces (3), casi siempre (4), siempre (5). (ver anexo 3). Según Escofet et al. (2018) mencionó que el instrumento es un recurso compuesto por preguntas que responden para el análisis de comprobación de objetivos.

3.4.3 Validez

La validez es un nivel de conformidad que muestra la consistencia de las preguntas para la medición correcta (Fernández et al., 2019). De tal modo, los dos instrumentos pasaron por un proceso de validación de expertos que fueron aprobados de manera conforme para la medición, dichos expertos fueron Dr. Lezama Gonzales Pedro Martin, Dr. Marlon

Frank Acuña Benites y Dr. Pereyra Acosta Manuel Antonio de profesión ingeniería de sistemas (ver anexo 6).

3.4.4 Confiabilidad

La confiabilidad es herramienta estadística conocida que produce resultados homogéneos con el uso repetido (Márquez, et al., 2018). Por lo tanto, se tomó prueba piloto para la fiabilidad del instrumento, considerando a 30 trabajadores que fue procesados por el alfa de Cronbach (ver anexo 4), el cual los instrumentos mostraron coeficientes superiores a 0.70, por ende, fueron fiables para medir, ya que el instrumento SGSI tuvo 0.842 y el instrumento de la protección de la información tuvo 0.885. (ver anexo 5)

3.5. Procedimientos

Primero se validó los cuestionarios con el respaldo de expertos de profesión, asimismo se pidió permiso al Gerente Municipal de una Municipalidad distrital de Lima contando con un consentimiento informado de los trabajadores, progresivamente se realizó las coordinaciones con el gerente municipal, efectuando una reunión con los trabajadores para participar en la recolección de datos, dicho momento se aplicó el cuestionario a 132 trabajadores especializados de manera presencial, entregándoles las hojas y brindándoles a la vez las instrucciones del llenado, el cual se tomó un tiempo de 20 minutos, luego se recolectó las hojas respondidas dejándoles el anuncio de que la información almacenada es confidencial y para uso académico, seguidamente se pasó los datos a Excel, donde se tabuló para luego ser procesado por el SPSS V.26 obteniendo el análisis de los resultados.

3.6. Método de análisis de datos

Optó métodos basado en diagnóstico del problema, donde se recopilaron y procesaron datos para determinar las hipótesis. Por lo tanto, se llevó a cabo análisis descriptivos e inferenciales.

Análisis descriptivo, se mostró los resultados de manera frecuencial y porcentual después de ser procesados por el SPSS V.26, asimismo

fueron analizados e interpretados por tablas y figuras donde se demostró el estado que muestran los trabajadores en la municipalidad estudiada en función a las variables. Según Ochoa y Yunkor (2020) este método brinda información coherente bajo análisis de descripción.

Análisis inferencial, se estableció correlación Rho Spearman para analizar relación de variables, además con dicho estadígrafo se comprobó las hipótesis de la investigación, como también el nivel de incidencia entre las variables y dimensiones. De acuerdo a Ramírez y Polack (2020) este análisis realiza la compilación del comportamiento de los fenómenos para demostrar los supuestos planteados.

3.7. Aspectos éticos

Requiere que la ciencia lleve a principios éticos que garantice el avance del conocimiento y condición humana (Elizalde, Toapanta y Pomaquero, 2020).

-Principio de autonomía, porque la investigación aplicó la autonomía de la participación libre de los trabajadores en la recopilación de datos, respetando su forma de pensar.

-Principio de consentimiento informado, ya que se contó con la autorización del gerente municipal acerca de la recolección de datos, además se informó el proceso del encuestado.

-Principio de beneficencia, a través de la presente se brindó el beneficio científico del conocimiento para la presente y futura comunidad.

-Principio a la veracidad, porque los datos recolectados fueron verídicos y no alterados.

-Principio de justicia, ya que los datos obtenidos fueron aplicados de manera académica, también se respetó las autorías siendo sin plagio alguno con respaldo del turnitin.

-Por último, se basó en código ético RESOLUCIÓN DE CONSEJO UNIVERSITARIO N°062-2023 de la UCV.

IV. RESULTADOS

En esta sección se realizó el análisis descriptivo, obteniendo las frecuencias y porcentajes de variables con sus dimensiones, también se generó el análisis inferencial para responder los objetivos y probar las hipótesis establecidas en la investigación.

Análisis descriptivo

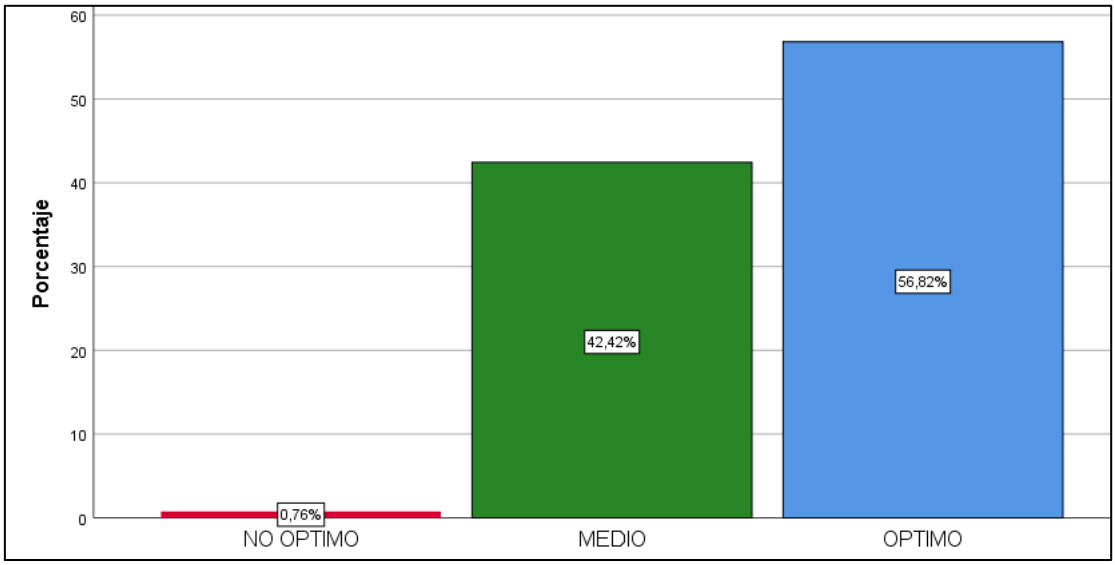
Tabla 1

Frecuencia de SGSI según ISO/IEC 27001:2022

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	1	,8	,8	,8
	MEDIO	56	42,4	42,4	43,2
	OPTIMO	75	56,8	56,8	100,0
	Total	132	100,0	100,0	

Figura 1.

Frecuencia de SGSI según ISO/IEC 27001:2022



Interpretación:

En la variable SGSI según ISO/IEC 27001:2022, el 0.8% de los trabajadores precisaron nivel no óptimo, 42.4% medio y 56.8% óptimo; entonces, la mayoría de trabajadores establecieron nivel óptimo al sistema de gestión de seguridad de información, puesto a que se cumple activamente con

procedimientos de protección de información mediante contraseñas y dispone controles contra el error humano en el procesamiento de la información.

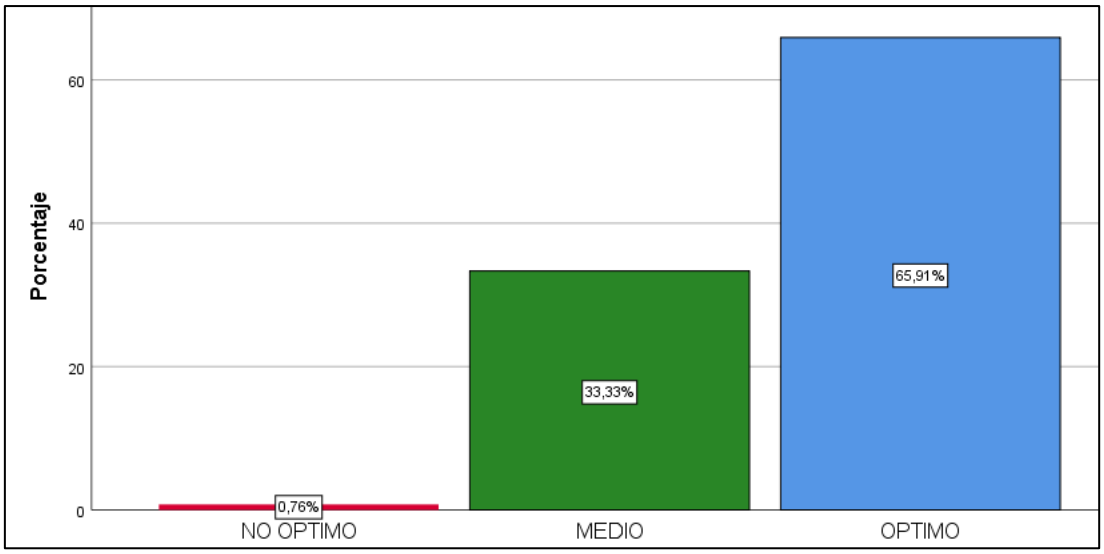
Tabla 2.

Frecuencia de Confidencialidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	1	,8	,8	,8
	MEDIO	44	33,3	33,3	34,1
	OPTIMO	87	65,9	65,9	100,0
	Total	132	100,0	100,0	

Figura 2.

Frecuencia de Confidencialidad



Interpretación:

En la dimensión confidencialidad del SGSI, el 0.8% de los trabajadores concretaron nivel no óptimo, 33.3% nivel medio y el 65.9% nivel óptimo; de tal manera, gran parte de los trabajadores establecieron nivel óptimo a la confidencialidad del SGSI, debido a que se usa técnicas como firma digital confidencial para validar documentos, también se varia constantemente las contraseñas de acceso a los aplicativos, como los accesos del área laboral que se encuentran resguardados.

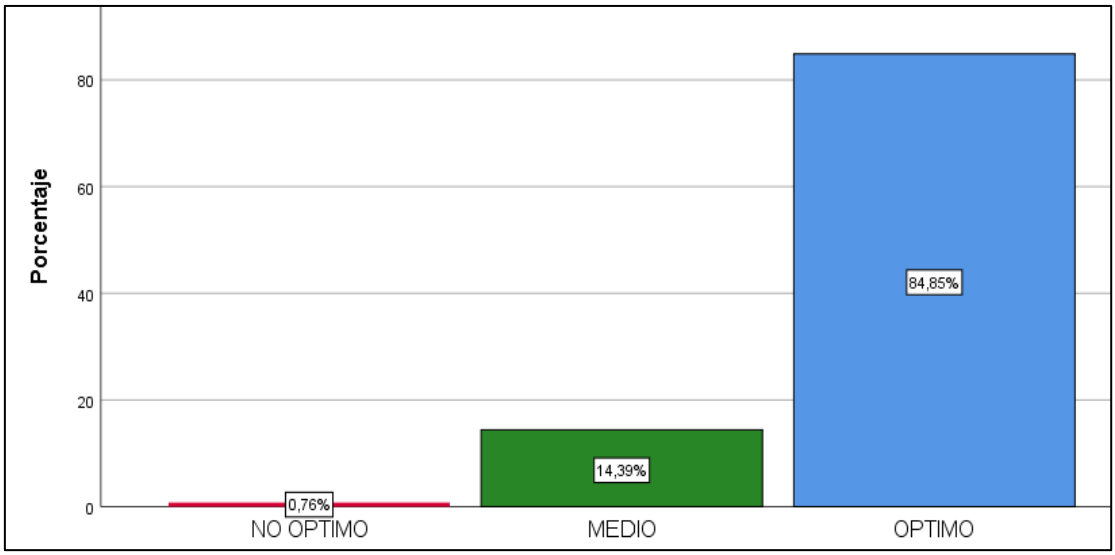
Tabla 3.

Frecuencia de Integridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	1	,8	,8	,8
	MEDIO	19	14,4	14,4	15,2
	OPTIMO	112	84,8	84,8	100,0
	Total	132	100,0	100,0	

Figura 3.

Frecuencia de Integridad



Interpretación:

En dimensión integridad del SGSI, el 0.8% de los trabajadores fijaron nivel no óptimo, 14.4% medio y 84.8% óptimo; de tal modo, la mayor parte de trabajadores ejecutaron nivel óptimo a la integridad del SGSI, porque se genera medidas preventivas frente impactos de virus informáticos, se gestiona backup de almacenamiento y copias de respaldo, además los trabajadores participan en auditorias fluidamente de sistema de información.

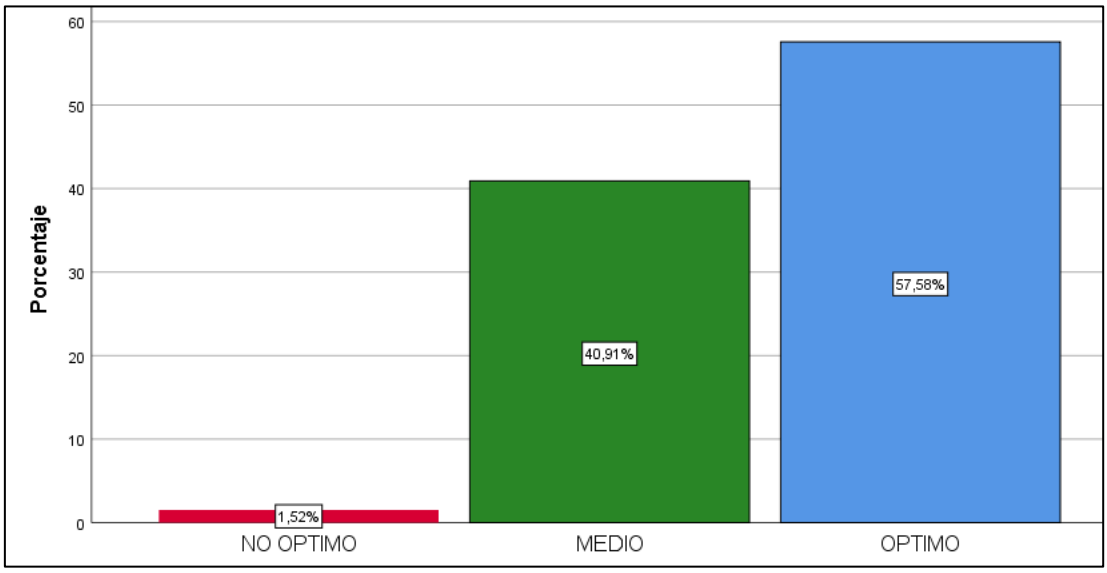
Tabla 4.

Frecuencia de Disponibilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	2	1,5	1,5	1,5
	MEDIO	54	40,9	40,9	42,4
	OPTIMO	76	57,6	57,6	100,0
	Total	132	100,0	100,0	

Figura 4.

Frecuencia de Disponibilidad



Interpretación:

En dimensión disponibilidad del SGSI, el 1.5% de los trabajadores fijaron nivel no óptimo, 40.9% nivel medio y otro 57.6% nivel óptimo; por lo tanto, la mayor multitud de trabajadores establecieron nivel óptimo a la disponibilidad del SGSI, por el motivo de que obtiene plan de contingencia para recuperar información en casos emergencia, asimismo existe un plan de soporte en los equipos informáticos para decepciones especializadas forestales y garantiza la velocidad de reacción de los marcos de datos.

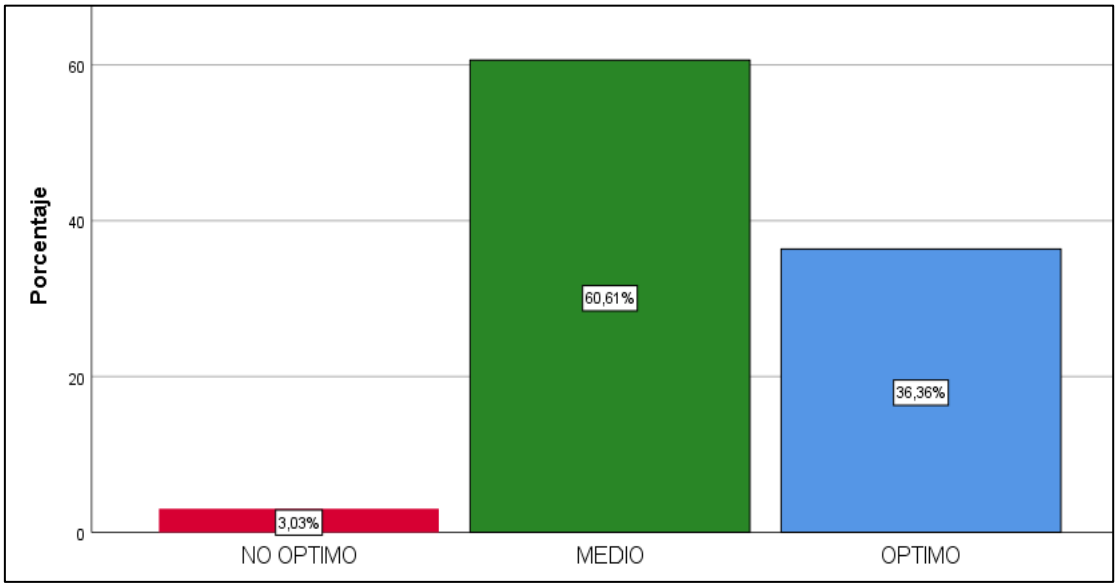
Tabla 5.

Frecuencia de Protección de información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	4	3,0	3,0	3,0
	MEDIO	80	60,6	60,6	63,6
	OPTIMO	48	36,4	36,4	100,0
	Total	132	100,0	100,0	

Figura 5.

Frecuencia de Protección de información



Interpretación:

En la variable protección de información, el 3% de los trabajadores precisaron nivel no óptimo, 60.6% medio y 36.4% óptimo; el cual, la mayoría de trabajadores establecieron nivel medio a la protección de información, debido a que la oficina tecnológica informática genera inspecciones fluidas de controles de seguridad, pero algunos casos se identifica deficiencia de seguridad por no minimizar la vulnerabilidad, es más cuentan con herramientas adecuadas para la seguridad.

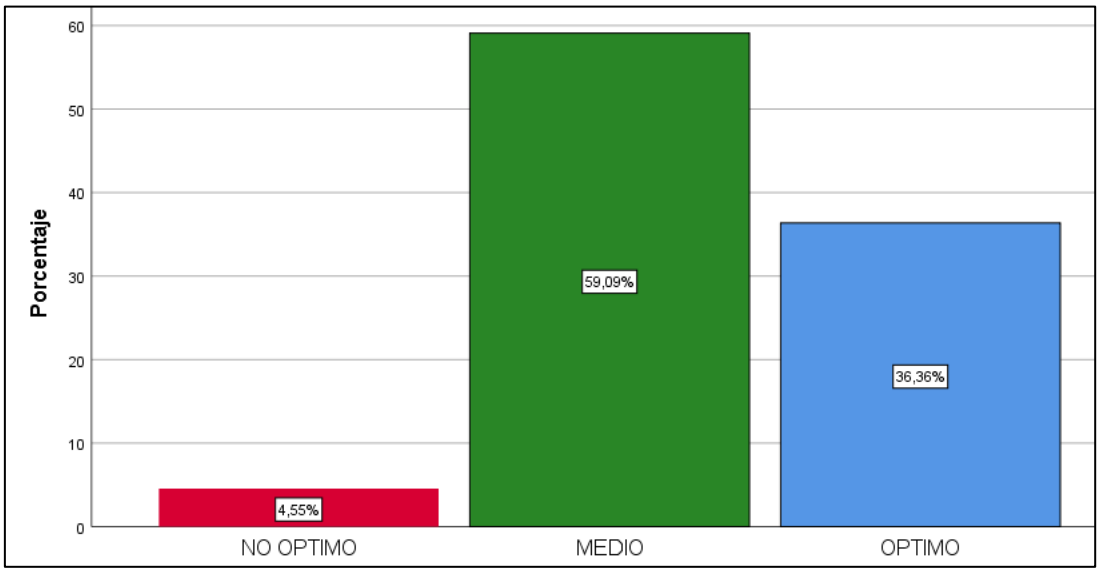
Tabla 6.

Frecuencia de Controles de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	6	4,5	4,5	4,5
	MEDIO	78	59,1	59,1	63,6
	OPTIMO	48	36,4	36,4	100,0
	Total	132	100,0	100,0	

Figura 6.

Frecuencia de Controles de seguridad



Interpretación:

En dimensión controles de seguridad, el 4.5% de los trabajadores fijaron nivel no óptimo, 59.1% nivel medio y 36.4% nivel óptimo; por lo tanto, la mayor multitud de trabajadores establecieron nivel medio a los controles de seguridad, por motivo de que solo en algunos casos la oficina tecnológica informática produce evaluaciones constantemente para analizar mejoras en controles de seguridad ejecutados, por otro lado, continuamente diseña mejoras que suman respuestas clave para los objetivos y cuenta con aparatos adecuados para proteger contra peligros externos y naturales con respecto a los datos.

.

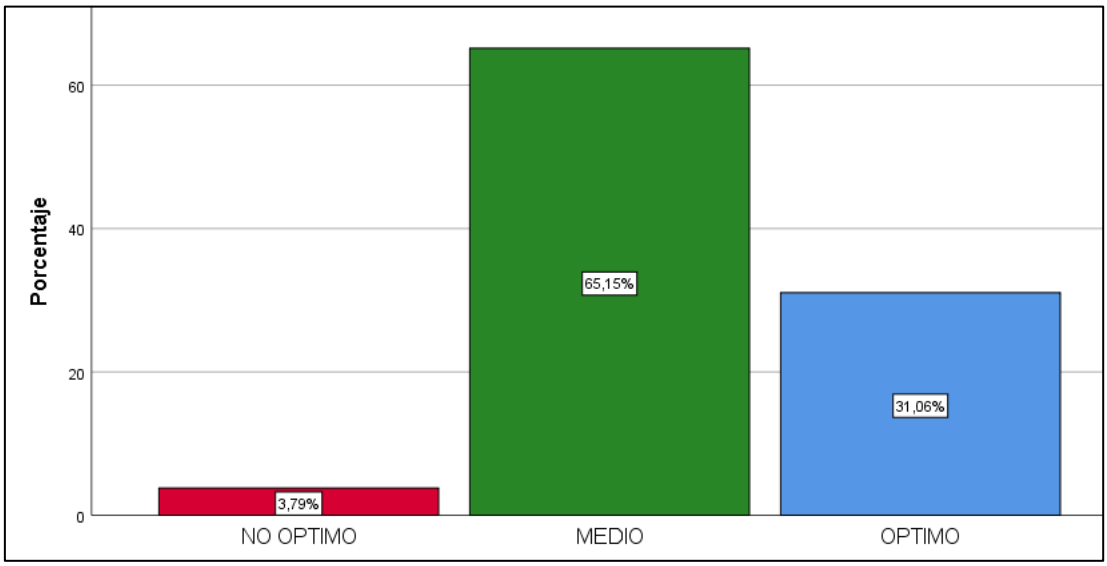
Tabla 7.

Frecuencia de Evaluación de riesgos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	5	3,8	3,8	3,8
	MEDIO	86	65,2	65,2	68,9
	OPTIMO	41	31,1	31,1	100,0
	Total	132	100,0	100,0	

Figura 7.

Frecuencia de Evaluación de riesgos



Interpretación:

En dimensión evaluación de riesgos, el 3.8% de los trabajadores detallaron nivel no óptimo, 65.2% nivel medio y 31.1% nivel óptimo; de tal modo, gran proporción de trabajadores fijaron nivel medio la evaluación de riesgos, ya que en ciertas circunstancias la oficina tecnológica informática no ha remediado lo suficiente las destacadas deficiencias de seguridad, sino que, en el lado positivo, aplica esfuerzos de seguridad para disminuir o moderar las posibilidades de seguridad de los datos. Además, cuando ocurre un episodio con beneficios de TI que impiden sus capacidades, se verifica. la adecuación de los esfuerzos de seguridad llevados a cabo centrándose en las posibilidades.

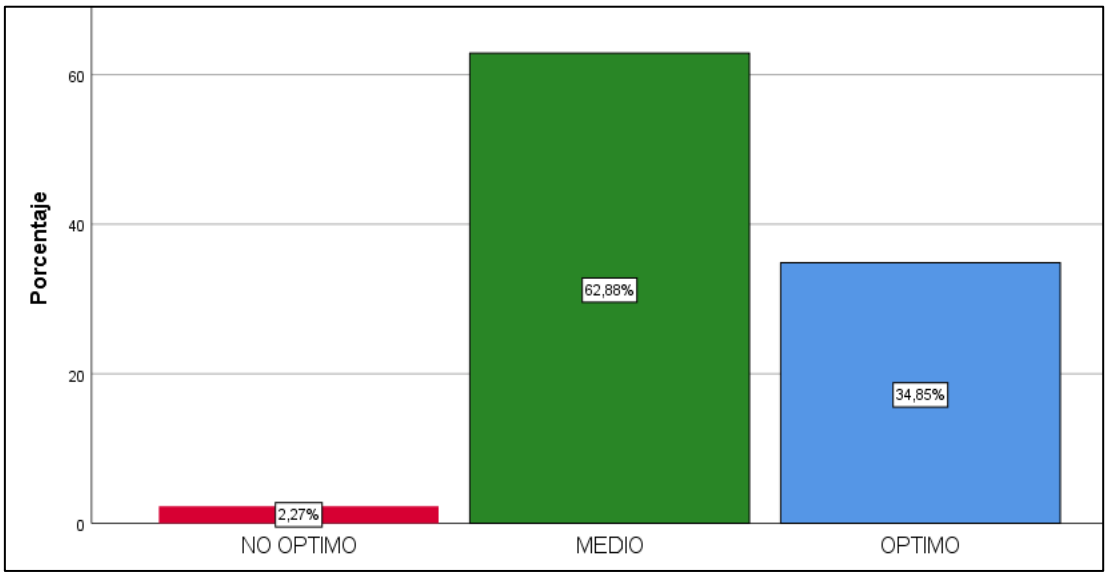
Tabla 8.

Frecuencia de Gestión de incidentes de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	NO OPTIMO	3	2,3	2,3	2,3
	MEDIO	83	62,9	62,9	65,2
	OPTIMO	46	34,8	34,8	100,0
	Total	132	100,0	100,0	

Figura 8.

Frecuencia de Gestión de incidentes de seguridad



Interpretación:

En dimensión gestión de incidentes de seguridad, el 2.3% de los trabajadores determinaron nivel no óptimo, 62.9% nivel medio y 34.8% nivel óptimo; por el cual, mayor parte de trabajadores fijaron nivel medio a la gestión de incidentes de seguridad, dado que la oficina de innovación de datos no realiza continuamente reproducciones de episodios de seguridad para evaluar la preparación y el límite de reacción, pero rastrea los incidentes de seguridad de los datos y los analiza para reconocer diseños, contar e informar episodios de seguridad de los datos y comprueba la seguridad de los esfuerzos realizados.

Análisis inferencial

En este punto se respondió los objetivos e hipótesis de investigación a través de la correlación Rho Spearman, a medida que la muestra son valores extremos, por ende, para hallar el nivel de influencia de la variable, se tomó en cuenta los siguientes criterios que se muestra a continuación:

Tabla 9.

Grado de Correlación

Rangos		**Relación**
r =	1	Perfecta
0,80	1	Muy alta
0,60	0,80	Alta
0,40	0,60	Moderada
0,20	0,40	Baja
0	0,20	Muy baja
r =	0	Nula

Nota: Bisquerra (2004) citado por Valdez et al. (2019).

Regla de decisión de hipótesis

Ho: ρ valor ≥ 0.05, se acepta la hipótesis nula.

Ha: ρ valor < 0.05, se rechaza la hipótesis nula.

OG: Determinar la incidencia SGSI según ISO/IEC 27001:2022 en la protección de información de una Municipalidad distrital, Lima 2023

H0: El SGSI según ISO/IEC 27001:2022 no incide significativamente en la protección de información de una Municipalidad distrital, Lima 2023.

HI: El SGSI según ISO/IEC 27001:2022 incide significativamente en la protección de información de una Municipalidad distrital, Lima 2023.

Tabla 10.

Correlación entre SGSI según ISO/IEC 27001:2022 y protección de información

			SGSI	PROTECCIÓN DE INFORMACIÓN
Rho Spearman	SGSI	Coeficiente de correlación	1,000	,611
		Sig. (bilateral)	.	,032
		N	132	132
	PROTECCIÓN DE INFORMACIÓN	Coeficiente de correlación	,611	1,000
		Sig. (bilateral)	,032	.
		N	132	132

Interpretación:

Se corroboró una correlación de 0.611 (incidencia alta) con significancia 0.032 < 0.05, de tal modo se rechazó hipótesis nula y se aceptó hipótesis alterna, determinando, el SGSI según ISO/IEC 27001:2022 incide significativamente en la protección de información de una Municipalidad distrital, Lima 2023, siendo así se demostró que al imponer una gestión de SGSI adecuada se obtiene un proceso seguro en la protección de datos.

OE1: Determinar la incidencia de la confidencialidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023

H0: La confidencialidad del SGSI no incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023

HI: La confidencialidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023

Tabla 11.

Correlación entre Confidencialidad del SGSI y protección de información

			CONFIDENCIALIDAD	PROTECCIÓN DE INFORMACIÓN
Rho Spearman	CONFIDENCIALIDAD	Coeficiente de correlación	1,000	,531
		Sig. (bilateral)	.	,008
		N	132	132
	PROTECCIÓN DE INFORMACIÓN	Coeficiente de correlación	,531	1,000
		Sig. (bilateral)	,008	.
		N	132	132

Interpretación:

Se evaluó una correlación de 0.531 (incidencia moderada) con significancia 0.008 < 0.05, por ello, se rechazó hipótesis nula y se aceptó hipótesis alterna, precisando, la confidencialidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023, esto da entender que el SGSI brinda una confidencialidad conforme, no colocando a disposición de nadie, salvo que sea autorizado, de tal modo revela que hay una alta protección de datos en la municipalidad.

OE2: Determinar la incidencia de la integridad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023

H0: La integridad del SGSI no incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023

HI: La integridad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023

Tabla 12.

Correlación entre Integridad del SGSI y protección de información

			INTEGRIDAD	PROTECCIÓN DE INFORMACIÓN
Rho Spearman	INTEGRIDAD	Coeficiente de correlación	1,000	,757
		Sig. (bilateral)	.	,003
		N	132	132
	PROTECCIÓN DE INFORMACIÓN	Coeficiente de correlación	,757	1,000
		Sig. (bilateral)	,003	.
		N	132	132

Interpretación:

Se analizó una correlación de 0.757 (incidencia alta) con significancia 0.003 < 0.05, por ende, se rechazó hipótesis nula y se aceptó hipótesis alterna, especificando, la integridad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023, esto demuestra el SGSI establece una alta integridad generando garantía en sus bases de datos que dispone, además de prevenir a cualquier cambio no autorizado.

OE3: Determinar la incidencia de la disponibilidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023

H0: La disponibilidad del SGSI no incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023

HI: La disponibilidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023

Tabla 13.

Correlación entre disponibilidad del SGSI y protección de información

			DIPONIBILIDAD	PROTECCIÓN DE INFORMACIÓN
Rho Spearman	DIPONIBILIDAD	Coeficiente de correlación	1,000	,579
		Sig. (bilateral)	.	,001
		N	132	132
	PROTECCIÓN DE INFORMACIÓN	Coeficiente de correlación	,579	1,000
		Sig. (bilateral)	,001	.
		N	132	132

Interpretación:

Se concretó una correlación de 0.579 (incidencia moderada) con significancia 0.001 < 0.05, por ende, se rechazó hipótesis nula y se aceptó hipótesis alterna, comprobando, la disponibilidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023, dado a que el SGSI ofrece una disponibilidad alta a usuarios autorizados acerca del proceso de información, mostrando garantía en la protección de los datos.

V. DISCUSIÓN

En esta sección se confrontó los hallazgos encontrados en la investigación con los hallazgos de los trabajos previos, con el fin de demostrar las semejanzas que se obtuvo al tener respuesta de los objetivos

En el objetivo general, se determinó que gran parte de los trabajadores precisaron al SGSI según ISO/IEC 27001:2022 en nivel óptimo, por otro lado, precisaron en nivel medio a la protección de información, en cuanto a la relación se decretó 0.611 incidencia alta con significancia 0.032 < 0.05, de tal manera, el SGSI según ISO/IEC 27001:2022 incide significativamente en la protección de información de una Municipalidad distrital, Lima 2023, siendo así se demostró que al imponer una gestión de SGSI adecuada se obtiene un proceso seguro en la protección de datos.

Estos hallazgos fueron congruentes con la investigación de Cuenca (2023) en una municipalidad de Lima, demostró que el SGSI y la protección de datos tuvieron correlación de 0.713 con significancia 0.000, además el SGSI fue nivel alto y la protección de datos fue nivel moderado, así pues, hubo influencia significativa entre SGSI ISO/IEC 27001: 2013 y protección de datos en una municipalidad de Lima. Asimismo, fue similar con el estudio de Correa (2023) en el gobierno Cantón Naranjal de Ecuador, tuvo una correlación 0.775 incidencia alta con significancia 0.003 < 0.05, también detalló nivel alto al SGSI y a la protección de datos, de manera que los controles del SGSI influyeron en la protección de la información del gobierno Cantón Naranjal.

Esta incidencia alta encontrada en la investigación y en los trabajos previos entre SGSI y protección de datos, demuestran que se cumple activamente con procedimientos de protección de información mediante contraseñas y dispone controles contra el error humano en el procesamiento de la información, es más se genera inspecciones fluidas de controles de seguridad con eficiencia en minimizar la vulnerabilidad y cuentan con herramientas adecuadas para la seguridad, este fundamento concuerda con la teoría de Bustamante et al. (2021), el SGSI evalúa los riesgos relacionados con los activos de información que se gestionan dentro de una organización a través de la norma ISO 27001 que requiere un SGSI como componente necesario con el respaldo

de los tres pilares de disponibilidad, integridad y confidencialidad de la información. Además, el SGSI en relación a la protección de información es fundamental para la toma de decisiones a nivel estratégico, táctico y operativo en diversas áreas funcionales del municipio, el cual actúa como herramienta poderosa para respaldar los procesos desarrollados y apoya todas las actividades que se realizan contribuyendo en el procesamiento de datos para generar información confidencial, integro y disponible en la utilidad de toma de decisiones de gestión (Vargas, et al., 2019)

En el primer objetivo específico, se estimó que la mayoría de trabajadores concretaron nivel óptimo a la confidencialidad del SGSI con correlación 0.531 incidencia moderada y significancia 0.008 < 0.05, por ello, la confidencialidad del SGSI incidió significativamente en la protección de información de una Municipalidad Distrital, Lima 2023, en tal sentido, el SGSI brindó una confidencialidad conforme, no colocando a disposición de nadie, salvo que sea autorizado, revelando que hay una alta protección de datos en la municipalidad.

Estos resultados fueron semejantes con la investigación de Guacanés y Vilatuña (2022) ejecutada en Colombia, evaluó un nivel alto en la confidencialidad de los datos con correlación 0.640 incidencia moderada y significancia 0.000, entonces la confidencialidad del sistema de gestión de seguridad de información incidió significativamente en la protección de datos. Del mismo modo, en la indagación de Guevara (2019) realizada en Ecuador, mostró que la confidencialidad se encontraba en nivel alto con correlación 0.540 incidencia moderada y significancia 0.000 < 0.05, estableciendo que la confidencialidad del SGSI ISO/IEC 27001 influyó significativamente en la protección de datos.

Esta incidencia moderada entre la confidencialidad y la protección de datos que se encontró en los análisis, da razón a que se usó técnicas como firma digital confidencial para validar documentos, también se varia constantemente las contraseñas de acceso a los aplicativos, como los accesos del área laboral que se encuentran resguardados, esto se respalda con De La Rosa (2021) la confidencialidad salvaguarda la protección de datos e información recabada, garantizando que solo las personas u organizaciones autorizadas tengan acceso

a la misma y que no se compartirá sin consentimiento, los esfuerzos de seguridad de datos deben garantizar que el secreto de la información no se ponga en peligro, en el mismo contexto Tonysé (2021) garantiza el proceso y almacenamiento de datos a mantenerse lo más secreto posible para evitar la divulgación no autorizada.

En el segundo objetivo específico, la mayor multitud de los trabajadores ejecutaron nivel óptimo a la integridad del SGSI con correlación 0.757 incidencia alta y significancia 0.003 < 0.05, por ende, la integridad del SGSI incidió significativamente en la protección de información de una Municipalidad Distrital, Lima 2023, ante ello, se infiere que el SGSI establece una alta integridad generando garantía en sus bases de datos que dispone, además de prevenir a cualquier cambio no autorizado.

Estos análisis fueron concordantes con la investigación de Castro (2022) quien evaluó la relación de seguridad de información y gestión del riesgo en una entidad del sistema electoral, donde se encontró a la integridad del SGSI en nivel alto con correlación 0.495 y significancia 0.000, declarando que la integridad del SGSI incidió positivamente con la protección de datos en una entidad del sistema electoral. En el mismo sentido el estudio de Ticona (2022) realizado en Arequipa en la entidad Severox Perú S.A.C., decretó que la integridad del SGSI fue nivel óptimo con significancia 0.000 y correlación 0.721 incidencia alta, por consiguiente, la integridad de la seguridad de información basado en ISO/IEC 27001:2013 incidió significativamente en la protección de datos de Severox Perú S.A.C.

Esta incidencia alta corroborada entre la integridad del SGSI y la protección de datos, da consecuencia a que se genera medidas preventivas frente impactos de virus informáticos, se gestiona backup de almacenamiento y copias de respaldo, además los trabajadores participan en auditorias fluidamente de sistema de información; dicha manifestación se infiere con Panaqué, Lizárraga y Mendoza (2021) cuando los datos se transfieren o almacenan, su integridad garantiza que no hayan sido alterados, perdidos o destruidos, ya sea intencionalmente o no, a su vez De La Rosa (2021) en cuanto a la integridad del

SGSI, mencionó que la información debe estar garantizada por los sistemas que la gestionan, lo que significa que debe mostrarse exactamente como fue diseñada, sin alteraciones o manipulaciones que no hayan sido expresamente autorizadas con protocolos y técnicas para reducir riesgos.

En el tercer objetivo específico, el mayor grupo de trabadores fijaron nivel óptimo a la disponibilidad del SGSI con correlación 0.579 incidencia moderada y significancia 0.001 < 0.05, total que, la disponibilidad del SGSI incidió significativamente en la protección de información de una Municipalidad Distrital, Lima 2023, a causa de que el SGSI ofrece una disponibilidad alta a usuarios autorizados acerca del proceso de información, mostrando garantía en la protección de los datos.

Estos resultados fueron similares con la indagación de Espinoza y Mendoza (2022) elaborado en Lima, determinaron que la disponibilidad del SGSI se encontraba en nivel alto con significancia 0.001 < 0.005 y correlación 0.540 incidencia moderada, por eso la confidencialidad del SGSI inciden significativamente en la protección de información en PYMES de Lima. De igual manera, la investigación de Torres y Chicaiza (2020) realizado en Ecuador, estimó la aplicación de modelo de SGSI en la entidad Megaprofer S.A, antes de la aplicación, la disponibilidad de información se encontraba en nivel casi moderado, después de establecer el SGSI, la disponibilidad de información fue nivel óptimo con significancia 0.033 < 0.050, precisando que la disponibilidad del SGSI incidió significativamente en la protección de datos en la entidad Megaprofer S.A.

Esta incidencia moderada entre la disponibilidad del SGSI y la protección de datos, da efecto a que se obtiene un plan de contingencia para recuperar información en casos emergencia, asimismo existe un plan de soporte en los equipos informáticos para decepciones especializadas forestales y garantiza la velocidad de reacción de los marcos de datos; así como puntualizó Duval, Delgado, Mendoza (2022) el principio esencial de seguridad de información, es disponibilidad de información o activos de información que garantiza acceso rápido y confiable a los datos y recursos por parte de individuos autorizados que

cuenten con credenciales requeridas, asimismo De La Rosa (2021) pormenorizó que la disponibilidad garantiza que todas las personas u organizaciones con derechos de acceso siempre puedan acceder a la información. Para esto, debe haber medidas de soporte y seguridad que puedan acceder a los datos según sea necesario y que protejan contra las interrupciones del servicio.

Todo ello, la correlación causal que se muestra entre las variables y dimensiones es de manera significativa y positiva, dando entender que el SGSI incide satisfactoriamente en la protección de información, por lo que en la presente municipalidad se está protegiendo y preservando la información generada por procesos que se ejecutan interiormente, además previene pérdidas potenciales debido a amenazas ocultas en el entorno, como acceso no autorizado accidental o intencional y degradación de calidad de la información que se obtiene.

Asimismo, los antecedentes recopilados contrastaron con la investigación contribuyendo con resultados similares enfocados en el mismo objetivo, lo cual se pudo decretar que el SGSI incide en la protección de información, expresando que la confidencialidad, integridad y disponibilidad disponen de procesos de seguridad. También, dicha investigación generó como aporte conocimientos y producción de ideas que se puede retomar en futuras investigaciones, así como soluciones prácticas.

Por otro lado, los análisis encontrados en la investigación se respaldan con las teorías del SGSI, como en el caso de la teoría general de la gestión del sistema de seguridad puesta en marcha por Ludwing Von Bertalanffy, fomentó que es el sistema colectivo para la toma de decisiones de manera concreta y fácil, cuyo enfoque es examinar los riesgos de una organización asociados a los datos que se manipulan para un bien común (Bustamante et al. 2021), en la misma línea, López (2019) el diagnóstico, la memoria, mantenimiento, toma de decisiones y la operación son algunas de la Teoría General de Sistemas y su perspectiva funcional con un nivel inicial que incluye política de Sistema de seguridad para la Gestión, incluyendo elementos de planificación, asignación, comunicación, retroalimentación, evaluación y medición.

También fueron respaldados por la teoría de Protección de la información, también llamada seguridad de información se basa en el acceso, la utilización, divulgación o destrucción no autorizada del sistema de una empresa que ha evolucionado considerablemente y dispone de la planificación de la continuidad para mantener los controles, programas y políticas bajo una confidencialidad y disponibilidad de los datos (Meraz, 2018), en el mismo contexto Parada, Gómez y Flores (2018) la seguridad de datos alude a la disposición de enfoques, métodos y dispositivos utilizados para cumplir, proteger y garantizar que ningún dato salga del sistema que la organización ha configurado. Es un componente crucial para que las empresas operen porque los datos que administran son cruciales para el trabajo que realizan.

La investigación expresó como límites al tamaño de la población distribuyéndose por un margen de error de 5% siendo así una muestra menor del total para la medición, puesto que puede afectar en la variabilidad de ponderaciones, precisión en los resultados y capacidad de los patrones; ya que a medida que se incrementa la muestra, el margen de error va a disminuir, en otra parte, la limitación del factor tiempo en el procedimiento de la recolección de datos que se tuvo un día en 20 minutos, puede que, por el escaso de tiempo que respondieron los trabajadores hayan retrucado las puntuaciones, lo cual puede generar en los resultados menor fiabilidad y consistencia.

VI. CONCLUSIONES

1. Se determinó una alta incidencia del SGSI según ISO/IEC 27001:2022 en la protección de información de una Municipalidad distrital, Lima 2023 con una correlación de 0.611 y significancia 0.032, en vista de que se cumple activamente con procedimientos de protección de información mediante contraseñas y herramientas adecuadas, además dispone controles contra el error humano en el procesamiento de la información.

2. Se estimó una incidencia moderada de la confidencialidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023 con una correlación 0.531 y significancia 0.008, teniendo en cuenta que se varia constantemente las contraseñas de acceso a los aplicativos y se usa técnicas como firma digital confidencial para validar documentos.

3. Se valoró una incidencia alta de la integridad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023 con una correlación 0.757 y significancia 0.003, debido a que se genera medidas preventivas frente impactos de virus informáticos y los trabajadores participan en auditorias fluidamente de sistema de información.

4. Se evaluó una incidencia moderada de la disponibilidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023, con una correlación 0.579 y significancia 0.001, puesto a que se obtiene un plan de contingencia para recuperar información en casos emergencia y garantiza la velocidad de reacción de los marcos de datos como también pueden disponer solo personas autorizadas.

VII. RECOMENDACIONES

1. Se recomienda monitorear los controles de seguridad de la información establecidos y contar con un plan integral de gestión de riesgos para continuar manteniendo estos niveles positivos, además, el gerente municipal debe establecer actividades de control y seguir utilizando la seguridad como base metodológica para capacitar y educar a los empleados en temas de seguridad de información y protección de datos ante riesgos, así como invertir en tecnología, ya que los ciberataques son el riesgo más potencial en la actualidad.

2. Es fundamental que en la municipalidad se use firmas digitales criptográfica en los documentos generados en los procesos, lo que mejora el acceso al entorno físico, ahorrará tiempo en papeleo, mano de obra directa y el uso de terceros, además esto apoyará en prevenir la divulgación de datos no autorizados.

3. Es necesario seguir realizando seguimiento continuo de las actividades planificadas en la municipalidad de acuerdo con la certificación según la norma de seguridad de la información ISO 27001, asimismo realizar prácticas en unidades estructurales con certificación ISO para compartir experiencias e incrementar la seguridad y gestión de riesgos, involucrando al personal interno y externo, auditorías externas.

4. El acceso a la información de los servicios clave debe ser virtual para evitar la continuidad o interrupción del proceso, para ello, deberá darse prioridad a la sistematización de sus actividades, lo que permitirá ahorrar documentos, autorizaciones y profesionalización de los empleados.

5. Se sugiere al jefe de informática que adicionalmente contrate un software integral de seguridad en la municipalidad, que obtenga paquetes de antivirus, antimalware, firewall, entre otras, lo cual permita proteger la información ante ataques externos, asimismo realizar copias de seguridad periódicamente.

6. La gerencia municipal tiene que fijar protocolos de permiso, teniendo en cuenta al menos cuatro criterios: Quién tendrá acceso y permiso para la edición de datos; quién va consultar las carpetas, pero no modificarlas; quien tendrá acceso mixto y por último quien solo va a establecer o depositar información, sin tener a ningún acceso más.

REFERENCIAS

Abrego, D., Sánchez, Y. y Medina, J. (2018). Influencia de los sistemas de información en los resultados organizacionales. *Contaduría y administración,* 62 (2). https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S018610422017000200303

Aguilar. J. G. (2021). Web system based on the Queuing Theory for customer service in a municipality in Peru. *CICIC 2021 - Undecima Conferencia Iberoamericana de Complejidad, Informatica y Cibernetica, Memorias,* 65-70. https://www.scopus.com/inward/record.uri?eid=2s2.085106063679&partnerID=40&md5=ab6e328d54f0be2c1d7d434acf9b92e9

Álvarez, A. (2020). Justificación de la Investigación. Nota académica, 8(4): 3. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10821/Nota%20Acad%C3%A9mica%205%20%2818.04.2021%29%20%20Justificaci%C3%B3n%20de%20la%20Investigaci%C3%B3n.pdf?sequence=4&isAllowed=y

Arias, J. (2021). Diseño y metodología de investigación. ENFOQUES CONSULTING: 133. ISBN: 9786124844423. https://www.researchgate.net/publication/361375510_Metodologia_de_la_Investigacion_El_metodo_ARIAS_para_hacer_el_proyecto_de_tesis

Arcos, M., Matute, K. y Fernández, M. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. *Revista Ibérica de Sistemas e Tecnologías de Información*, 5(60), 100-114. https://www.proquest.com/docview/2865402056/46D2BDD0427C4937PQ/7?sourcetype=Scholarly%20Journals

Baca, L., De La Vega, C., Corredor, C., Diaz, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, 8 (3), 1-11.

https://www.proquest.com/docview/2468684801/27EDA1A2C5214587PQ/37?sourcetype=Scholarly%20Journals

Bustamante, S., Valles, M., Cuellar, I. y Levano, D. (2021). Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, 12(2), pp. 69-79. http://scielo.senescyt.gob.ec/pdf/enfoqueute/v12n2/13906542enfoqueute-12-02-00069.pdf

Castro, H (2022). Seguridad de la Información y Gestión del Riesgo en una Entidad del Sistema Electoral, año 2021. [Tesis posgrado, Universidad César Vallejo]. Ingeniero de sistemas. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/77870/Castro_RH-SD.pdf?sequence=1&isAllowed=y

Castillo, G. y Pérez, E. (2018). Diagnóstico de los sistemas de información en las empresas priorizadas según los requerimientos actuales. *Humanidades y Ciencias de la Educación,* 6 (2), 1-11. https://www.redalyc.org/pdf/3505/350550884007.pdf

Correa, M. (2023). *Modelo de sistema de gestión de seguridad de la información, para establecer controles basados en la norma ISO/IEC 27001:2013 mediante el código de prácticas de seguridad de la información ISO/IEC 27002:2022 en el departamento de tecnologías de la información del gobierno autónomo descentralizado municipal del Cantón Naranjal*. [Tesis posgrado, Universidad Estatal del Milagro]. Ingeniero de sistemas. https://repositorio.unemi.edu.ec/bitstream/123456789/6971/1/ALEX%20AVILA%20COELLO.pdf

Coronel, I. y Quirumbay, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *RCTU*, 9 (2), 97-109. http://scielo.senescyt.gob.ec/scielo.php?script=sci_abstract&pid=S1390-76972022000100097&lng=es&nrm=iso

Cortés, M., Mur, N., Iglesias, M., Cortés, M. (2020). Algunas consideraciones para el cálculo del tamaño muestral en investigaciones de las Ciencias

Médicas**.** *Revista Medisur*, 18(5). http://scielo.sld.cu/pdf/ms/v18n5/1727-897X-ms-18-05-937.pdf

Cuenca, N. (2023). *SGSI según ISO/IEC 27001:2013 para el Control de Activos de TI en una empresa privada de Outsourcing, Lima 2023.* [Tesis posgrado, Universidad César Vallejo]. Ingeniero de sistemas. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/109516/Cuenca_NEE-SD.pdf?sequence=1&isAllowed=y

Delgado, J. (2021). La investigación científica: su importancia en la formación de investigadores. *Ciencia Latina Revista científica Multidisciplinar*, 5 (3). https://ciencialatina.org/index.php/cienciala/article/view/476/585

De La Cruz, P. (2020). El hipotético-deductivismo en la explicación de las ciencias sociales. *Horizonte de la Ciencia*, 10(18). https://www.redalyc.org/journal/5709/570968990003/570968990003.pdf

De La Rosa, T. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, 13(5), 495-506. http://scielo.sld.cu/pdf/rus/v13n5/2218-3620-rus-13-05-495.pdf

Duval, E., Delgado, J. y Mendoza, A. (2022). Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001. *Revista de investigación de sistemas e informática* 15(1): 113-126. DOI: https://doi.org/10.15381/risi.v15i1.23362

Elizalde, Y., Toapanta, C. y Pomaquero, J. (2020). Importancia y relevancia de la ética en la investigación. *Imaginario Social*, 3 (2). http://www.revista-imaginariosocial.com/index.php/es/article/view/4/7

Espinoza, F. y Mendoza, R. (2022). *Método de seguridad de la información basada en la ISO 27001 para el seguimiento y control de vulnerabilidades en Pymes* [Tesis posgrado, Universidad César Vallejo]. Ingeniero de sistemas. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/93135/Huaman_EFL-Ipanaque_MR-SD.pdf?sequence=1

Escofet, A., Folgueiras, P., Luna, E. & Palou, B. (2016). Elaboration and Validation of a Questionnaire for the Evaluation of Service-Learning Projects, *Revista mexicana de investigación educativa*, 21 (70). http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S140566662016000300929

Fernández, V. (2020). Tipos de justificación científica. *Espíritu Emprendedor TES*, 4(3): 65-76. https://www.espirituemprendedortes.com/index.php/revista/article/view/207/275

Fernández, R., Avello, R., Sánchez, S. & Quintana, M. (2019). Validation of instruments as a guarantee of credibility in scientific research. *Revista cubana de ciencias*, 48 (2). http://www.revmedmilitar.sld.cu/index.php/mil/article/view/390/331

Flores Ccanto F., Ramos Vera P.P., Ramos Vera F., Ramos Vera A.M. (2019). Gestión de innovación tecnológica y globalización como factores impulsadores de la calidad de servicio y competitividad. *Revista Venezolana Gerencia*, 24 (88). https://www.scopus.com/inward/record.uri?eid=2s2.085083571700&partnerID=40&md5=0659636ff58565f3abf1d2a166ec16be

Fong, N. y Bayona, S. (2022). Consideraciones para el Cumplimiento de la Política de Seguridad de la Información. *Revista Ibérica de Sistemas e Tecnologías de Información*, 2(51), 528-539. https://www.proquest.com/docview/2735285199/27EDA1A2C5214587PQ/36?sourcetype=Scholarly%20Journals

Guerra, E., Neira, H. y Diaz, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información Tecnológica,* 32(5). https://www.scielo.cl/pdf/infotec/v32n5/0718-0764-infotec-32-05-145.pdf

González, D., Alvarado, C. & Marín, C, (2018). Design and Validation of a Survey for the Characterization of Goat Production Units. *Revista de la Facultad*

de Ciencias Veterinarias, 58 (2). http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S02586576201700 0200003

Guerrero, V. (2022). Quantitative approach: taxonomy from the depth level of the search for knowledge. *Revista Llalliq*; 2 (1). http://revistas.unasam.edu.pe/index.php/llalliq/article/view/936/997

Guacanés y Vilatuña (2022). *Propuesta de diseño de un SGSI basado en la norma ISO/IEC 27001. Caso de estudio la empresa Ultralink*. [Tesis pregrado, Universidad Politécnica Nacional]. Ingeniero de sistemas. https://bibdigital.epn.edu.ec/handle/15000/22812

Guevara, R. (2019). Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de tecnologías de la información y comunicación del distrito 18d01 de Educación. [Tesis pregrado, Universidad Técnica de Ambato]. Ingeniero de sistemas. https://repositorio.uta.edu.ec/handle/123456789/26932

Guevara, E., Delgado, J., y Mendoza, A. (2022). Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001. *Investigación de sistemas e informática*, 15(1), 113-126. https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/ 23362/18739

Hernández, R. y Mendoza, C. (2018). Metodología de investigación: Las turas cuantitativa, cualitativa y mixta. México: Mc Graw Interamericana Editores. https://ebookcentral.proquest.com/lib/upnpe/reader.action?docID=54858 14&query=metodolog%C3%ADa+de+la+investigaci%C3%B3n+#

ISO 27001 (2022). Gestión de la seguridad de la información. https://www.normas-iso.com/iso-27001/

Jiménez, G. y López, D. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. Revista Ibérica de Sistemas e Tecnologías de Información, 3(62), 16-31. https://www.proquest.com/docview/2880949554/46D2BDD0427C4937P Q/10?sourcetype=Scholarly%20Journals

López, F. (2019). *Sistema de Gestión de Seguridad de la Información*. Logopolis. https://logopoliskpo.com/2019/06/07/sistema-de-gestion-de-seguridad-de-la-informacion/

Mahecha, N., Gómez, L., Moreno, I., Londoño, C., Camacho, H. (2023). Sistemas integrados de gestión. *Revista SIGNOS*, 15(2), 1-30. https://www.proquest.com/docview/2854527607/27EDA1A2C5214587PQ/35?sourcetype=Scholarly%20Journals

Marlon, D. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*, 21 (2). https://www.redalyc.org/journal/6378/637869113010/html/

Márquez, H., Zurita, J. & Miranda, G. (2018). The research protocol VII. Validity and reliability of measurements. *Artículo Alerg. Mexico*, 65 (4): 414-421. http://www.scielo.org.mx/pdf/ram/v65n4/2448-9190-ram-65-04-414.pdf

Mejía, J., Agudelo, A., Rivas, M., Delgado, I. (2023). Método para Gestionar la Seguridad de activos de Información. Revista Ibérica de Sistemas e Tecnologías de Información, 2(62), 252-266. https://www.proquest.com/docview/2880950430/46D2BDD0427C4937PQ/11?sourcetype=Scholarly%20Journals

Meraz, A. (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. *Revista del instituto de ciencias jurídicas de puebla*, 12 (41), 293-310. https://www.scielo.org.mx/pdf/rius/v12n41/1870-2147-rius-12-41-293.pdf

Ochoa, J. & Yunkor, Y., (2020). The descriptive study in scientific research. *Peruvian legal act. Scientific article*, (2) 2 http://revistas.autonoma.edu.pe/index.php/AJP/article/view/224/191

Panaqué, J., Lizárraga, Y. y Mendoza, A. (2021). Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones. *Perfiles de ingeniería*, 18(20), 67-76. DOI: https://doi.org/10.31381/perfiles_ingenieria.v18i18.5399

Parada, D., Gómez, U y Flores, A. (2018). Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. *Información tecnológica*, 29 (1). https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071807642018000100027

Peris. J. (2023). La importancia de un Sistema de Gestión de Seguridad de la Información. *Artículo Service Managment.* https://news.itsmf.es/la-importancia-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

Quispe, A., Pinto, D., Huamán, M., Bueno, G., Valle, A. (2020). Metodologías cuantitativas: Cálculo del tamaño de muestra con STATA y R. *Revista del Cuerpo Médico Hospital Nacional Almanzor Aguinaga Asenjo*, 13(1). http://www.scielo.org.pe/pdf/rcmhnaaa/v13n1/2227-4731-rcmhnaaa1301-78.pdf

Ramírez, E. y Rinconc, M. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista Ibérica de Sistemas y Tecnologías de Información*, 46(6), 13pp. https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

Ramírez, A. & Polack, A. (2020). Inferential statistics. Choice of a non-parametric statistical test in scientific research*. Horizon of Science*, 10 (19) 191-208. https://www.redalyc.org/journal/5709/570962992015/html/

Ramos, C. (2020). The scope of an investigation. *Revista Ciencia América*, 9 (3), 1-6. https://dialnet.unirioja.es/servlet/articulo?codigo=7746475

Rodríguez, L., Cruzado, C., Mejía, C. y Alarcón, M. Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, 8 (3). http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Romero, L. (2020). Importance of the Materials and Methods section. *Communicate magazine*, (24) no. 4. https://www.revistacomunicar.com/wp/escuela-de-autores/importancia-de-la-seccion-materiales-y-metodos-en-los-articulos cientificos/

Shojaie, B. (2018). Implementation of information security management systems based on the ISOIEC 27001 standard in different cultures (Doctoral dissertation, Staats-und Universitätsbibliothek Hamburg Carl von Ossietzky). https://ediss.sub.uni-hamburg.de/handle/ediss/7572

Ticona, O. (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. [Tesis pregrado, Universidad César Vallejo]. Ingeniero de sistemas. https://repositorio.ucv.edu.pe/handle/20.500.12692/88248

Tonysé, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001**.** *Revista Universidad y Sociedad*, 13 (5), 495-506. http://scielo.sld.cu/pdf/rus/v13n5/2218-3620-rus-13-05-495.pdf

Torres, C. y Chicaiza, D. (2020). *Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* [Tesis pregrado, Universidad Politécnica Nacional]. Ingeniero de sistemas. https://repositorio.uta.edu.ec/handle/123456789/30690

Valdez, R., Fernández, R., León, M., Simón, N., Álvarez, D. (2019). Análisis de la rugosidad superficial de diferentes maderas en las provincias de Pinar del Río y Artemisa, Cuba. *Revista Cubana de Ciencias Forestales*, 7(1) 1-16. http://scielo.sld.cu/pdf/cfp/v7n1/2310-3469-cfp-7-01-1.pdf

Vargas Encalada E.E., Rengifo Lozano R.A., Guizado Oscco F., Sánchez Aguirre F.D.M. (2019). Information system as a tool to reorganize manufacturing processes. Revista Venezolana de Gerencia, 24 (89). https://www.scopus.com/inward/record.uri?eid=2s2.085068045823&partnerID=40&md5=0ee0b82145eef91809b172efcc5b37db

Vásquez, L. (2018). Sistema integrado de gestión de monitoreo de riesgos más allá de las ISO. *Revista SIGNOS*, 10(2), 25-40. https://www.proquest.com/docview/2482239488/46D2BDD0427C4937PQ/15?sourcetype=Scholarly%20Journals

Villalba, K. y Donado, S. (2022). Pasos para diseñar un modelo de madurez con marco de trabajo ágil para la implementación a sistemas de gestión de la seguridad de TI alineado a las políticas de gobierno colombiano para el sector público. *Revista Ibérica de Sistemas e Tecnologías de Información*, 2(49), 501-507. https://www.proquest.com/docview/2714755710/46D2BDD0427C4937PQ/4?sourcetype=Scholarly%20Journals

Villela, F. (2019). Justificación metodológica del uso de animales en investigación biomédica. *Revista Colombiana de Bioética*, 14(1), 52-68. https://www.redalyc.org/journal/1892/189260608004/189260608004.pdf

Zuña, E., Arce, A., Romero, W., y Soledispa, C. (2019). Análisis de la seguridad de la información en las Pymes de la ciudad de Milagro. *Universidad y Sociedad*, 11(4), 487-492. http://scielo.sld.cu/pdf/rus/v11n4/2218-3620-rus-11-04-487.pdf

ANEXOS

Anexo 1: Matriz de consistencia

PROBLEMA	OBJETIVO	HIPÓTESIS	METODOLOGÍA
PROBLEMA PRINCIPAL ¿Cómo el SGSI según ISO/IEC 27001:2022 incide en la protección de información de una Municipalidad distrital, Lima 2023?	**OBJETIVO PRINCIPAL** Determinar la incidencia SGSI según ISO/IEC 27001:2022 en la protección de información de una Municipalidad distrital, Lima 2023	**HIPÓTESIS PRINCIPAL** El SGSI según ISO/IEC 27001:2022 incide significativamente en la protección de información de una Municipalidad distrital, Lima 2023.	**Tipo:** Aplicado **Nivel:** Correlacional **Diseño:** No experimental **Enfoque:** Cuantitativo **Técnica:** Encuesta **Instrumento:** 2 cuestionarios
PROBLEMA ESPECIFICOS ¿Cómo la confidencialidad del SGSI incide en la protección de información de una Municipalidad Distrital, Lima 2023? ¿Cómo la integridad del SGSI incide en la protección de información de una Municipalidad Distrital, Lima 2023? ¿Cómo la disponibilidad del SGSI incide en la protección de información de una Municipalidad Distrital, Lima 2023?	**OBJETIVOS ESPECIFICOS** Determinar la incidencia de la confidencialidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023 Determinar la incidencia de la integridad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023 Determinar la incidencia de la disponibilidad del SGSI en la protección de información de una Municipalidad Distrital, Lima 2023	**HIPÓTESIS ESPECIFICOS** La confidencialidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023 La integridad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023 La disponibilidad del SGSI incide significativamente en la protección de información de una Municipalidad Distrital, Lima 2023.	

Anexo 2: Matriz de operacionalización

VARIABLES DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ÍTEMS	ESCALA DE MEDICIÓN
Variable 1: SGSI según ISO/IEC 27001:2022	El SGSI es un conjunto de directrices o procedimientos utilizados para identificar riesgos y especificar las acciones que se deben tomar para mitigarlos con la identificación de los activos de la información en base al análisis del conocimiento y la aplicación de los controles (De La Rosa, 2021)	La variable SGSI según ISO/IEC 27001:2022 se ha operacionalizado haciendo uso de tres dimensiones (confidencialidad, integridad y disponibilidad); asegurándose que la información recabada ha sido evaluada en los siguientes 3 niveles: No óptimo (1), Medio (2) y Óptimo (3)	Confidencialidad	- Protección de la información - Accesos - Redes - Información critica - Claves y contraseñas	1 al 6	Ordinal Nunca (1) Casi nunca (2) A veces (3) Casi siempre (4) Siempre (5)
			Integridad	- Protección de datos - Fiabilidad de los recursos - Ataques - Almacenamiento - Sistema de información	7 al 12	
			Disponibilidad	- Acceso a la información - Sistemas de información - Aspectos técnicos - Causas humanas y naturales	13 al 18	
Variable 2: Protección de la información	La protección de información se refiere a un grupo de medidas preventivas y reactivas que aseguran la información con un manejo adecuado de los datos, ya que es un activo intangible invaluable y, por lo tanto, su gestión y protección debe ser principal en cualquier organización (Guevara, Delgado y Mendoza, 2022)	La variable protección de información se ha operacionalizado haciendo uso de tres dimensiones (controles de seguridad, evaluación de riesgos y gestión de incidentes de seguridad); asegurándose que la información recabada ha sido evaluada en los siguientes 3 niveles: No óptimo (1), Medio (2) y Óptimo (3)	Controles de seguridad	- Revisión - Disponibilidad - Mejora	1 al 6	Niveles Óptimo Medio No óptimo
			Evaluación de riesgos	- Revisión - Confiabilidad - Verificación	7 al 12	
			Gestión de incidentes de seguridad	- Revisión - Verificación - Mejora	13 al 18	

Anexo 3: Instrumento de recolección de datos

Cuestionario de Sistema de gestión de seguridad de la información

El Siguiente cuestionario está compuesto por 18 ítems, que tiene como objetivo recopilar datos sobre SGSI según ISO/IEC 27001:2022 en una Municipalidad distrital de Lima 2023. Se le recomienda leer cuidadosamente las preguntas y encerrar la frecuencia que usted crea oportuna.

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

Nro.	Cuestionario	Escala				
	Preguntas	1	2	3	4	5
1	Cumple activamente con los procedimientos de protección de la información					
2	Los accesos a los ambientes de trabajo se encuentran protegidos					
3	Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas					
4	Se usa técnicas como firma digital confidencial para validar documentos					
5	La información crítica del proceso se encuentra en ambientes seguros y resguardado bajo llaves					
6	Cambia periódicamente las contraseñas de acceso a sus aplicativos					
7	Establece controles de protección de datos frente a modificaciones, eliminaciones por entes no autorizados					
8	Garantiza la fiabilidad de los equipos informáticos, funcionan adecuadamente					
9	Establece medidas de prevención contra ataques de virus informáticos					
10	Gestiona backup de almacenamiento y copias de respaldo					
11	Participa activamente en auditorias periódicas de sistema de información					
12	Gestiona el desarrollo de software bajo técnicas como el criptográficas para la protección de la información					

13	El acceso a la información se encuentra disponible para realizar labores					
14	Se garantiza rapidez de respuesta de los sistemas de información					
15	Cuenta con el plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas					
16	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres					
17	Establece controles preventivos frente errores humanos en el tratamiento de la información					
18	Tiene voluntad de aplicar controles de seguridad de información en sus labores diarias.					

Cuestionario de protección de la información

El Siguiente cuestionario está compuesto por 18 ítems, que tiene como objetivo recopilar datos sobre la protección de información en una Municipalidad distrital de Lima, 2023. Se le recomienda leer cuidadosamente las preguntas y encerrar la frecuencia que usted crea oportuna.

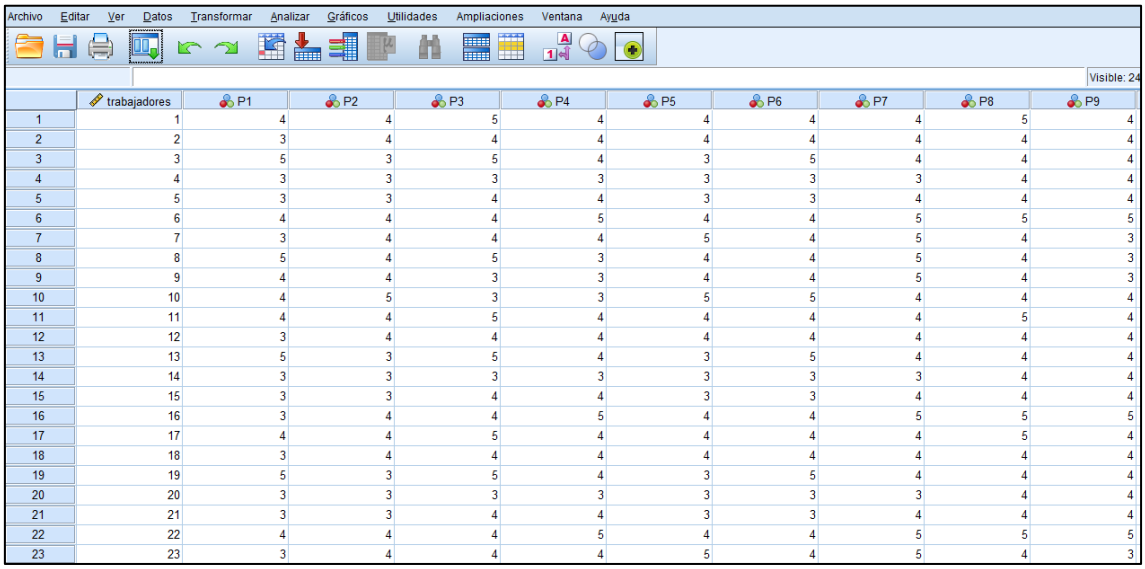
Nunca	Casi nunca	A veces	Casi siempre	Siempre
1	2	3	4	5

Nro.	Cuestionario	Escala				
	Preguntas	1	2	3	4	5
1	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?					
2	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?					
3	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?					
4	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?					
5	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?					
6	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?					
7	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?					

8	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?					
9	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?					
10	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?					
11	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?					
12	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?					
13	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?					
14	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?					
15	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?					
16	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?					
17	¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?					
18	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?					

Anexo 4: Prueba piloto

Variable SGSI según ISO/IEC 27001:2022

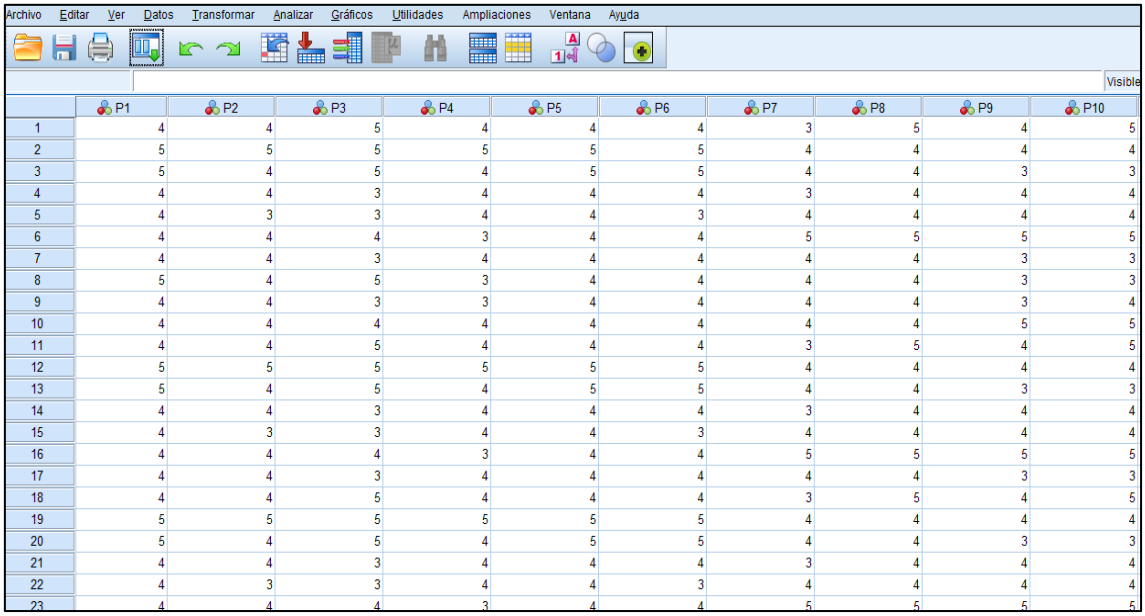


Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

Visible: 24

	trabajadores	P1	P2	P3	P4	P5	P6	P7	P8	P9
1	1	4	4	5	4	4	4	4	5	4
2	2	3	4	4	4	4	4	4	4	4
3	3	5	3	5	4	3	5	4	4	4
4	4	3	3	3	3	3	3	3	4	4
5	5	3	3	4	4	3	3	4	4	4
6	6	4	4	4	5	4	4	5	5	5
7	7	3	4	4	4	5	4	5	4	3
8	8	5	4	5	3	4	4	5	4	3
9	9	4	4	3	3	4	4	5	4	3
10	10	4	5	3	3	5	5	4	4	4
11	11	4	4	5	4	4	4	4	5	4
12	12	3	4	4	4	4	4	4	4	4
13	13	5	3	5	4	3	5	4	4	4
14	14	3	3	3	3	3	3	3	4	4
15	15	3	3	4	4	3	3	4	4	4
16	16	3	4	4	5	4	4	5	5	5
17	17	4	4	5	4	4	4	4	5	4
18	18	3	4	4	4	4	4	4	4	4
19	19	5	3	5	4	3	5	4	4	4
20	20	3	3	3	3	3	3	3	4	4
21	21	3	3	4	4	3	3	4	4	4
22	22	4	4	4	5	4	4	5	5	5
23	23	3	4	4	4	5	4	5	4	3

Variable Protección de la información



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
1	4	4	5	4	4	4	3	5	4	5
2	5	5	5	5	5	5	4	4	4	4
3	5	4	5	4	5	5	4	4	3	3
4	4	4	3	4	4	4	3	4	4	4
5	4	3	3	4	4	3	4	4	4	4
6	4	4	4	3	4	4	5	5	5	5
7	4	4	3	4	4	4	4	4	3	3
8	5	4	5	3	4	4	4	4	3	3
9	4	4	3	3	4	4	4	4	3	4
10	4	4	4	4	4	4	4	4	5	5
11	4	4	5	4	4	4	3	5	4	5
12	5	5	5	5	5	5	4	4	4	4
13	5	4	5	4	5	5	4	4	3	3
14	4	4	3	4	4	4	3	4	4	4
15	4	3	3	4	4	3	4	4	4	4
16	4	4	4	3	4	4	5	5	5	5
17	4	4	3	4	4	4	4	4	3	3
18	4	4	5	4	4	4	3	5	4	5
19	5	5	5	5	5	5	4	4	4	4
20	5	4	5	4	5	5	4	4	3	3
21	4	4	3	4	4	4	3	4	4	4
22	4	3	3	4	4	3	4	4	4	4
23	4	4	4	3	4	4	5	5	5	5

Anexo 5: Confiabilidad de los instrumentos

Variable Sistema de gestión de seguridad de la información

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	30	100,0
	Excluido[a]	0	,0
	Total	30	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,842	18

Variable Protección de la información

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	30	100,0
	Excluido[a]	0	,0
	Total	30	100,0

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

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,885	18

Anexo 6: Validación de juicios de expertos

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de SGSI según ISO/IEC 27001:2022 y protección de información". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Lezama Gonzales Pedro Martin
Grado profesional:	Maestría ( ) Doctorado (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (x)
Áreas de experiencia profesional:	Ingeniero de sistemas
Institución donde labora:	Cooperativa de ahorro y crédito ABACO
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de SGSI según ISO/IEC 27001:2022 y protección de información
Autor (a):	José Manuel Guizado Castillo
Procedencia:	Cuestionario adaptado
Administración:	Directa
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una municipalidad distrital de Lima
Significación:	Nivel de significancia: 0.05

4. Soporte teórico

Variable 1	Dimensiones	Definición
SGSI según ISO/IEC 27001:2022	Confidencialidad Integridad Disponibilidad	El SGSI es un conjunto de directrices o procedimientos utilizados para identificar riesgos y especificar las acciones que se deben tomar para mitigarlos con la identificación de los activos de la información en base al análisis del conocimiento y la aplicación de los controles (De La Rosa, 2021)

Variable 2	Dimensiones	Definición
Protección de la información	Controles de seguridad Evaluación de riesgos Gestión de incidentes de seguridad	La protección de información se refiere a un grupo de medidas preventivas y reactivas que aseguran la información con un manejo adecuado de los datos, ya que es un activo intangible invaluable y, por lo tanto, su gestión y protección debe ser principal en cualquier organización (Guevara, Delgado y Mendoza, 2022)

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de gestión de riesgos elaborado por Cristian Alejandro Luque Aroni en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. *No cumple con el criterio*
2. *Bajo Nivel*
3. *Moderado nivel*
4. *Alto nivel*

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE SGSI SEGÚN ISO/IEC 27001:2022 Y PROTECCIÓN DE INFORMACIÓN

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: SGSI según ISO/IEC 27001:2022

- **Primera dimensión: Confidencialidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir la confidencialidad del SGSI.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Protección de la información	1. Cumple activamente con los procedimientos de protección de la información				✓				✓				✓	
Accesos	2. Los accesos a los ambientes de trabajo se encuentran protegidos				✓				✓				✓	
Redes	3. Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas				✓				✓				✓	
	4. Se usa técnicas como firma digital confidencial para validar documentos				✓				✓				✓	
Información critica	5. La información crítica del proceso se encuentra en ambientes seguros y resguardado bajo llaves				✓				✓				✓	
Claves y contraseñas	6. Cambia periódicamente las contraseñas de acceso a sus aplicativos				✓				✓				✓	

- **Segunda dimensión: Integridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de integridad del SGSI.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Protección de datos	7. Establece controles de protección de datos frente a modificaciones, eliminaciones por entes no autorizados				✓				✓				✓	
Fiabilidad de los recursos	8. Garantiza la fiabilidad de los equipos informáticos, funcionan				✓				✓				✓	

	adecuadamente													
Ataques	9. Establece medidas de prevención contra ataques de virus informáticos				✓				✓				✓	
Almacenamiento	10. Gestiona backup de almacenamiento y copias de respaldo				✓				✓				✓	
Sistema de información	11. Participa activamente en auditorias periódicas de sistema de información				✓				✓				✓	
	12. Gestiona el desarrollo de software bajo técnicas como el criptográficas para la protección de la información				✓				✓				✓	

- **Tercera dimensión: Disponibilidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión medir el nivel de disponibilidad del SGSI.

Indicadores	**Ítem**	**Claridad**				**Coherencia**				**Relevancia**				**Observaciones/ Recomendaciones**
		1	2	3	4	1	2	3	4	1	2	3	4	
Acceso a la información	13. El acceso a la información se encuentra disponible para realizar labores				✓				✓				✓	
Sistema de información	14. Se garantiza rapidez de respuesta de los sistemas de información				✓				✓				✓	
	15. Cuenta con el plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				✓				✓				✓	
Aspectos técnicos	16. Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				✓				✓				✓	
	17. Establece controles preventivos frente errores humanos en el tratamiento de la información				✓				✓				✓	
Causas humanas y naturales	18. Tiene voluntad de aplicar controles de seguridad de información en sus labores diarias				✓				✓				✓	

Dimensiones del instrumento: Protección de la información

- **Primera dimensión: Controles de seguridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de los controles de seguridad

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	19. ¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?				✓				✓				✓	
	20. ¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?				✓				✓				✓	
Disponibilidad	21. ¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?				✓				✓				✓	
	22. ¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?				✓				✓				✓	
Mejora	23. ¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?				✓				✓				✓	
	24. ¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?				✓				✓				✓	

- **Segunda dimensión: Evaluación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de evaluación de riesgos

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	25. ¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?				✓				✓				✓	
	26. ¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?				✓				✓				✓	
Confiabilidad	27. ¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?				✓				✓				✓	
	28. ¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?				✓				✓				✓	
Verificación	29. ¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?				✓				✓				✓	
	30. ¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?				✓				✓				✓	

- **Tercera dimensión: Gestión de incidentes de seguridad**

- Objetivos de la Dimensión: El objetivo de esta dimensión medir el nivel de Gestión de incidentes de seguridad

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	31. ¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?				✓				✓				✓	
	32. ¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?				✓				✓				✓	
Verificación	33. ¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?				✓				✓				✓	
	34. ¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?				✓				✓				✓	
Mejora	35. ¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?				✓				✓				✓	
	36. ¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?				✓				✓				✓	

Dr. Lezama Gonzales Pedro Martin

DNI: 09656793

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de SGSI según ISO/IEC 27001:2022 y protección de información". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

6. Datos generales del juez

Nombre del juez:	Marlon Frank Acuña Benites
Grado profesional:	Maestría ( ) Doctorado (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	Ingeniero de sistemas
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

7. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

8. Datos

Nombre de la Prueba:	Cuestionario de SGSI según ISO/IEC 27001:2022 y protección de información
Autor (a):	José Manuel Guizado Castillo
Procedencia:	Cuestionario adaptado
Administración:	Directa
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una municipalidad distrital de Lima
Significación:	Nivel de significancia: 0.05

9. Soporte teórico

Variable 1	Dimensiones	Definición
SGSI según ISO/IEC 27001:2022	Confidencialidad Integridad Disponibilidad	El SGSI es un conjunto de directrices o procedimientos utilizados para identificar riesgos y especificar las acciones que se deben tomar para mitigarlos con la identificación de los activos de la información en base al análisis del conocimiento y la aplicación de los controles (De La Rosa, 2021)

Variable 2	Dimensiones	Definición
Protección de la información	Controles de seguridad Evaluación de riesgos Gestión de incidentes de seguridad	La protección de información se refiere a un grupo de medidas preventivas y reactivas que aseguran la información con un manejo adecuado de los datos, ya que es un activo intangible invaluable y, por lo tanto, su gestión y protección debe ser principal en cualquier organización (Guevara, Delgado y Mendoza, 2022)

10. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de gestión de riesgos elaborado por Cristian Alejandro Luque Aroni en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	5. No cumple con el criterio	El ítem no es claro.
	6. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	7. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	8. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	5. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	6. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	7. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	8. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	5. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	6. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	7. Moderado nivel	El ítem es relativamente importante.
	8. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

5. *No cumple con el criterio*
6. *Bajo Nivel*
7. *Moderado nivel*
8. *Alto nivel*

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE SGSI SEGÚN ISO/IEC 27001:2022 Y PROTECCIÓN DE INFORMACIÓN

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: SGSI según ISO/IEC 27001:2022

- **Primera dimensión: Confidencialidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir la confidencialidad del SGSI.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Protección de la información	Cumple activamente con los procedimientos de protección de la información				✓				✓				✓	
Accesos	Los accesos a los ambientes de trabajo se encuentran protegidos				✓				✓				✓	
Redes	Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas				✓				✓				✓	
	Se usa técnicas como firma digital confidencial para validar documentos				✓				✓				✓	
Información critica	La información crítica del proceso se encuentra en ambientes seguros y resguardado bajo llaves				✓				✓				✓	
Claves y contraseñas	Cambia periódicamente las contraseñas de acceso a sus aplicativos				✓				✓				✓	

- **Segunda dimensión: Integridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de integridad del SGSI.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Protección de datos	Establece controles de protección de datos frente a modificaciones, eliminaciones por entes no autorizados				✓				✓				✓	
Fiabilidad de los recursos	Garantiza la fiabilidad de los equipos informáticos, funcionan				✓				✓				✓	

	adecuadamente													
Ataques	Establece medidas de prevención contra ataques de virus informáticos				✓				✓				✓	
Almacenamiento	Gestiona backup de almacenamiento y copias de respaldo				✓				✓				✓	
Sistema de información	Participa activamente en auditorias periódicas de sistema de información				✓				✓				✓	
	Gestiona el desarrollo de software bajo técnicas como el criptográficas para la protección de la información				✓				✓				✓	

- **Tercera dimensión: Disponibilidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión medir el nivel de disponibilidad del SGSI.

Indicadores	**Ítem**	**Claridad**				**Coherencia**				**Relevancia**				**Observaciones/ Recomendaciones**
		1	2	3	4	1	2	3	4	1	2	3	4	
Acceso a la información	El acceso a la información se encuentra disponible para realizar labores				✓				✓				✓	
Sistema de información	Se garantiza rapidez de respuesta de los sistemas de información				✓				✓				✓	
	Cuenta con el plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				✓				✓				✓	
Aspectos técnicos	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				✓				✓				✓	
	Establece controles preventivos frente errores humanos en el tratamiento de la información				✓				✓				✓	
Causas humanas y naturales	Tiene voluntad de aplicar controles de seguridad de información en sus labores diarias				✓				✓				✓	

Dimensiones del instrumento: Protección de la información

- **Primera dimensión: Controles de seguridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de los controles de seguridad

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?				✓				✓				✓	
	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?				✓				✓				✓	
Disponibilidad	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?				✓				✓				✓	
	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?				✓				✓				✓	
Mejora	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?				✓				✓				✓	
	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?				✓				✓				✓	

- **Segunda dimensión: Evaluación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de evaluación de riesgos

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?				✓				✓				✓	
	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?				✓				✓				✓	
Confiabilidad	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?				✓				✓				✓	
	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?				✓				✓				✓	
Verificación	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?				✓				✓				✓	
	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?				✓				✓				✓	

- **Tercera dimensión: Gestión de incidentes de seguridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión medir el nivel de Gestión de incidentes de seguridad

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?				✓				✓				✓	
	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?				✓				✓				✓	
Verificación	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?				✓				✓				✓	
	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?				✓				✓				✓	
Mejora	¿Está usted satsfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?				✓				✓				✓	
	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes de seguridad de la información?				✓				✓				✓	

Dr. Marlon Frank Acuña Benites
DNI: 42097456

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de SGSI según ISO/IEC 27001:2022 y protección de información". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

11. Datos generales del juez

Nombre del juez:	Pereyra Acosta Manuel Antonio
Grado profesional:	Maestría (x) Doctorado ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa (x) Organizacional ( )
Áreas de experiencia profesional:	Ingeniero de computación y sistemas
Institución donde labora:	Pontificia Universidad Católica del Perú
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

12. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

13. Datos

Nombre de la Prueba:	Cuestionario de SGSI según ISO/IEC 27001:2022 y protección de información
Autor (a):	José Manuel Guizado Castillo
Procedencia:	Cuestionario adaptado
Administración:	Directa
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de una municipalidad distrital de Lima
Significación:	Nivel de significancia: 0.05

14. Soporte teórico

Variable 1	Dimensiones	Definición
SGSI según ISO/IEC 27001:2022	Confidencialidad	El SGSI es un conjunto de directrices o procedimientos utilizados para identificar riesgos y especificar las acciones que se deben tomar para mitigarlos con la identificación de los activos de la información en base al análisis del conocimiento y la aplicación de los controles (De La Rosa, 2021)
	Integridad	
	Disponibilidad	

Variable 2	Dimensiones	Definición
Protección de la información	Controles de seguridad	La protección de información se refiere a un grupo de medidas preventivas y reactivas que aseguran la información con un manejo adecuado de los datos, ya que es un activo intangible invaluable y, por lo tanto, su gestión y protección debe ser principal en cualquier organización (Guevara, Delgado y Mendoza, 2022)
	Evaluación de riesgos	
	Gestión de incidentes de seguridad	

15. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de gestión de riesgos elaborado por Cristian Alejandro Luque Aroni en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	9. No cumple con el criterio	El ítem no es claro.
	10. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	11. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	12. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	9. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	10. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	11. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	12. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	9. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	10. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	11. Moderado nivel	El ítem es relativamente importante.
	12. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

9. No cumple con el criterio
10. Bajo Nivel
11. Moderado nivel
12. Alto nivel

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE SGSI SEGÚN ISO/IEC 27001:2022 Y PROTECCIÓN DE INFORMACIÓN

Cada pregunta consta de una afirmación relacionada con cada dimensión de la variable y deberá evaluarla en una escala de tipo Likert de cinco puntos, donde 1 significa "Nunca" y 5 significa "Siempre".

Dimensiones del instrumento: SGSI según ISO/IEC 27001:2022

- **Primera dimensión: Confidencialidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir la confidencialidad del SGSI.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Protección de la información	Cumple activamente con los procedimientos de protección de la información				✓				✓				✓	
Accesos	Los accesos a los ambientes de trabajo se encuentran protegidos				✓				✓				✓	
Redes	Gestiona la aplicación de los procedimientos de protección y mantenimiento de redes informáticas				✓				✓				✓	
	Se usa técnicas como firma digital confidencial para validar documentos				✓				✓				✓	
Información critica	La información crítica del proceso se encuentra en ambientes seguros y resguardado bajo llaves				✓				✓				✓	
Claves y contraseñas	Cambia periódicamente las contraseñas de acceso a sus aplicativos				✓				✓				✓	

- **Segunda dimensión: Integridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de integridad del SGSI.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Protección de datos	Establece controles de protección de datos frente a modificaciones, eliminaciones por entes no autorizados				✓				✓				✓	
Fiabilidad de los	Garantiza la fiabilidad de los				✓				✓				✓	

recursos	equipos informáticos, funcionan adecuadamente													
Ataques	Establece medidas de prevención contra ataques de virus informáticos				✓				✓				✓	
Almacenamiento	Gestiona backup de almacenamiento y copias de respaldo				✓				✓				✓	
Sistema de información	Participa activamente en auditorias periódicas de sistema de información				✓				✓				✓	
	Gestiona el desarrollo de software bajo técnicas como el criptográficas para la protección de la información				✓				✓				✓	

- **Tercera dimensión: Disponibilidad**
- Objetivos de la Dimensión: El objetivo de esta dimensión medir el nivel de disponibilidad del SGSI.

Indicadores	**Ítem**	**Claridad**				**Coherencia**				**Relevancia**				**Observaciones/ Recomendaciones**
		1	2	3	4	1	2	3	4	1	2	3	4	
Acceso a la información	El acceso a la información se encuentra disponible para realizar labores				✓				✓				✓	
Sistema de información	Se garantiza rapidez de respuesta de los sistemas de información				✓				✓				✓	
	Cuenta con el plan de mantenimiento de equipos informáticos para la prevención de fallas técnicas				✓				✓				✓	
Aspectos técnicos	Cuenta con un plan de contingencia para recuperación de la información en caso de desastres				✓				✓				✓	
	Establece controles preventivos frente errores humanos en el tratamiento de la información				✓				✓				✓	
Causas humanas y naturales	Tiene voluntad de aplicar controles de seguridad de información en sus labores diarias				✓				✓				✓	

Dimensiones del instrumento: Protección de la información

- **Primera dimensión: Controles de seguridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de los controles de seguridad

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	¿Considera usted que la oficina de tecnología de información realiza revisiones periódicas de los controles de seguridad en la institución?				✓				✓				✓	
	¿Considera usted que, habiéndose identificado una deficiencia de seguridad, se ejecutan los controles de seguridad necesarios para minimizar la vulnerabilidad?				✓				✓				✓	
Disponibilidad	¿Puede afirmar que la oficina de tecnología de información cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales respecto a la información?				✓				✓				✓	
	¿Qué tan conforme está usted con la disponibilidad de los sistemas informáticos en la institución?				✓				✓				✓	
Mejora	¿Coincide en que la oficina de tecnología de información realiza evaluaciones periódicas para identificar mejoras en los controles de seguridad implementados?				✓				✓				✓	
	¿Está de acuerdo con que la oficina de tecnología de información planifica constantes mejoras que contribuyen a soluciones estratégicas para los objetivos de la institución?				✓				✓				✓	

- **Segunda dimensión: Evaluación de riesgos**
- Objetivos de la Dimensión: El objetivo de esta dimensión es medir el nivel de evaluación de riesgos

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	¿Ha notado si la oficina de tecnología de información realiza revisiones periódicas de los riesgos de seguridad de la institución?				✓				✓				✓	
	¿Considera usted que la oficina de tecnología de información corrige de manera adecuada las deficiencias de seguridad identificadas?				✓				✓				✓	
Confiabilidad	¿Considera usted que se identifican y priorizan los riesgos de seguridad de la información de la institución?				✓				✓				✓	
	¿Considera usted que se establecen y aplican medidas de seguridad para reducir o mitigar los riesgos de seguridad de la información en la institución?				✓				✓				✓	
Verificación	¿Cuándo se presenta una incidencia con los servicios de TI que interfiera con sus funciones, se verifica la efectividad de las medidas de seguridad implementadas para reducir o mitigar los riesgos de seguridad de la información?				✓				✓				✓	
	¿Considera usted que la oficina de tecnologías verifica las medidas de seguridad implementadas en la institución?				✓				✓				✓	

- **Tercera dimensión: Gestión de incidentes de seguridad**
- Objetivos de la Dimensión: El objetivo de esta dimensión medir el nivel de Gestión de incidentes de seguridad

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Revisión	¿Considera usted que se notifican y reportan los incidentes de seguridad de la información en la institución?				✓				✓				✓	
	¿Puede usted afirmar que la oficina de tecnología de información realiza una revisión periódica de los procedimientos de gestión de incidentes de seguridad en la institución?				✓				✓				✓	
Verificación	¿Cree usted que la oficina de tecnologías de la información realiza simulaciones de los incidentes de seguridad para evaluar la preparación y capacidad de repuesta de la institución?				✓				✓				✓	
	¿Usted considera cierto que la oficina de tecnología de información lleva un registro de los incidentes de seguridad de la información y se analizan para identificar patrones o tendencias?				✓				✓				✓	
Mejora	¿Está usted satisfecho con el nivel mostrado por parte de los profesionales del equipo de oficina de tecnología de información?				✓				✓				✓	
	¿Está conforme con las mejoras realizadas por la oficina de tecnología de información respecto a las revisiones periódicas de los procedimientos de gestión de incidentes				✓				✓				✓	

	de seguridad de la información?												

Mgtr. Pereyra Acosta Manuel Antonio
DNI: 07268839

Anexo 7: Ficha técnica SGSI

Nombre original: Cuestionario sobre SGSI según ISO/IEC 27001:2022 en una Municipalidad distrital de Lima 2023

Autor: José Manuel Guizado Castillo

Procedencia: Lima

Año de elaboración: 2023

Administración: Individual y Colectiva

Aplicación: 132 trabajadores

Materiales: Formato de preguntas, hoja de respuestas.

Número de ítems: 18 ítems

Objetivo: El objetivo del cuestionario es recopilar datos sobre SGSI según ISO/IEC 27001:2022 en una Municipalidad distrital de Lima 2023

Anexo 8: Ficha técnica de Protección de información

Nombre original: Cuestionario sobre protección de la información en una Municipalidad distrital de Lima 2023

Autor: José Manuel Guizado Castillo

Procedencia: Lima

Año de elaboración: 2023

Administración: Individual y Colectiva

Aplicación: 132 trabajadores

Materiales: Formato de preguntas, hoja de respuestas.

Número de ítems: 18 ítems

Objetivo: El objetivo del cuestionario es recopilar datos sobre la protección de la información en una Municipalidad distrital de Lima 2023

Anexo 9: Niveles de medición

V1: SGSI	
PREGUNTAS	18
ESCALA	5
MAX	90
MIN	18
DIFERENCIA	72
NIVELES	3
EQUILIBRIO	24
OPTIMO	66-90
MEDIO	42-65
NO OPTIMO	18-41

D1: CONFIDENCIALIDAD	
PREGUNTAS	6
ESCALA	5
MAX	30
MIN	6
DIFERENCIA	24
NIVELES	3
EQUILIBRIO	8
OPTIMO	22-30
MEDIO	14-21
NO OPTIMO	6-13

D2: INTEGRIDAD	
PREGUNTAS	6
ESCALA	5
MAX	30
MIN	6
DIFERENCIA	24
NIVELES	3
EQUILIBRIO	8
OPTIMO	22-30
MEDIO	14-21
NO OPTIMO	6-13

D3: DISPONIBILIDAD	
PREGUNTAS	6
ESCALA	5
MAX	30
MIN	6
DIFERENCIA	24
NIVELES	3
EQUILIBRIO	8
OPTIMO	22-30
MEDIO	14-21
NO OPTIMO	6-13

V2: PROTECCIÓN DE INFORMACIÓN	
PREGUNTAS	18
ESCALA	5
MAX	90
MIN	18
DIFERENCIA	72
NIVELES	3
EQUILIBRIO	24
OPTIMO	66-90
MEDIO	42-65
NO OPTIMO	18-41

D1: CONTROLES DE SEGURIDAD	
PREGUNTAS	6
ESCALA	5
MAX	30
MIN	6
DIFERENCIA	24
NIVELES	3
EQUILIBRIO	8
OPTIMO	22-30
MEDIO	14-21
NO OPTIMO	6-13

D2: EVALUACIÓN DE RIESGOS	
PREGUNTAS	6
ESCALA	5
MAX	30
MIN	6
DIFERENCIA	24
NIVELES	3
EQUILIBRIO	8
OPTIMO	22-30
MEDIO	14-21
NO OPTIMO	6-13

D3: GESTIÓN DE INCIDENTES DE SEGURIDAD	
PREGUNTAS	6
ESCALA	5
MAX	30
MIN	6
DIFERENCIA	24
NIVELES	3
EQUILIBRIO	8
OPTIMO	22-30
MEDIO	14-21
NO OPTIMO	6-13

Anexo 10: Calculo muestral

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

Dónde:

n: Tamaño de la muestra

N: Población

Z: Nivel de confianza 95% (Z= 1.96)

d: Error de muestra: 5% (0,05)

p: Probabilidad de éxito: 0.50

q: Probabilidad de fracaso: 0.50

$$n = \frac{200 * (1.96)^2(0.5)(0.5)}{(0.05)^2 * (200-1) + (1.96)^2(0.5)(0.5)}$$

$$n = 132$$

Anexo 12: Carta de Autorización

Municipalidad Distrital de Pachacámac

"Año de la unidad, la paz y el desarrollo"

Lima, 21 de noviembre de 2023

Carta 112-2023-GM/MDP

JOSE MANUEL GUIZADO CASTILLO
Mz K1B Lt 9 Asoc. de Vivienda MARKO JARA, Ancon -Lima

ASUNTO: SOLICITUD DE PERMISO PARA REALIZAR INVESTIGACIÓN ACADÉMICA

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, en atención a su solicitud de permiso para realizar investigación académica en el marco de la investigación titulada: "***SGSI SEGÚN ISO/IEC 27001:2022 Y SU INCIDENCIA EN LA PROTECCIÓN DE INFORMACIÓN EN UNA MUNICIPALIDAD DISTRITAL, LIMA 2023***" del programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Universidad Cesar Vallejo.

Al respecto, le comunicamos que se le estará brindando las facilidades para acceder a la información requerida siempre que la misma no esté protegida por la Ley N.° 29733, Ley de Protección de Datos Personales y su reglamento. Asimismo, siempre que no esté catalogada como información confidencial o reservada como parte de los procesos internos de la entidad; o sea parte de los procesos de contrataciones en el marco de la Ley N° 30225, Ley de Contrataciones del Estado, su reglamento y modificatorias.

Sin otro particular, hago propicia la ocasión para expresarle los sentimientos de mi especial consideración y estima personal.

Atentamente,

MUNICIPALIDAD DISTRITAL DE PACHACAMAC

Abog. JOSÉ LUIS ESPICHÁN PÉREZ
GERENTE MUNICIPAL