Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática
Escuela Profesional de Ingeniería de Sistemas

Sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano - 2023

Tesis

Para optar el Título Profesional de Ingeniero de Sistemas

Autores

Jose Alexander Oyola Gomez
Ana Lisbet Dominguez Vilela

ANA DORIS MAGDALENA BARRERA LOZA
ING. INDUSTRIAL
Reg. Colegio de Ingenieros Nº 98696

Asesor

Dra. Ana Doris Magdalena Barrera Loza

Huacho–Perú

2024

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	**DNI**	**FECHA DE SUSTENTACIÓN**
Oyola Gomez, Jose Alexander	76378496	16/09/2024
Dominguez Vilela, Ana Lizbet	76565254	16/09/2024
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Dra. Ana Doris Magdalena Barrera Loza	15727274	0000-0001-8296-6519
DATOS DE LOS MIEMROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Dr. Juan Carlos Meyhuay Fidel	15681861	0000-0001-7177-5370
Dr. Edwin Ivan Farro Pacifico	15735619	0000-0002-8735-8851
Dr. Bernal Valladares Carlos Enrique	15614554	0000-0002-7421-9537

Ana Lizbet Dominguez Vilela 2024-056122

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS DE LA INSTITUCIÓN EDUCATIVA ESTA...

Quick Submit

Quick Submit

Facultad de Ingeniería Industrial, Sistemas e Informática

Detalles del documento

Identificador de la entrega
trn:oid:::1:2992507020

Fecha de entrega
28 ago 2024, 3:37 p.m. GMT-5

Fecha de descarga
23 sep 2024, 3:35 p.m. GMT-5

Nombre de archivo
Borrador_de_tesis_final_-_Oyola.docx

Tamaño de archivo
1.8 MB

93 Páginas

17,511 Palabras

94,310 Caracteres

18% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Exclusiones

▸ N.º de fuentes excluidas

Fuentes principales

14% Fuentes de Internet

10% Publicaciones

9% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS DE LA INSTITUCIÓN EDUCATIVA ESTATAL Nº20827 MERCEDES INDACOCHEA LOZANO - 2023

DEDICATORIA

Gracias a nuestros padres por ser los principales impulsores de nuestros sueños, por su confianza y fe en nosotros y por la disposición de mi madre para acompañarme en cada larga y agotadora noche de estudio, ella me alivió. Tomé una taza de café y me sentí cansado, fue como agua en el desierto para mí; gracias a mi padre que siempre quiso y deseó lo mejor para mi vida, gracias por cada consejo y todas las enseñanzas que me guiaron a lo largo de mi vida.

AGRADECIMIENTO

Agradecemos a todos los ingenieros que nos ayudaron con las inquietudes durante todo el desarrollo de esta, a la institución por darnos la información necesaria para hacer posible esta tesis y a las demás personas que de una otra manera aportaron para el desarrollo de la tesis.

ÍNDICE

ÍNDICE DE TABLA

ÍNDICE DE FIGURA

RESUMEN

Título de la investigación: "Sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano - 2023". **Autores:** Bach. Ana Lizbet Dominguez Vilela y Bach. José Alexander Oyola Gomez. **Objetivo:** Determinar el nivel de correlación existente entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023. **Metodología:** Se empleó el método deductivo, partiendo de conceptos generales para abordar situaciones específicas. La investigación es aplicada, ya que se enfoca en resolver problemas concretos y contemporáneos previamente identificados. El diseño del estudio es no experimental y de tipo transversal, ya que los datos se recopilaron en un único momento en la línea de tiempo. La investigación es de nivel correlacional, lo que implica medir la asociación entre las variables. **Población y muestra:** La población está formada por seis empleados y todos ellos están involucrados en el uso y procesamiento de la información que se encuentra en la base de datos; la muestra es censal, eso quiere decir que se consideró a los 6 empleados de la población. **Técnica e instrumento:** Se utilizó la técnica de encuesta, donde se aplicó un cuestionario compuesto por 16 ítems. Los datos recopilados se procesaron utilizando el software estadístico SPSS 26.0 para llevar a cabo el análisis estadístico de los mismos. **Resultados:** El modelo de estimación de Coeficiente de Pearson muestra un coeficiente de 0,860 y una significancia de 0,028, lo que confirma con un 95% de certeza, que si existe una correlación positiva baja entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Palabras Claves: Sistema de gestión de seguridad de la información y la base de datos.

ABSTRACT

Research title: "Information security management system and database of the State Educational Institution Nº20827 Mercedes Indacochea Lozano - 2023", **Author:** Bach. Ana Lizbet Dominguez Vilela andy Bach. José Alexander Oyola Gomez. **Objective:** Determine the level of correlation between the information security management system and the database of the State Educational Institution Nº20827 Mercedes Indacochea Lozano in 2023. **Methodology:** The Deductive method was used, because we started from generic points to address particular situations. The research is Applied because it is aimed at solving contemporary and specific problems that were previously identified. The study design is non-experimental and cross-sectional, since the data were collected at a single moment in time. The research is correlational level, which implies measuring the association between the variables. **Population and sample:** The population is made up of 6 workers who are involved with the use and processing of the information found in the database; The sample is census, that means that the 6 workers of the population were taken. **Technique and instrument:** The survey technique was used, where a questionnaire consisting of 16 items was applied. The collected data were processed with the SPSS 26.0 statistical software to carry out their statistical analysis. **Results:** The Pearson Coefficient estimation model shows a coefficient of 0.860 and a significance of 0.028, which confirms with 95% certainty, the existence of a low positive correlation between the information security management system and the database. the State Educational Institution Nº20827 Mercedes Indacochea Lozano in 2023.

Keywords: Information and database security management system.

INTRODUCCIÓN

Este trabajo de investigación se titula “Sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano - 2023” y fue desarrollado para evidenciar que el sistema de gestión de seguridad de la información, al cual llamaremos SGSI, tiene correlación con la base de datos de dicha institución, permitiendo la mejora de los procesos y la mejor aplicación posible de los controles que salvaguardan la confidencialidad de los datos contenidos en la base de datos, para lo cual también fueron necesarias capacitaciones y concientizar al personal; la investigación se desarrolló de conformidad con los lineamientos de investigaciones y estructura establecida por la UNJFSC, los cuales se detallan a continuación:

En el capítulo I los autores explicaron el planteamiento del problema, la descripción de la realidad problemática, procediendo a la formulación de problemas y sus respectivos objetivos, la justificación, los límites y la viabilidad del estudio.

En el capítulo II los autores desarrollaron el marco teórico, constituido por los antecedentes, bases teóricas y las definiciones de términos técnicos utilizados en la investigación, que sirvieron para entender la investigación. Este capítulo incluye también las hipótesis y la operacionalización de las variables.

En el capítulo III los autores desarrollaron el marco metodológico en donde indican el método, diseño, tipo y nivel de la investigación que establecieron para su desarrollo. También señalan la población y muestra, las técnicas aplicadas para la recolectar los datos y para la transformación de la información.

En el capítulo IV presentamos el producto de pruebas estadísticas realizadas con el software SPSS 26.0 y las pruebas de hipótesis realizadas a cabo para establecer el nivel de relación entre las variables y sus dimensiones respectivamente.

En el capítulo V Los autores discutieron los resultados obtenidos en la investigación y los compararon con los productos de los estudios de referencia usados en esta investigación.

El capítulo VI Los autores presentaron las conclusiones a las que llegaron al finalizar la investigación, así como las recomendaciones que consideraron necesarias para que la institución las siga.

Para concluir, en el capítulo VII se incluyeron las referencias bibliográficas que se utilizaron como base para este trabajo, las que fueron citadas siguiendo las normas de la 6ta edición de APA.

Capítulo I. Planteamiento del problema

1.1. Descripción de la realidad problemática

Debido a los avances tecnológico que el mundo, en los últimos años, viene enfrentando Arroyo (2019) y Fuentes (2020) indican que esto ha obligado a las organizaciones adoptar nuevas herramientas tecnológicas para poder procesar, transferir y almacenar información. Por medio de la informática se ha automatizado procesos y el manejo de la información dentro de todo tipo de organización, produciendo muchos beneficios, también gracias a Internet, se puede establecer un contacto más cercano con los clientes y ofrecerles un mejor servicio.

Pero, las organizaciones tienen que tener en cuenta que, con el incremento de utilización de la tecnología, ha aumentado los delitos informáticos, sobre todo en nuestro País desde la pandemia, generando pérdida y robo de información, destrucción de información a través de virus y troyanos, etc. Además, Fuentes (2020) señala que deben considerar que también existe la posibilidad del error humano involuntario, una mala manipulación y uso de la información por parte de trabajadores que tienen acceso a la información sensible de la empresa, todo esto afecta a las empresas ocasionándoles pérdidas no sólo económicas, sino pérdidas en la permanencia de los servicios que ofrecen a sus clientes, reducción en su productividad, incumplimientos, etc.

Silva (2022) nos indica que actualmente la tecnología es necesaria para todo tipo de organización debido a que brinda gran soporte a sus procesos, pero eso conlleva a que hay que gestionar los riesgos que el uso de esa tecnología puede ocasionar, sobre todo si afecta a la información vital de la empresa.

Las organizaciones se vienen enfrentando cada día más a más riesgos porque han aumentado las amenazas de todo tipo, tal como lo indica la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), como fraudes informáticos, virus informáticos, robo,

divulgación, mala manipulación, virus, etc., debido a que los delincuentes informáticos se han organizado y actualizado, además que para los delitos informáticos no hay limitación geográfica para realizar sus delitos. Silva (2022) y Akly (2019) resaltan que las organizaciones han tomado conciencia de que la información es un activo vital, por lo que es fundamental activar un SGSI para su cuidado y protección en las diversas formas de presentación, tanto física como digital, que garantice que se tenga información confiable y adecuada para el juicio de decisiones, eliminando o reduciendo amenazas como robo, divulgación, mala manipulación, virus, etc. Añaden que toda empresa debe hacer una mejora continua de la seguridad de su información, renovando las políticas de seguridad, controles y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de todos los activos de información, los cuales están siendo supervisados, revisados y actualizados.

En la institución educativa estatal nº20827 Mercedes Indacochea Lozano se vienen implementando herramientas tecnológicas en algunos de sus procesos, por lo que se cuenta con una base de datos que contiene información para las actividades de ingreso de notas de sus alumnos, generación de reportes como primeros puestos, records académicos, etc. En esta institución desconocen la existencia de normas, políticas y leyes acerca del tratamiento y seguridad de la información, tampoco han establecido lineamientos sobre la seguridad de la información que les ayude a la prevención y control de riesgos considerando tanto amenazas externas como internas, por lo que ya se han presentado ciertos incidentes con la base de datos. Debido a que el personal no cuenta con capacitación sobre el uso del sistema de información, en la Institución educativa Mercedes Indacochea Lozano, son pocas las personas que lo usan y tienen acceso a la base de datos, recargando su trabajo en cuanto al ingreso de notas de todos los alumnos. A pesar de que la implementación tecnológica se viene haciendo de forma lenta, es necesario conocer las amenazas y vulnerabilidades a las que se viene enfrentando la base de

datos, así como también implementar controles de seguridad necesarios según el análisis de riesgos.

Ante estos problemas, la presente investigación está enfocada a implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma Técnica Peruana SO/IEC27001 y determinar cuál es el nivel de asociación entre la variable sistema de gestión de seguridad de la información y la variable base de datos en la institución educativa estatal nº20827 Mercedes Indacochea Lozano en el 2023.

1.2. Formulación del problema

1.2.1. Problema general.

¿Cuál es el nivel de relación entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023?

1.2.2. Problemas específicos.

1. ¿Cuál es el nivel de relación entre la integridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023?
2. ¿Cuál es el nivel de relación entre la disponibilidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023?
3. ¿Cuál es el nivel de relación entre la confidencialidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023?

1.3. Objetivos de la investigación

1.3.1. Objetivo general.

Determinar el nivel de relación que existe entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

1.3.2. Objetivos específicos.

1. Determinar el nivel de relación que existe entre la integridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.
2. Determinar el nivel de relación que existe entre la disponibilidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.
3. Determinar el nivel de relación que existe entre la confidencialidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

1.4. Justificación de la investigación

1.4.1. Justificación práctica.

Este estudio basa su justificación práctica porque, con su resultado, se determinó el nivel de asociación entre el SGSI y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, con lo cual la institución educativa pudo gestionar los riesgos a los que se enfrenta la base de datos con lo cual mejoró su seguridad. Además, con dichos resultados de este trabajo se hicieron las recomendaciones necesarias para optimizar la gestión de seguridad de la información de la base de datos.

1.4.2. Justificación teórica.

Este trabajo se justifica teóricamente por la aplicación de teorías y definiciones básicas sobre SGSI y sobre base de datos para poder explicar condiciones íntimas que están afectando a la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano. Esto posibilita a los investigadores confrontar diversas concepciones obtenidas de las dos variables y sus dimensiones, además con este trabajo se podrá generar contribuciones teóricas sobre las variables de este trabajo, los cuales serán la base teórica en nuevas investigaciones.

1.4.3. Justificación metodológica.

El diseño del presente estudio es no experimental, y se desarrolló en el nivel correlacional. Para cumplir con los objetivos de la investigación, se empleó a la encuesta como técnicas de investigación y al cuestionario como instrumento de investigación; para el procesamiento de datos se aplicaron métodos estadísticos. Los resultados de esta investigación se sustentan en métodos de investigación validados.

1.5. Delimitaciones del estudio

1.5.1. Delimitación espacial.

El desarrollo de este estudio se realizó en la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano, la que está situada en la av. Mercedes Indacochea Nº657, en el distrito de Huacho, provincia de Huaura, en el departamento de Lima.

1.5.2. Delimitación social.

En este trabajo se incluye a los colaboradores que tienen acceso y hacen uso de la base de datos del Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano.

1.5.3. Delimitación temporal.

Se aplicó el tipo transversal para la toma de datos en esta investigación, es decir, se tomaron en un solo momento determinado para encontrar el nivel de asociación entre el SGSI y la base de datos del Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano, desarrollándose entre los meses de julio y diciembre del 2023.

1.5.4. Delimitación conceptual.

En este estudio se consideraron las diversas teorías estudiadas, actualizadas y utilizadas por diversos autores durante los últimos años, relacionadas a temas como el SGSI y bases de datos.

1.6. Viabilidad del estudio

Para el desarrollo de este estudio de investigación, los investigadores cuentan con el fondo necesario auto financiándolo haciéndolo viable, cuentan con principios teóricos respaldados por profesionales especializados en la materia, incluyendo asesores, metodólogos y estadísticos.

Capítulo II. Marco teórico

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales.

Akly (2019) hizo una investigación para Maestría llamado "Modelo de Seguridad basado en la Norma ISO/IEC 27001/2013, para minimizar los riesgos en la seguridad lógica de la información" en la Universidad Autónoma Gabriel Rene Moreno, en la ciudad de Santa Cruz, Bolivia. Su principal objetivo fue desarrollar un Modelo de Seguridad, basado en la ISO /IEC 27001/2013, para minimizar los riesgos de la seguridad lógica de la información en la Dirección de Gestión Catastral, la investigación es de tipo aplicada porque propone una alternativa de solución basada en un diagnóstico en el contexto donde se investiga para la determinación de posibles riesgos y vulnerabilidades, y mediante el método de la modelación plantea una posible solución a los problemas identificados con el desarrollo de un Modelo de Seguridad lógica de la información, la técnica para obtener los datos fue la encuesta, aplicando como instrumento un cuestionario aplicados a 18 personas que conformaban la población y muestra. Concluyó con que mediante un Modelo de Seguridad basado en la Norma ISO/IEC/27001/2013 logró minimizar los peligros relacionados a la seguridad lógica de la información, se desarrollaron siete políticas (seguridad de contraseñas, contra código malicioso, seguridad de información, gestión de privilegios, contra manipulación de aplicaciones, de Capacitaciones y contra amenazas ambientales y naturales) y sus respectivos procedimientos, para el contexto donde se investiga.

Arroyo (2019) desarrolló un trabajo de tesis nombrado "Diseño de un plan de gestión de la seguridad y de la información para el sistema de intranet de la Prefectura de Esmeraldas, basado en estándares internacionales" en la Pontificia Universidad Católica del Ecuador – Sede

Esmeraldas. Su finalidad principal fue diseñar un plan de gestión de la seguridad y de la información para el sistema de intranet de la prefectura de Esmeraldas, apoyándose en modelos internacionales, de método cuantitativo, diseño experimental, de tipo cuasi experimental, la técnica que empleó para recolectar información fue la entrevista, la población y muestra la conformaron 10 trabajadores. Concluye con que es importante contar con un plan de manejo de riesgo de acuerdo a lo que indica la norma de la ISO 27001, el cual permite implementar controles para el tratamiento de riesgos y así prevenir situaciones no deseadas con el manejo de la información.

Chaverra (2021), en su tesis llamada "Implementación de sistema de gestión de la seguridad de la información para el aseguramiento del proceso de ingreso de notas en un portal web universitario", desarrollada en la Universidad de San Buenaventura, en Medellín, Colombia, su principal fin se fijó en la implementación de un SGSI para el asegurar el ingreso de notas en un portal web universitario, en cuanto a la metodología la que da un mayor cubrimiento del riesgo, relacionada a la seguridad de la información en una institución es la MAGERIT, porque contempla un análisis de riesgos con más detalle por lo cual fue la que aplicó el investigador. Concluyó que implantar un SGSI logra administrar de forma óptima y ordenada toda la información de sus procesos internos relacionados al almacenamiento y procesamiento de notas en su portal web, es necesario seguir lineamientos de la norma ISO 27001, aplicando estos estándares, que contribuirán a un mejor manejo de la información corporativa de forma confidencial y segura; teniendo en cuenta la información financiera, propiedad intelectual, detalle de los colaboradores o información de partes interesadas.

Garcés y Moreno (2019) desarrollaron una investigación de posgrado llamada "Diseño del SGSI para los procesos de administración de bases de datos y administración de hosting de

aplicaciones de la Empresa Softdev LTDA., basado en la norma ISO IEC 27001:2013" en la Universidad Piloto de Colombia, en la ciudad de Bogotá. El propísito primordial fue formular un SGSI (sistema de gestión de seguridad de la información) para el tratamiento administrativo de la base de datos y administración de hosting de aplicaciones de Softdev Ltda., apoyado en la norma ISO IEC 27001: 2013. Este estudio es de tipo aplicado porque quiere resolver problemas de seguridad de sus activos de información de la empresa, se caracteriza por ser de nivel descriptivo y de diseño no experimental. En su conclusión indica que con la investigación se demostró la relevancia que cuenta con un sistema de gestión de seguridad de la información (SGSI) como instrumento para la realización de los fines estratégicos de la organización, debido a que evidencia a la alta dirección el comportamiento de los riesgos los cuales pueden ser obstáculos para el cumplimiento de objetivos ya que pueden afectar a la confidencialidad, integridad y disponibilidad de sus activos de información crítica de la organización.

Guerra (2020), elaboró una tesis titulada "Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la biblioteca de la Universidad de la Costa", en Barranquilla, Colombia, su finalidad principal fue implementar un SGSI, basado en la normativa ISO/IEC 27001:2013, El propósito de esta norma es analizar, reducir el riesgo, mejorar y garantizar la información, determinando procesos estandarizados en la biblioteca de la Universidad de la Costa, una institución educativa superior, la investigación es de tipo aplicada, retrospectiva, transversal, descriptivo y documental. Infirió con que el SGSI es importante dentro de la organización debido a que ha logrado determinar los peligros de cada procedimiento, del mismo modo que comprender el nivel de su repercusión para su evaluación, en línea con las amenazas y vulnerabilidades, también se implementaron controles para aligerar o mitigar los peligros de los procedimientos de calidad en la biblioteca de la Universidad de la Costa.

2.1.2. Antecedentes nacionales.

Fuentes (2020) elaboró una investigación llamada “Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca”. Tuvo como objetivo principal el desarrollo de una proposición de SGSI, apoyándose en la norma ISO/IEC 27003, que permita optimizar la gestión de la seguridad de la información en la Universidad Nacional de Cajamarca. Este trabajo es tipo básico, de diseño no experimental, aplicó la metodología española MAGERIT para desarrollar un proceso para distinguir y examinar los peligros de seguridad de la información en las actividades académicas de la Universidad Nacional de Cajamarca. Este proceso estima la relevancia de los activos de TI previamente distinguidos dentro del SGSI. Como conclusión se infirió que la dimensión Contexto de la organización contribuye con un 35.7% al SGSI expuesto, lo que quiere decir que es aceptable en relación a su adaptación de los procesos y procedimientos realizados en la UNC, la dimensión Liderazgo contribuye con casi 4%, lo que quiere decir que a los usuarios no les importa dicha dimensión y para finalizar, la dimensión Planificación obtuvo que contribuye con el 13% al SGSI.

Guardia (2020) realizó una investigación para su grado de maestro titulada “Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Publico Eleazar Guzmán Barrón - Huaraz - 2018”, realizada en la Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú. Su finalidad es proyectar un prototipo de seguridad de la información que minimice los peligros informáticos en la administración académica del Instituto de Educación Superior Tecnológico Público “Eleazar Guzmán Barrón”. El tipo de investigación es aplicada, de enfoque cuantitativo, de diseño experimental, de nivel explicativo, de tipo longitudinal. De

inferencia comprobó que el modelo de gestión de seguridad de la información expuesto, logra implementar mecanismos y controles para reducir al máximo el riesgo.

Ponce (2023), en su estudio de investigación llamado “Sistema de gestión de seguridad de la información para la Protección de datos en una inmobiliaria, Lima 2022” desarrollado en la Universidad César Vallejo, Trujillo, Perú. Su propósito general fue optimizar la seguridad de datos en una inmobiliaria en la ciudad de Lima durante el año 2022 logrado gracias a la propuesta de implementar un SGSI. El tipo de la investigación fue aplicada y de diseño pre experimental. Contaron con una muestra poblacional de 8 instituciones (entre públicas y privadas), las que se evaluaron gracias a una encuesta de satisfacción. Concluye con que el nivel de riesgo de seguridad de la información se aplacó en un 60.00%, las estimaciones que se obtuvieron en las operaciones estadísticas antes y después de implementar la salida fueron de 4.47 y 1.37 puntos. Esto demuestra que un SGSI eleva al máximo la seguridad de los datos de una compañía inmobiliaria en la ciudad de Lima durante el año 2022.

Valverde (2018) elaboró la tesis titulada “Seguridad de la información aplicando el ISO 27001:2013 para la oficina de Registros y archivos académicos de la Universidad Nacional del Callao 2017”, en la Universidad Nacional del Callao. El propósito primordial fue determinar cómo se puede mejorar la seguridad de la información de la Oficina de Registros y Archivos Académicos mediante la ISO 27001:2013. La investigación es de carácter aplicado, con un diseño experimental de nivel explicativo y corte longitudinal, con un enfoque cuantitativo, con una población y muestra de 25 personas. Concluyó que con la implementación de la ISO 27001:2013, esta repercute de modo significativo en la confidencialidad de la seguridad de la información de la Oficina de Registros y Archivos Académicos, aumentando de 67% a 97%,

la disponibilidad ha aumentado significativamente de 28% a 95% y la integridad aumentó considerablemente de 17 % a 95%.

Vegas (2019) desarrolló una tesis titulada “Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001”. Tuvo como propósito principal el diseño de un SGSI para las actividades académicas de la Universidad Nacional de Piura de acuerdo con la NTP ISO/IEC 27001. Este estudio es de tipo aplicado, recolectó información cuantitativa y cualitativa, de diseño no experimental, aplicó la técnica de encuestas para la recolección de datos, aplicando como instrumento un cuestionario. Concluyó con que, al encontrar un porcentaje bajo de cumplimiento del 39%, que demuestra que hay desgano relacionado a la seguridad de la información dentro la organización, lo cual se debe a que hay controles básicos en el funcionamiento de la seguridad de la información; pero que aún no se encuentran documentados ni se ha sensibilizado ni capacitado al personal sobre su uso y tampoco hay procedimientos y métricas para medir el cumplimiento de dichos controles, por lo que es fundamental implantar un SGSI.

2.2. Bases teóricas

2.2.1. Sistema de gestión de seguridad de la información (X).

Ccesa (2017) dentro de su estudio de investigación lo conceptualiza como un grupo de procesos que ayudan a instituir, implantar, sostener y arreglar de forma continua la seguridad de la información, con lo cual, es necesario conocer los peligros a los que afronta la institución. Además, agrega que implementando un SGSI permite establecer procesos consecuentes y tener bien definidas las responsabilidades según un conjunto de políticas, planes y procesos que constan como información acreditada.

Para Camapaza (2019) a través del SGSI se implementan una serie de procesos que garantizan la continuidad de la seguridad de la información, esto gracias también a la conceptualización y atribución de responsabilidades de acuerdo a políticas, planes y procedimientos los cuales estarán documentados.

Para Castro (2018), el SGSI está formado por elementos interrelacionados con relación al esquema organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos aplicados por una institución para definir políticas y fines de la seguridad de la información. Además, implementar SGSI se apoya en la norma ISO 27001 y se apoya en el ciclo Deming para permitir la implantación de un tratamiento de mejora continua. El ciclo Deming consta de las etapas a continuación mencionadas:

Planificar: en esta etapa es importante definir el ámbito y la política de seguridad, esto comienza con examinar los riesgos para comprender la condición actual de la entidad, instala un planeamiento para tratar la información y sus peligros, y luego implementa controles para los continuos riesgos que la organización no ha considerado hasta ahora.

Hacer: en esta fase correspondiente al ciclo Deming o ciclo PDCA se enfoca en planificar cómo se van a tratar los diversos riesgos, lo cual permite concientizar a los colaboradores de una empresa, y el establecimiento de indicadores para los diversos controles los cuales se irán implementando.

Verificar: en esta etapa considera el desarrollo de auditorías que verifiquen una óptima implantación del SGSI, y que luego se realicen auditorías internas y verificar una óptima gestión general de la empresa.

Actuar: en esta etapa se evalúan los resultados obtenidos con la auditoria y se procede a tomar actos correctivos, preventivos o de progreso.

Figura 1. Ciclo de Deming
Fuente: ISO 27000

Según Trujillo (2020), el SGSI brinda diversos procedimientos e instrumentos apoyados en la norma ISO27001, la que ayuda a diversas empresas o instituciones a conocer sus debilidades en cuanto a seguridad de la información, brindando apoyo al personal para contar con una gestión efectiva de los peligros establecidos.

2.2.1.1. Seguridad de la información.

Según la Norma ISO 27001 (2013), la seguridad de la información ayuda a prevenir diversas amenazas para asegurar la continuidad del negocio, reducir daños y maximizar el retorno de inversiones y oportunidades. Además, se debe tener en cuenta que la información puede existir en diversas formas, ya sea impresa en forma física, recopilada digitalmente, transferida por medios electrónicos, presentada por medio de imágenes o expuesta en una charla. La información debe protegerse y resguardarse de manera adecuada en todo momento, sin importar la forma en que se presente o los medios utilizados para distribuirla o almacenarla, para preservar la confidencialidad, integridad y disponibilidad, que son los pilares fundamentales de la seguridad de la información. Para asegurar que la seguridad de la información se gestione de manera adecuada, es necesario seguir un proceso sistemático, documentado y conocido por todos en la organización, desde una perspectiva de gestión de riesgos empresariales, este proceso es lo que constituye un Sistema de Gestión de Seguridad de la Información (SGSI).

Huincho (2019) acerca de la seguridad de la información indica “es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma” (p.13).

Godoy (2014) señala que el objetivo de la seguridad de la información es salvaguardar la información y los sistemas que la gestionan contra accesos, usos, divulgaciones, interrupciones o destrucciones no autorizadas. La seguridad está relacionada a la certitud, carencia de riesgo o contingencia. La seguridad es el estado de un sistema o información, ya sea informático o no, que garantiza que no está expuesto a peligros, daños o riesgos. Se entiende como peligro o daño a cualquier cosa que afecten directamente el procesamiento o los resultados obtenidos. Además, considera que la seguridad de la información consiste en un grupo de medidas preventivas y reactivas implementadas por las empresas en sus sistemas tecnológicos para preservar y salvaguardar la información manteniendo su confidencialidad, la disponibilidad e integridad.

2.2.1.2. Ventajas de la ISO/IEC 27001:2013.

La Norma ISO 27001 (2013) señala que, al implementarse, las ventajas obtenidas son:

- Obtener ventaja comercial: Al obtener la certificación, una empresa tiene una ventaja competitiva sobre su competencia, ya que sus clientes buscan preservar la seguridad de su información, lo que aumenta su situación de confianza.
- Cumplir con requisitos legales: La norma ISO concede una metodología que ayuda a las organizaciones a ejecutar con leyes, normativas y requisitos asociados con la seguridad de la información.
- Mejorar la organización: Impulsa a las empresas a establecer sus procedimientos y actividades clave, incluyendo a aquellos que no estén asociados con la seguridad de la información, para garantizar la permanencia de la empresa.
- Costes menores: Debido a que cada incidente genera un gasto, la implementación de la norma ayuda a prevenir incidentes de seguridad.

2.2.1.3. Gestión del riesgo.

Arévalo, Cedillo y Moscoso (2017) señalan que “la Gestión de Riesgos se define como una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales sólo puede ocurrir una pérdida para la organización” (p.31).

Osorio (2016) en su investigación afirma que la administración del riesgo se basa en el pronóstico e identificación de hechos o circunstancias que pudieran influir en elementos estratégicos, financieros, sociales y legales de algún otro tipo de organización, y para lograr una administración de riesgos efectiva, es crucial que todo el personal de la empresa esté al tanto de los riesgos a los que se enfrentan a diario, esto permitirá proteger de manera más eficiente los activos de información.

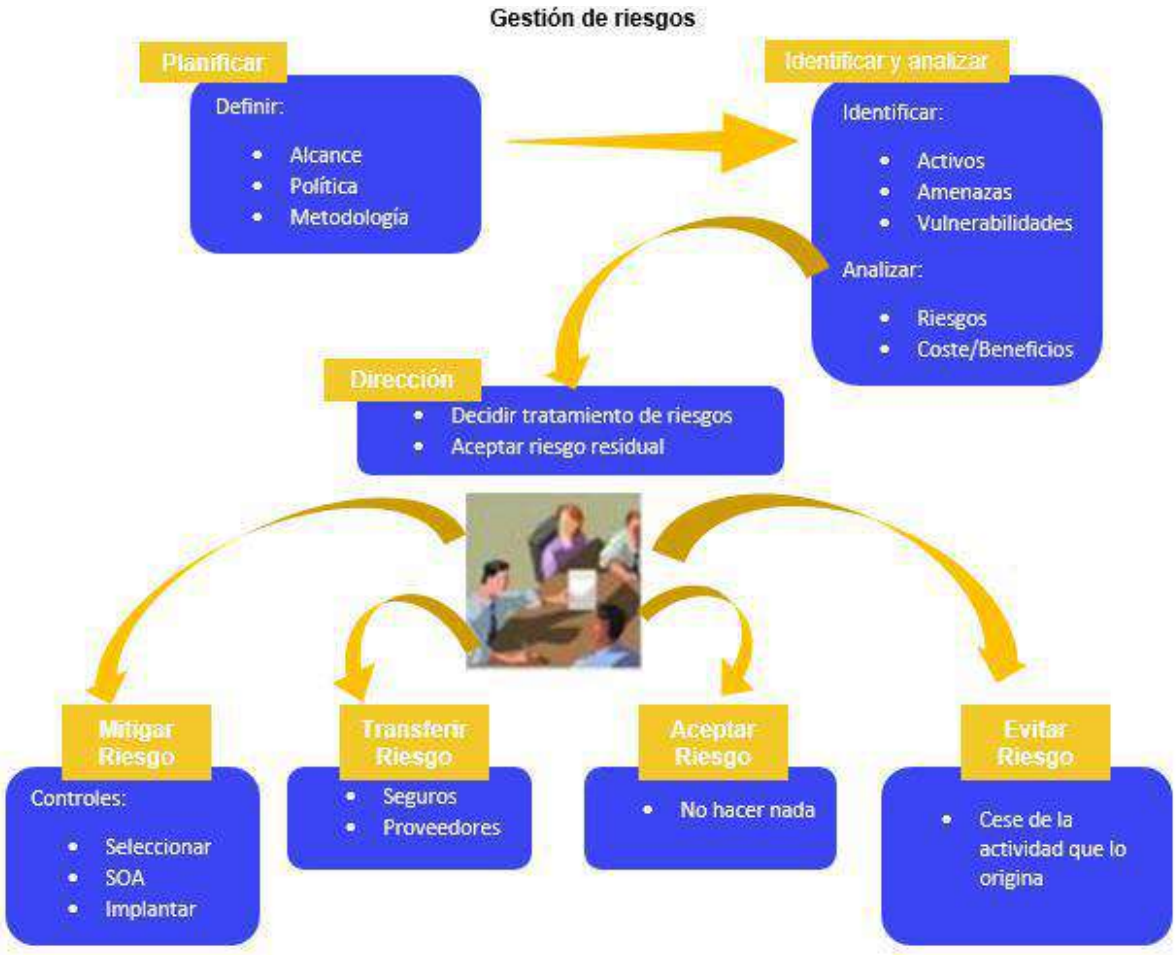


Figura 2. Gestión del riesgo

Fuente: ISO27001, 2017

2.2.1.4. Dimensiones de Sistemas de gestión de seguridad de la información.

Las dimensiones que se consideraron para la variable Sistema de gestión de seguridad de la información se basaron en la ISO 27001, debido a que indica que dicho sistema debe preservar la confidencialidad, integridad y disponibilidad de la información. Del mismo modo los indicadores se basaron en los dominios de dicha norma y en la norma ISO 27004 sobre monitoreo, medición, análisis y evaluación, siendo los más adecuados de acuerdo a los problemas que venía afrontando la institución educativa.

2.2.1.4.1. Integridad de la información (X1).

Méndez (2021) define a la integridad como “la propiedad que busca mantener los datos libres de modificaciones no autorizadas; es decir, que los datos sean exactamente fueron creados sin alteraciones ni manipulaciones por parte de terceros” (p.20).

Godoy (2014) señala que la integridad es aquella característica que indaga que los datos se mantengan libre de toda modificación sin autorización (es diferente a la integridad referencial que contienen las bases de datos), la integridad implica sostener la información exactamente como se creó, omitiendo manipulaciones o alteraciones de parte de personas o procedimientos sin autorización.

Vergara (2017) indicó sobre integridad “busca asegurar que no se realicen modificaciones por personas no autorizadas a datos o procesos, que no se realicen modificaciones no autorizadas por personal autorizado a datos o procesos y que los datos sean consistentes tanto interna como externamente” (p.37).

Narro (2021) señalo sobre integridad, que esta tiene por objetivo que la información manejada dentro de toda la organización y que transita de un lado a otro, tenga alguna modificación no autorizada o exista error en ella, sea voluntario o involuntarios, y con ello asegurar que no existan tomas de decisiones a partir de información errónea, lo que podría causar pérdidas financieras, violaciones de datos personales y amenazas para la supervivencia de la empresa..

Sandoval (2021) añade que la validez y consistencia de los datos almacenados y procesados en un sistema informático se conocen como integridad de la información. Por lo

tanto, los instrumentos utilizados para la seguridad informática deben garantizar que los procesos de actualización estén sincronizados y que la información no se duplique, y asegurar que los usuarios del sistema manipulen adecuadamente dicha información. Esto es muy importante en los sistemas descentralizados, en los que existen diversos tipos de usuarios, computadoras y procesos que comparten la misma información.

2.2.1.4.2. Disponibilidad de la información (X2).

Godoy (2014) la explica como la peculiaridad que permite que la información esté accesible para las personas, procesos o aplicaciones que necesitan disponer de ella, El término "disponibilidad" se refiere al hecho de que las personas autorizadas pueden acceder a los sistemas y la información cuando lo necesiten.

Narro (2021) señala que “la disponibilidad garantiza el acceso a la información en cualquier momento del día, mes o año cuando sea necesario; la falta de disponibilidad en la actualidad generaría únicamente la paralización parcial de actividades” (p.16).

Sandoval (2021) señaló, acerca de la disponibilidad, a que ésta hace referencia a la capacidad de acceder continuamente a los datos procesados y almacenados en un sistema informático. Por lo tanto, los instrumentos utilizados para garantizar la seguridad informática deben fortalecer la capacidad de mantener el sistema informático en condiciones óptimas para que los usuarios puedan acceder a los datos según sus necesidades y con la frecuencia deseada, esto es muy importante en los sistemas informáticos para garantizar un servicio permanente al usuario. La seguridad informática protege los datos de una computadora para evitar daños, alteraciones, garantizar su disponibilidad, mantenerla en óptimas condiciones para su procesamiento en todo momento y preservar su confidencialidad.

Vergara (2017) sustenta que “la disponibilidad, asegura que los usuarios autorizados tienen el acceso adecuado a la información” (p.37).

Méndez (2021) indica que gracias a la disponibilidad “la información puede ser accedida en el momento que sea requerida a través de canales adecuados siguiendo los procesos correctos” (p.21).

2.2.1.4.3. Confidencialidad de la información (X3).

Godoy (2014) determinó a la confidencialidad como “la propiedad que imposibilita la divulgación de información a personas o sistemas no autorizados, asegurando únicamente a aquellas personas que cuenten con la debida autorización para el acceso a la información.” (p. 165).

Vergara (2017) afirma que La confidencialidad se ocupa de evitar el acceso no autorizado a la información, ya sea intencional o no. La confidencialidad puede perderse de diversas maneras, como la publicación intencional de información confidencial de una empresa.

Méndez (2021) sostiene que “la confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados; es decir, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización” (p.20).

Narro (2021) señala sobre la confidencialidad que ésta tiene por finalidad que la información sea accesible sólo a los usuarios con autorización en los distintos niveles existentes en la empresa (personas, entidades o sistemas); la confidencialidad tiene como objetivo evitar

el robo total o parcial de información crítica, ya sea por parte del personal interno o de ciberdelincuentes, y especialmente evitar su difusión o uso indebido.

Sandoval (2021) afirma que la confidencialidad se refiere a la protección de la información que se almacena y procesa en un sistema informático, para ello, todos Los instrumentos de seguridad informática deben proteger el sistema de intrusiones y accesos no autorizados de personas o programas. Esto es crucial en sistemas distribuidos, es decir, en sistemas en los que los trabajadores, las computadoras y los datos están en lugares diferentes, pero están conectados física y lógicamente.

2.2.2. Base de datos (Y).

Monfil (2018) la define de esta forma "conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos. Las bases de datos se diseñan para representar entidades y sus interrelaciones con el objetivo de satisfacer las necesidades de información de una organización" (p. 5).

Morejón (2018) dentro de su trabajo de investigación señala lo siguiente:

> El término base de datos surgió en 1963, en la informática una base de datos consiste en una colección de datos interrelacionados y un grupo de programas para acceder a dichos de datos. En otras palabras, una base de datos no es más que un grupo de información (un conjunto de datos) relacionada que se encuentra agrupada o estructurada. (p. 16)

2.2.2.1. Sistema gestor de base de datos.

Monfil (2018) indica que:

> Consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a dichos datos. Estos sistemas están diseñados para administrar grandes cantidades de datos y ofrecen herramientas para la gestión de la base de datos, además de proporcionar un acceso controlado a la misma. (p. 5)

En su investigación Jiménez (2016) sobre el tema indica:

> Un gestor de base de datos o sistema de gestión de base de datos proporcionan programas, procedimientos, lenguajes que posibilitan a sus usuarios, almacenar, modificar y extraer información de una base de datos. Entre las ventajas de estos sistemas es el proporcionar métodos para mantener la integridad, calidad, seguridad e integración, garantizando una administración eficiente de los datos que maneja una organización, entidad o institución. (p. 35)

Morejón (2018) sobre el sistema de gestión de base de datos indicó:

> Consiste en suministrar al usuario las herramientas que le permitan manipular, en términos abstractos, los datos, o sea, de forma que no le sea necesario conocer el modo de almacenamiento de los datos en la computadora, ni el método de acceso empleado. Los programas de aplicación operan sobre los datos almacenados manipulación de la información que facilitan el trabajo de los usuarios. (p. 16)

2.2.2.2. Funciones de un sistema gestor de bases de datos.

Jiménez (2016) indica que las funciones del sistema gestor de bases de datos son las siguientes:

> Definición de datos: Un Sistema Gestor de datos debe tener componentes procesadores de varios lenguajes, permitir datos fuente externos para convertirlos a versión objeto.
>
> Manipulación de datos: Es importante admitir que el usuario pueda extraer, añadir, actualizar, es decir el SGBD debe incluir componentes denominados DML (lenguaje manipulador de datos).
>
> Integridad y seguridad de los datos: El administrador determina lineamientos para la seguridad de base de datos, el SGBD debe controlar y rechazar los intentos maliciosos.
>
> Recuperación y concurrencia de datos: Un sistema gestor de base de datos debe velar el fiel cumplimiento de controles de Recuperación y concurrencia.
>
> Diccionario de datos: Debe tener un diccionario de datos que permita realizar consultas. (p. 35-36)

2.2.2.3. Lenguajes de bases de datos.

Morejón (2018) sobre indica en su trabajo de tesis:

> Los sistemas de base de datos proporcionan un lenguaje de definición de datos para especificar el esquema de la base datos y un lenguaje de manipulación de datos para expresar las consultas y las modificaciones de la base de datos. En la práctica, los lenguajes de definición y manipulación de datos no son dos lenguajes diferentes; en cambio, simplemente forman parte de un único lenguaje de bases de datos, como puede ser el muy usado SQL. (p. 16)

2.2.2.4. Dimensiones de base de datos.

Las dimensiones que se consideraron para la variable Base de datos se basaron en los dominios de la norma ISO 27001, debido a que indica que deben cuidarse todos los activos de información, incluida la infraestructura tecnológica. Del mismo modo los indicadores se basaron en los dominios de dicha norma y en la norma ISO 27004 sobre monitoreo, medición, análisis y evaluación, siendo los más adecuados de acuerdo a los problemas que venía afrontando la institución educativa.

2.2.2.4.1. Infraestructura tecnológica (Y1).

Blaz y Miranda (2017) indican que:

> Puede ser definido como un conjunto de funciones interrelacionadas, hardware y software empleados para programar y almacenar programas y datos. Es el conjunto de elementos físicos (hardware) y lógicos (software) que permiten procesar la información del usuario realizando igualmente un control eficiente de todos los recursos posibles. (p. 45)

2.2.2.4.2. Capacidad de respuesta (Y2).

Retuerto (2017) en cuanto a la capacidad de respuesta, se destaca que está estrechamente vinculada con la rapidez de reacción y la capacidad de los empleados para abordar situaciones o problemas que surgen durante la jornada laboral. Por eso es importante que la alta dirección de la empresa se preocupe en realizar capacitaciones para fomentar un entorno laboral cómodo y satisfactorio para sus colaboradores, lo que les permite hacer su trabajo con la mejor mentalidad y mejorar la imagen del servicio.

Arias (2019) indica que es “la disposición que tiene la empresa para ofrecer respuestas de manera oportuna y ágil a los usuarios, esto debe proporcionarse de manera eficiente y rápida, la finalidad es que siempre debe superar las expectativas estipuladas” (p.20).

Vergara (2017) la define como “la atención demostrada y la disposición positiva de los colaboradores, asimismo, las habilidades para inspirar credibilidad y confianza ante los usuarios (clientes). La capacidad de respuesta determina poder ofrecer un servicio al cliente con rapidez” (p. 46).

2.2.2.4.3. Fiabilidad (Y3).

Retuerto (2017) la define como la habilidad para brindar el servicio prometido de manera precisa y conforme a lo acordado. Es relevante comprender la relevancia de la fiabilidad para un cliente importante. Por ello, toda institución debe prestar atención a este aspecto para saciar las expectativas del cliente antes de brindar el servicio. Se deben establecer adecuadamente los procesos necesarios para el cumplimiento de esta exigencia, de esta manera, la organización puede alcanzar el objetivo que es poder brindarle a su cliente, un servicio estupendo, de lo contrario, al no cumplirse con esto, el servicio no será considerado como bueno por parte del cliente.

Vergara (2017) la define como “la destreza para realizar la prestación prometida de manera confiable. La fiabilidad, es entendida como la capacidad de cumplir bien a la primera con los compromisos adquiridos” (p. 46).

Arias (2019) agrega en cuanto a fiabilidad que el servicio se debe prestar de manera efectiva y precisa desde el principio. Ahí radica la capacidad de los trabajadores de una empresa

para ofrecer un servicio excelente de forma segura, fiable y cautelosa. Para ello, deben seguir con los procedimientos establecidos, ejecutar adecuadamente las labores de trabajo, en el tiempo disponible y especificado.

2.3. Definiciones de términos básicos

Activo

Narro (2021) en su definición indica "todo aquel elemento que contenga algún tipo de información, que deben estar clasificados de acuerdo a su criticidad, funcionalidad o la sensibilidad con la que debe ser tratada, con el fin de proteger dicha información." (p.29).

Amenazas

Méndez (2021) en su definición indica "suceso desfavorable que puede ocurrir teniendo consecuencias negativas sobre los activos informáticos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor" (p.21).

Análisis de riesgo

Sandoval (2017) en su definición indica "el estudio de las posibles amenazas y probables eventos no deseados es decir los daños y consecuencias que éstas puedan producir" (p.32).

Ataque

Cáceda (2021) en su definición indica "intento de destruir, exponer, alterar, inhabilitar, robar u obtener un acceso no autorizado para usar un activo de manera no autorizada" (p.17).

Control

Cáceda (2021) en su definición señala "medio de la gestión de riesgos, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter jurídico. También se utiliza como sinónimo de salvaguardia o de contramedida" (p.17).

Eficiencia

Trinidad (2019) indica que existe eficiencia "cuando se logran los objetivos planificados en la organización, utilizando el menor costo posible y en el mínimo tiempo, sin gastar recursos y con el máximo nivel de calidad factible" (p.53).

Eficacia

Trinidad (2019) en su definición indica "capacidad de alcanzar el efecto que se espera. Además, contenido de una empresa para lograr los objetivos trazados, obtener los resultados deseables, realizando las cosas correctamente" (p. 53).

Hardware

Carreño (2019) sobre su definición indica "se refiere a la parte física de un sistema informático, poseen componentes electrónicos y mecánicos, un ejemplo claro es el servidor" (p. 33).

Impacto

Narro (2021) indica que el impacto "es considerado como la medida del daño causado cuando una amenaza se materializa sobre un activo, es así que el impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo (p. 29).

Información

Trinidad (2019) señala "por información nos referimos al conjunto integral de datos con un específico significado" (p. 53).

ISO 27001

Chura y Rojas (2022) señalan "es una herramienta que permite mejorar la seguridad a través de su implementación y así permitan salvaguardar la información debido que es el activo de mayor importancia de una organización" (p. 23).

Riesgo

Méndez (2021) lo define como la posibilidad de que una amenaza encuentre las vulnerabilidades de los activos y dañe a la organización; considerada como la combinación de la probabilidad de un evento y sus consecuencias. El riesgo determina lo que podría pasarles a los diferentes activos de la información si estos no son protegidos de manera adecuada. Es importante saber de cada activo que es lo que se va a proteger, así como saber en qué medida las características están en peligro, es decir, analizar el sistema.

Servidor

Carreño (2019) sobre su definición indica "es un ordenador físico central integrado a una red informática que ejecuta aplicaciones que proporcionan servicios a otros programas, denominados clientes" (p. 33).

Software

Carreño (2019) sobre su definición indica "es el soporte lógico de un sistema informático, que está compuesto por un conjunto de componentes lógicos necesarios que realizan tareas específicas" (p. 33).

Vulnerabilidad

Cáceda (2021) la define como "debilidad de un activo o control que puede ser aprovechada por una amenaza" (p. 17)

2.4. Formulación de las hipótesis

2.4.1. Hipótesis general.

El SGSI se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

2.4.2. Hipótesis específica.

1. La integridad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.
2. La disponibilidad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.
3. La confidencialidad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

2.5. Operacionalización de las variables

Tabla 1

Operacionalización de las variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA
Sistema de gestión de seguridad de la información (X)	Ccesa (2017) dentro de su investigación lo define como un conjunto de procesos que ayudan a establecer, implementar, mantener y mejorar de forma continua la seguridad de la información, para lo cual hay que conocer los riesgos a los que se enfrenta la organización. Además, agrega que la implementación de un SGSI permite establecer procesos formales y una clara definición de responsabilidades según una serie de políticas, planes y procedimientos que constan como información documentada.	Sistema de gestión de seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información, es decir, aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en la institución.	X.1.- Integridad de la información. X.2.- Disponibilidad de la información. X.3.- Confidencialidad de la información.	X.1.1.- Seguridad de la comunicación. X.1.2.- Gestión de incidentes. X.1.3.- Seguridad de los procedimientos. X.2.1.- Acceso a la información en el tiempo requerido. X.2.2.- Continuidad del negocio. X.2.3.- Procedimientos de respaldo. X.3.1.- Niveles de accesibilidad. X.3.2.- Autenticación. X.3.3.- Autorización.	Escala de valoración Likert: 1 = Muy en desacuerdo 2 = Algo en desacuerdo 3 = Ni de acuerdo ni en desacuerdo 4 = Algo de acuerdo 5 = Muy de acuerdo

Base de datos (Y)	Monfil (2018) en su definición indica que es “conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos. Las bases de datos se diseñan para representar entidades y sus interrelaciones con el objetivo de satisfacer las necesidades de información de una organización” (p. 5).	La base de datos es una recopilación de datos almacenados electrónicamente que puede contener palabras, números, imágenes, vídeos y archivos, además de almacenar, permite recuperar y editar datos.	Y.1.- Infraestructura tecnológica.	Y.1.1.- Software. Y.1.2.- Hardware.	Escala de valoración Likert: 1 = Muy en desacuerdo 2 = Algo en desacuerdo 3 = Ni de acuerdo ni en desacuerdo 4 = Algo de acuerdo 5 = Muy de acuerdo
			Y.2.- Capacidad de respuesta.	Y.2.1.- Tiempo de respuesta. Y.2.2.- Mejora continua.	
			Y.3.- Fiabilidad.	Y.3.1.- Eficiencia. Y.3.2.- Eficacia.	

Fuente: Elaborado por los autores.

Capítulo III. Metodología

3.1. Diseño metodológico

3.1.1. Método de la investigación.

Para el presente trabajo de investigación se aplicó el método Deductivo, porque los autores partieron de aspectos generales en la investigación para ir encontrando situaciones particulares dentro de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

3.1.2. Diseño de la investigación.

Para la presente investigación se empleó el diseño No Experimental debido a que los investigadores no intervinieron ni manipularon ninguna de las dos variables, además valoraron el comportamiento de ambas variables para establecer si existe correlación entre ellas.

Es de tipo Transversal o transaccional porque comprendió el estado actual que presenta una población determinada, por lo que para la recolección de los datos de la población se realizó en un solo momento determinado durante el año 2023.

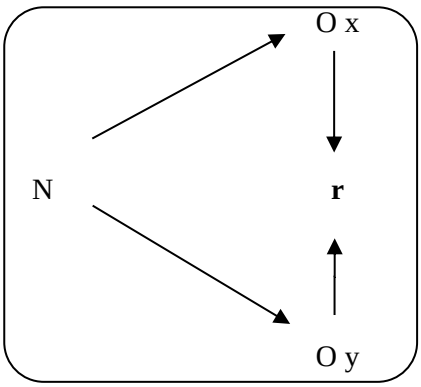
3.1.3. Tipo de Investigación.

La investigación es de tipo Aplicada ya que está orientada a problemas de actualidad, concretos e identificables de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023 a los que se les aplicó soluciones actuales.

Para este tipo de investigación se consideró como punto de inicio el conocimiento generado por la investigación básica y del marco teórico definido para identificar problemas sobre los que se debe actuar como para definir las estrategias de solución.

3.1.4. Nivel de Investigación.

El nivel de investigación que se desarrolló fue el Correlacional, porque lo que se quiso fue medir el grado de asociación entre las variables presentes, es decir se pretende demostrar la relación que existe entre el Sistema de gestión de seguridad de la información y la base da datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, a través de las encuestas las cuales se realizaron a los trabajadores de dicho instituto. La relación que existe entre las variables identificadas la podemos ver en la siguiente figura:



Denotación:

N = Población

Ox = Observación a la variable x.

Oy = Observación a la variable y.

r = Relación entre variables.

3.2. Población y muestra

3.2.1. Población.

En la presente investigación se consideró como población objetivo a 06 trabajadores que tienen acceso a la base de datos de la Institución Educativa Estatal Nº20827 Mercedes

Indacochea Lozano en el 2023, quienes son los que están involucrados directamente con el manejo y seguridad de dicha base de datos. Estos trabajadores son los siguientes:

- ✓ Director.
- ✓ Secretaria de la Dirección.
- ✓ Subdirector administrativo.
- ✓ Subdirector pedagógico (2 personas).
- ✓ Coordinador de Innovación y soporte tecnológico.

3.2.2. Muestra.

Para el presente estudio la población es pequeña, por lo que se consideró una muestra censal, es decir, que para la muestra de estudio se consideró a la totalidad de las unidades de observación, que vale decir a los 06 trabajadores que vienen laborando y tienen acceso a la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

3.3. Técnicas e instrumentos para la recolección de datos

3.3.1. Técnicas

La técnica a emplearse fue la encuesta, la cual estuvo orientada a la recolección de datos los cuales fueron proporcionados por los trabajadores que tienen acceso a la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

3.3.2. Instrumentos

El instrumento que se empleó en la recolección de la información, fue el cuestionario de encuestas, porque es un instrumento que sirve para recoger los datos que nos proporcionaron los trabajadores que tienen acceso a la base de datos de la Institución Educativa Estatal Nº20827

Mercedes Indacochea Lozano en el 2023, a través de un grupo de preguntas que constituyen el tema de la encuesta. Utilizamos el cuestionario simple con preguntas de opción múltiple con escala de calificación de 5 alternativas, para lo cual se utilizó la escala de Likert.

El cuestionario de encuestas fue sometido a validez de contenido mediante la técnica del juicio de expertos, para confirmar que el instrumento es válido y confiable.

3.3.2.1 Validación del Instrumento.

Para poder validar el instrumento que se utilizó para la recolección de datos, se realizó el juicio de experto, los cuales dieron una puntuación mostrada en la siguiente tabla:

Tabla 2

Juicio de expertos para el instrumento

Expertos	Grado	Puntuación
Ing. Juan José Flores Cueto	Doctor	89,5
Ing. José Antonio Garrido Oyola	Maestro	91,0
Ing. Wigberto Martín Nicho Virú	Maestro	90,0
Promedio general		90,2 %

Fuente: Elaboración propia.

Luego se promediaron los puntajes que dio cada uno de los expertos, obteniendo un puntaje del 90,2% para el instrumento, lo cual indica que está en el rango de “Excelente”, demostrando que el instrumento para la presente investigación tiene una alta valoración, llevada a cabo por expertos profesionales con conocimientos en instrumentos de recolección de datos.

3.3.2.2 Confiabilidad del Instrumento.

Para comprobar la Confiabilidad del instrumento ya validado se realizó una prueba piloto a 10 trabajadores de otra institución educativa del estado, los cuales presentan características similares a los sujetos considerados en la muestra. El procesamiento de las respuestas de la encuesta se realizó con el software SPSS Versión 26, luego del cual se obtuvieron los resultados siguientes:

Tabla 3
Resumen del procesamiento de los casos del instrumento

		N	%
Casos	Válidos	10	100,0
	Excluidos[a]	0	,0
	Total	10	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Fuente: Elaboración propia.

Tabla 4
Estadísticos de fiabilidad del instrumento

Alfa de Cronbach	N de elementos
0,92	10

Fuente: Elaboración propia.

Utilizamos el modelo estadístico Alpha de Cronbach, arrojando una confiabilidad de 0,92 para el instrumento, lo cual significa que tiene un nivel elevado de confiabilidad. La aplicación del análisis de Confiabilidad es un modelo estadístico de los más rigurosos para este tipo de pruebas.

3.4. Técnicas para el procedimiento de la información

3.4.1. Análisis documental

Mediante el análisis documental y sus respectivos instrumentos se revisaron fuentes bibliográficas, revistas, publicaciones especializadas y portales de Internet los cuales estuvieron relacionados con el tema de la investigación.

Por medio de la entrevista y el cuestionario, elaborado por los autores de la investigación, se recopiló información sobre cada una de las dimensiones de cada variable, las preguntas estuvieron referidas a los aspectos concretos para recopilar los datos.

3.4.2. Análisis estadístico

Se realizó utilizando el paquete estadístico SPSS 26.0 con el que se procesaron los datos obtenidos mediante los cuestionarios, para luego hacer su respectiva interpretación, análisis y discusión sobre los cuadros y gráficos estadísticos. También permitió encontrar los resultados, contrastar las hipótesis para poder construir las conclusiones que fueron el resultado final de la presente investigación.

Capítulo IV. Resultados

4.1. Análisis de los resultados

4.1.1. Tablas y gráficos de niveles de las dimensiones de la variable Sistema de Gestión se Seguridad de la información.

Tabla 5

Niveles de Integridad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio 7 - 10	2	33,3	33,3	33,3
	Alto 11 - 15	4	66,7	66,7	100,0
	Total	6	100,0	100,0	

Fuente: Elaboración propia.

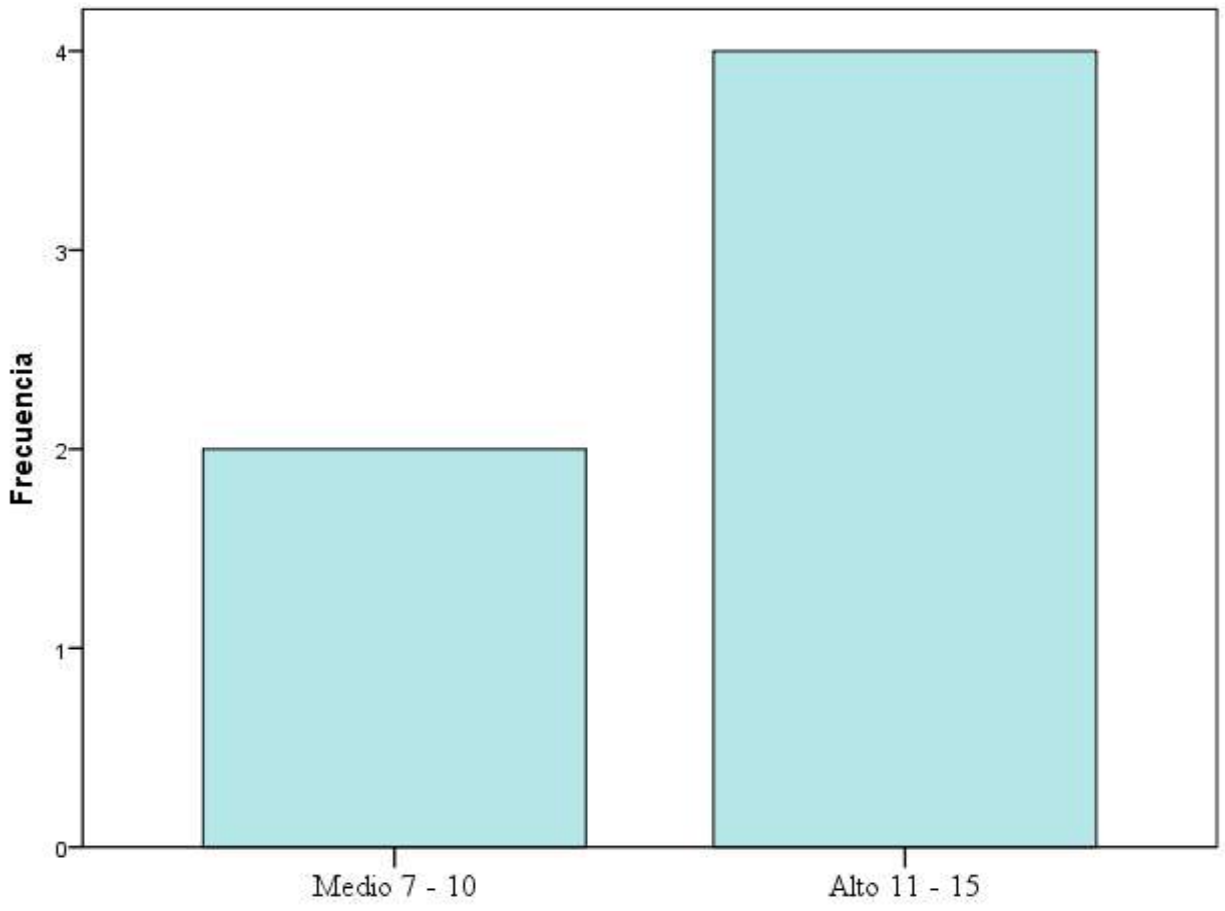


Figura 3. Niveles de integridad de la información

Fuente: Elaboración propia.

La dimensión Integridad de la información tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo <= 6, medio 7 - 10 y alto 11 - 15. De los 6 datos, el 33,3% de los trabajadores calificó la dimensión integridad de la información en un nivel medio y el 66,7% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

Tabla 6

Niveles de Disponibilidad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 3 - 6	2	33,3	33,3	33,3
	Medio 7 - 10	1	16,7	16,7	50,0
	Alto 11 - 15	3	50,0	50,0	100,0
	Total	6	100,0	100,0	

Fuente: Elaboración propia.

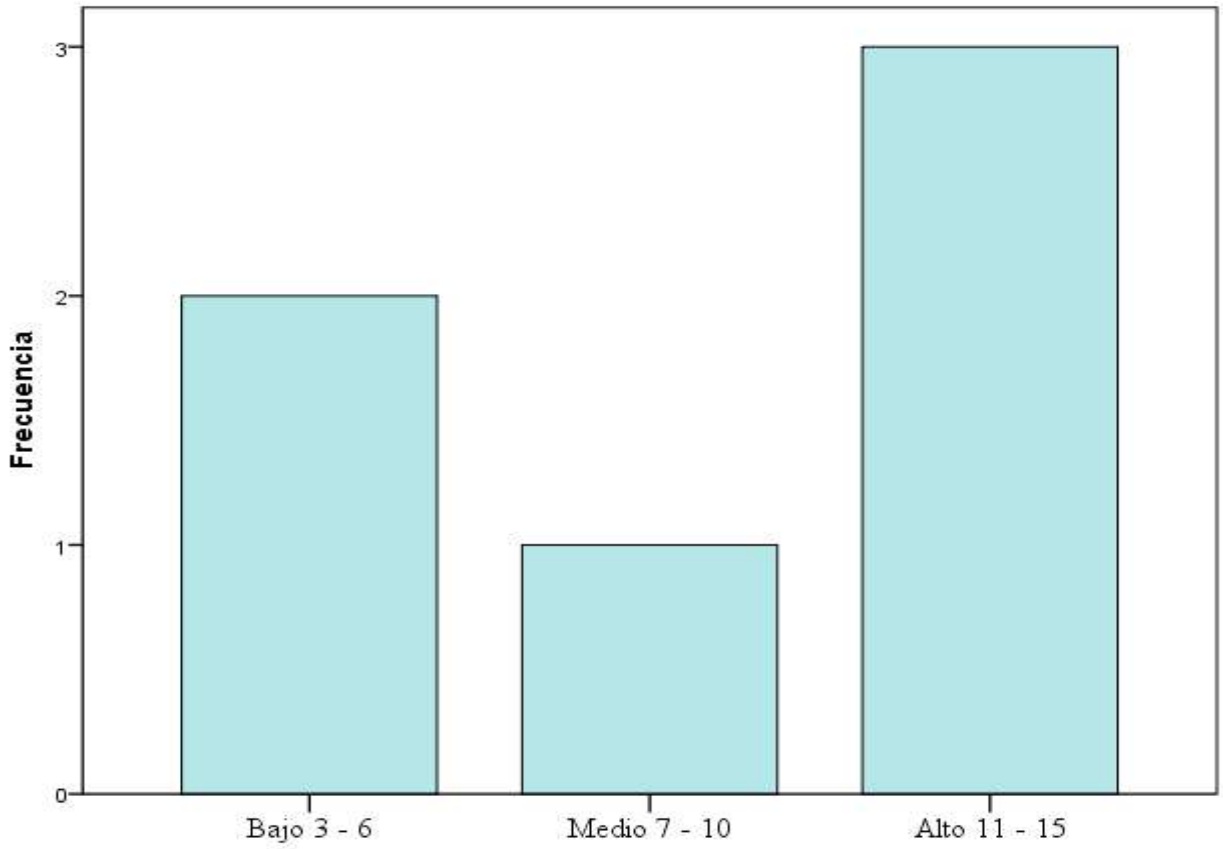


Figura 4. Niveles de disponibilidad de la información

Fuente: Elaboración propia.

La dimensión Disponibilidad de la información tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo <= 6, medio 7 - 10 y alto 11 - 15. De los 6 datos, el33,3% de los trabajadores calificó la dimensión disponibilidad de la información en un nivel bajo, el 16,7% en un nivel medio y el 50% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

Tabla 7

Niveles de Confidencialidad de la información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 3 - 6	2	33,3	33,3	33,3
	Medio 7 - 10	1	16,7	16,7	50,0
	Alto 11 - 15	3	50,0	50,0	100,0
	Total	6	100,0	100,0	

Fuente: Elaboración propia.

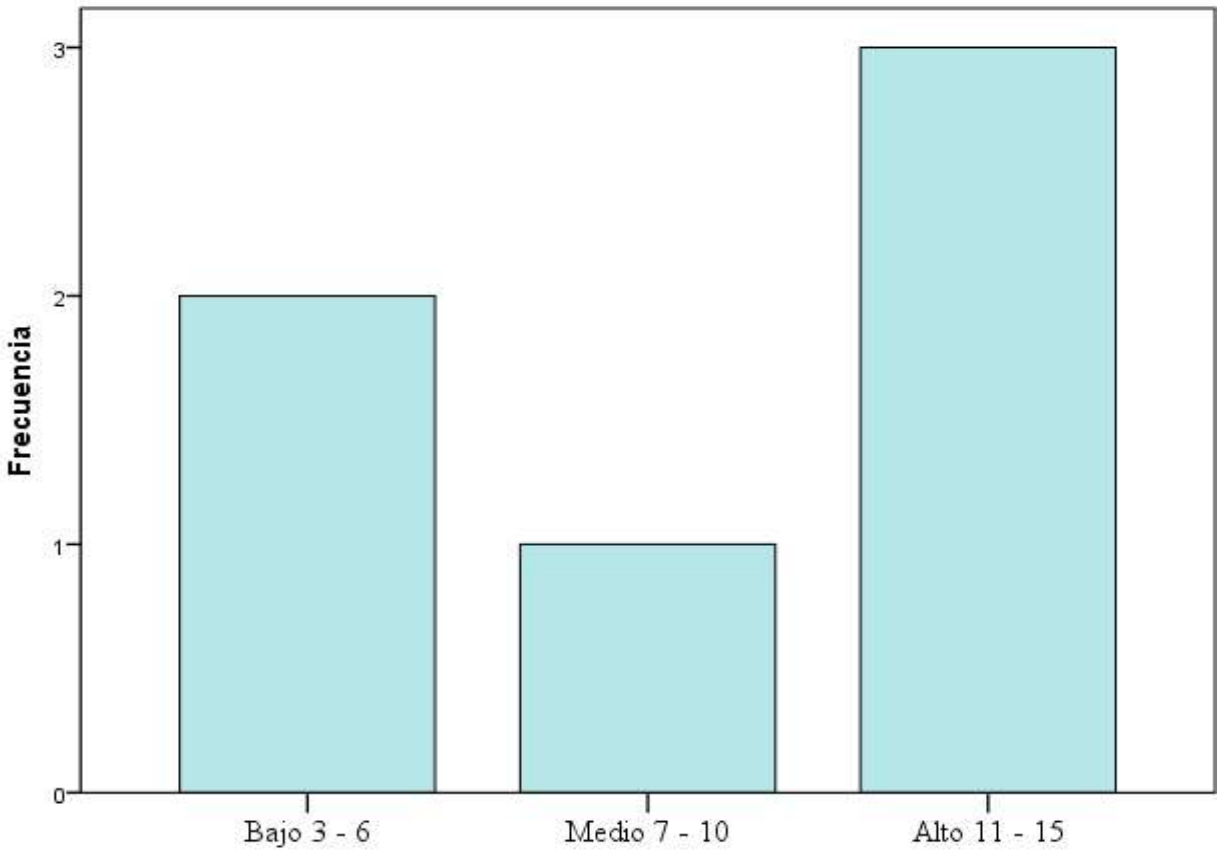


Figura 5. Niveles de confidencialidad de la información

Fuente: Elaboración propia.

La dimensión Confidencialidad de la información tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo <= 6, medio 7 - 10 y alto 11 - 15. De los 6 datos, el 33,3% de los trabajadores calificó la dimensión confidencialidad de la información en un nivel bajo, el 16,7% en un nivel medio y el 50,0% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

4.1.2. Tablas y gráficos de niveles de las dimensiones de la variable Calidad de servicio de las redes.

Tabla 8

Niveles de Infraestructura tecnológica

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 3 - 6	2	33,3	33,3	33,3
	Alto 11 - 15	4	66,7	66,7	100,0
	Total	6	100,0	100,0	

Fuente: Elaboración propia.

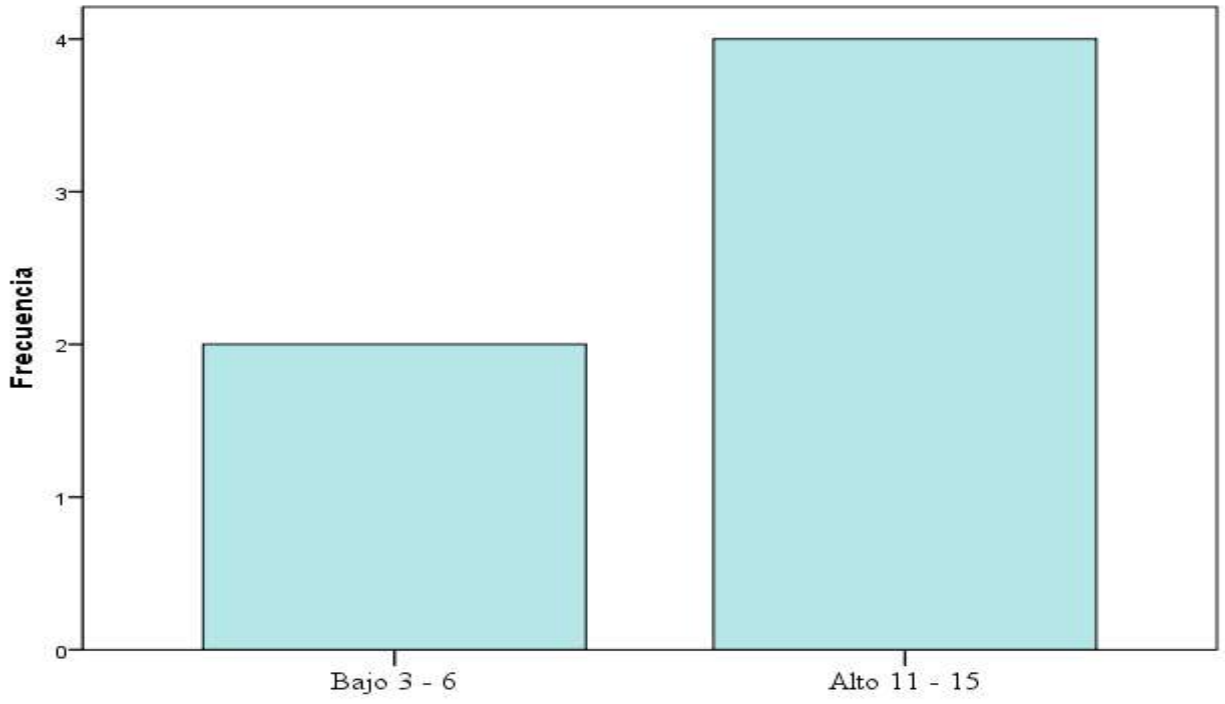


Figura 6. Niveles de infraestructura tecnológica

Fuente: Elaboración propia.

La dimensión Infraestructura tecnológica tiene 3 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo <= 6, medio 7 - 10 y alto 11 - 15. De los 6 datos, el 33,3% de los trabajadores calificó la dimensión infraestructura tecnológica en un nivel bajo y el 66,7% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

Tabla 9

Niveles de Capacidad de respuesta

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Medio 5 - 7	2	33,3	33,3	33,3
	Alto 8 - 10	4	66,7	66,7	100,0
	Total	6265	100,0	100,0	

Fuente: Elaboración propia.

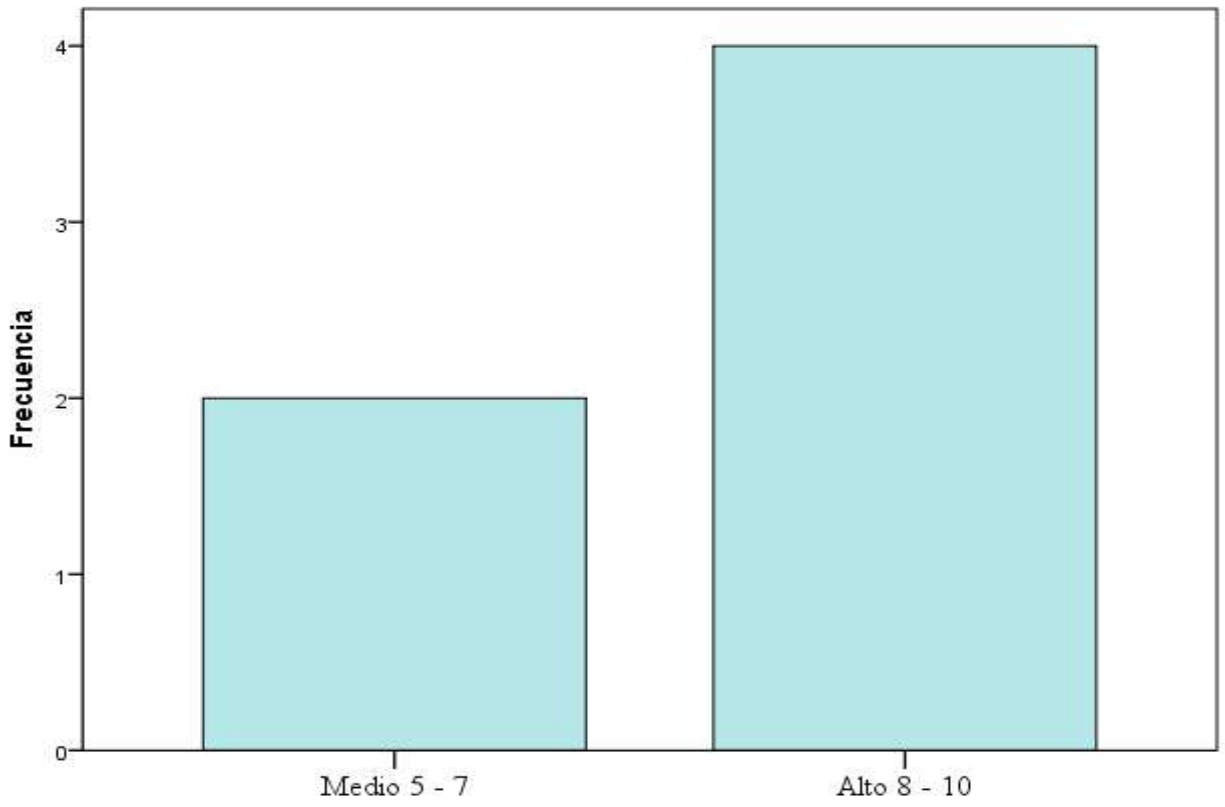


Figura 7. Niveles de capacidad de respuesta

Fuente: Elaboración propia.

La dimensión Capacidad de respuesta tiene 2 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo <= 4, medio 5 - 7 y alto 8 - 10. De los 6 datos, el 33,3% de los trabajadores calificó la dimensión capacidad de respuesta en un nivel medio y el 66,7% en un nivel alto, obteniendo la mayor dispersión en el nivel alto.

Tabla 10
Niveles de Fiabilidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo 2 - 4	1	16,7	16,7	16,7
	Medio 5 - 7	3	50,0	50,0	66,7
	Alto 8 - 10	2	33,3	33,3	100,0
	Total	6	100,0	100,0	

Fuente: Elaboración propia.

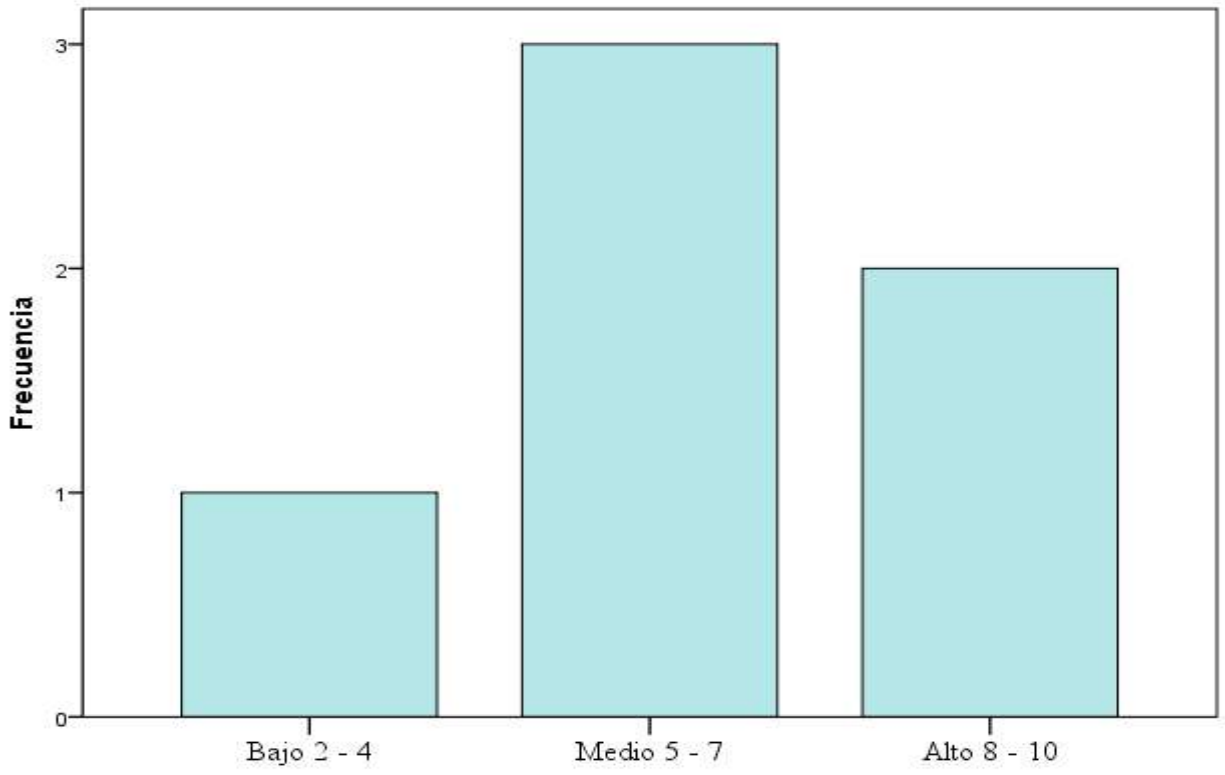


Figura 8. Niveles de fiabilidad
Fuente: Elaboración propia.

La dimensión Fiabilidad tiene 2 preguntas dentro del cuestionario de encuesta, hemos establecido una escala de tres niveles para esta dimensión siendo éstas: bajo <= 4, medio 5 - 7 y alto 8 - 10. De los 6 datos, el 16,7% de los trabajadores calificó la dimensión fiabilidad en un nivel bajo, el 50,0% en un nivel medio y el 33,3% en un nivel alto, obteniendo la mayor dispersión en el nivel medio.

4.1.3. Prueba de normalidad.

Planteamos la hipótesis de normalidad:

Ho: La distribución de la muestra sigue una distribución normal.

H1: La distribución de la muestra no sigue una distribución normal.

Establecemos el nivel de significancia:

El nivel de significancia establecido es de 0,05 y el nivel de confianza es de 95%.

Establecemos la regla de decisión:

Si p < 0,05: Se rechaza Ho

Si p >= 0,05: Se acepta Ho

Elección de la prueba estadística:

Como prueba estadística se eligió el Test de Shapiro - Wilk porque es aplicada para muestras menores a 50 (n<50), y en el caso de la presente investigación la muestra es igual a 6.

4.1.3.1. Calcular la nueva significación de las variables Sistema de gestión de seguridad de la información y Base de datos.

Al utilizar el SPSS, hallamos las nuevas significancias:

Tabla 11
Prueba de normalidad de las variables Sistemas de gestión de seguridad de la información y Base de datos

	Shapiro - Wilk		
	Estadístico	gl	Sig.
Sistema de gestión de seguridad de la información	,875	6	,249
Base de datos	,904	6	,399

Fuente: Elaboración propia.

Decisión:

Nueva significancia de la variable Sistema de gestión de la información = 0,249

0,249 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Nueva significancia de la variable Calidad de servicio = 0,000

0,399 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Interpretación:

Se tomó el estadístico de Shapiro - Wilk, porque la muestra es de 6 trabajadores, el cual muestra unas significancias de ambas variables mayores que 0,05 por lo que se acepta la hipótesis Ho y se rechaza la hipótesis H1, eso indica que la muestra tiene distribución de probabilidad normal, por lo que se concluye con que el análisis debe utilizar pruebas paramétricas.

4.1.3.2. Calcular la nueva significación de las dimensiones de la variable Sistemas de gestión de seguridad de la información.

Al utilizar el SPSS, hallamos las nuevas significancias:

Tabla 12
Prueba de normalidad de las dimensiones de la variable Sistemas de gestión de seguridad de la información

	Shapiro - Wilk		
	Estadístico	gl	Sig.
Integridad de la información	,925	6	,540
Disponibilidad de la información	,831	6	,111
Confidencialidad de la información	,847	6	,150

Fuente: Elaboración propia.

Decisión:

Nueva significancia de la dimensión Integridad de la información = 0,540

0,540 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Nueva significancia de la dimensión Disponibilidad de la información = 0,111

0,111 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Nueva significancia de la dimensión Confidencialidad de la información = 0,150

0,150 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Interpretación:

Se tomó el estadístico de Shapiro - Wilk, porque la muestra es de 6 trabajadores, el cual muestra unas significancias de ambas variables mayores que 0,05 por lo que se acepta la hipótesis Ho y se rechaza la hipótesis H1, eso indica que la muestra tiene distribución de probabilidad normal, por lo que se concluye con que el análisis debe utilizar pruebas paramétricas.

4.1.3.3. Calcular la nueva significación de las dimensiones de la Base de datos.

Al utilizar el SPSS, hallamos las nuevas significancias:

Tabla 13

Prueba de normalidad de las dimensiones de la variable Base de datos

	Shapiro - Wilk		
	Estadístico	gl	Sig.
Infraestructura tecnológica	,828	6	,103
Capacidad de respuesta	,863	6	,201
Fiabilidad	,955	6	,783

Fuente: Elaboración propia.

Decisión:

Nueva significancia de la dimensión Infraestructura tecnológica = 0,103

0,103 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Nueva significancia de la dimensión Capacidad de respuesta = 0,201

0,201 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Nueva significancia de la dimensión Fiabilidad = 0,783

0,783 >= 0,05 se acepta Ho, demostrando que la distribución de la muestra sigue una distribución normal.

Interpretación:

Se tomó el estadístico de Shapiro - Wilk, porque la muestra es de 6 trabajadores, el cual muestra unas significancias de ambas variables mayores que 0,05 por lo que se acepta la hipótesis Ho y se rechaza la hipótesis H1, eso indica que la muestra tiene distribución de probabilidad normal, por lo que se concluye con que el análisis debe utilizar pruebas paramétricas.

4.2. Contrastación de hipótesis

4.2.1. Hipótesis general.

Formulación de hipótesis para contrastar:

H1: El sistema de gestión de seguridad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

H0: El sistema de gestión de seguridad de la información no se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra sigue una distribución normal, se eligió el modelo de correlación de Coeficiente de Pearson como prueba estadística para poder establecer si existe una relación entre el SGSI y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 14
Correlación entre ambas variables

		Sistema de gestión de seguridad de la información	Base de datos
Sistema de gestión de seguridad de la información	Correlación de Pearson	1	,860*
	Sig. (bilateral)	.	,028
	N	6	6
Base de datos	Correlación de Pearson	,860*	1
	Sig. (bilateral)	,028	.
	N	6	6

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,860 y un Valor p = 0,028

Toma de la decisión:

Como regla de decisión se estableció que si el valor p < 0,05 se acepta H1 y se rechaza H0. Como el valor p = 0,028 y 0,028 < 0,05 se acepta la H1 y se rechaza la H0.

Interpretación del p-valor:

Como el valor p = 0,028 y 0,028 < 0,05 se afirma, con un 95% de confianza, que el SGSI se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, obteniendo una correlación positiva alta de 0,860.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor p = 0,028 y ser menor a 0,05 teniendo una correlación positiva alta de 0,860 por lo que se acepta H1, por lo tanto, se puede afirmar que el sistema de gestión de seguridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

4.2.2. Hipótesis específica 1.

Formulación de hipótesis para contrastar:

H1: La integridad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

H0: La integridad de la información no se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra sigue una distribución normal, se eligió el modelo de correlación de Coeficiente de Pearson como prueba estadística para poder establecer si existe una relación entre el SGSI y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 15

Correlación entre la integridad de la información y la base de datos

			Integridad de la información	Base de datos
	Integridad de la información	Correlación de Pearson	1	,875*
		Sig. (bilateral)	.	,022
		N	6	6
	Base de datos	Correlación de Pearson	,875*	1
		Sig. (bilateral)	,022	.
		N	6	6

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,875 y un Valor p = 0,022

Toma de la decisión:

Como regla de decisión se estableció que si el valor p < 0,05 se acepta H1 y se rechaza H0. Como el valor p = 0,022 y 0,022 < 0,05 se acepta la H1 y se rechaza la H0.

Interpretación del p-valor:

Como el valor p = 0,022 y 0,022 < 0,05 se afirma, con un 95% de confianza, que la integridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, obteniendo una correlación positiva alta de 0,875.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor p = 0,022 y ser menor a 0,05 teniendo una correlación positiva alta de 0,875 por lo que se acepta H1, por lo tanto, se puede afirmar que la integridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

4.2.3. Hipótesis específica 2.

Formulación de hipótesis para contrastar:

H1: La disponibilidad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

H0: La disponibilidad de la información no se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra sigue una distribución normal, se eligió el modelo de correlación de Coeficiente de Pearson como prueba estadística para poder establecer si existe una relación entre el SGSI y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 16

Correlación entre la disponibilidad de la información y la base de datos

		Disponibilidad de la información	Base de datos
Disponibilidad de la información	Correlación de Pearson	1	,857*
	Sig. (bilateral)	.	,029
	N	6	6
Base de datos	Correlación de Pearson	,857*	1
	Sig. (bilateral)	,029	.
	N	6	6

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,857 y un Valor p = 0,029

Toma de la decisión:

Como regla de decisión se estableció que si el valor p < 0,05 se acepta H1 y se rechaza H0. Como el valor p = 0,029 y 0,029 < 0,05 se acepta la H1 y se rechaza la H0.

Interpretación del p-valor:

Como el valor p = 0,029 y 0,029 < 0,05 se afirma, con un 95% de confianza, que la disponibilidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, obteniendo una correlación positiva alta de 0,857.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor p = 0,029 y ser menor a 0,05 teniendo una correlación positiva alta de 0,857 por lo que se acepta H1, por lo tanto, se puede afirmar que la disponibilidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

4.2.4. Hipótesis específica 3.

Formulación de hipótesis para contrastar:

H1: La confidencialidad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

H0: La confidencialidad de la información no se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Establecer el nivel de significancia:

El nivel de significancia establecido fue de 0,05. Si el valor P es inferior al nivel de significación, entonces se rechaza la H0. El resultado será más significativo cuanto menor sea el valor P.

Elección de la prueba estadística:

Debido a que la distribución de la muestra sigue una distribución normal, se eligió el modelo de correlación de Coeficiente de Pearson como prueba estadística para poder establecer si existe una relación entre el SGSI y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, y que dicha relación no se debe al azar, sino que es una relación estadísticamente significativa.

Tabla 17

Correlación entre la confidencialidad de la información y la base de datos

		Confidencialidad de la información	Base de datos
Confidencialidad de la información	Correlación de Pearson	1	,821*
	Sig. (bilateral)	.	,045
	N	6	6
Base de datos	Correlación de Pearson	,821*	1
	Sig. (bilateral)	,045	.
	N	6	6

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: Elaboración propia.

Se halló una correlación de 0,821 y un Valor p = 0,045

Toma de la decisión:

Como regla de decisión se estableció que si el valor p < 0,05 se acepta H1 y se rechaza H0. Como el valor p = 0,045 y 0,045 < 0,05 se acepta la H1 y se rechaza la H0.

Interpretación del p-valor:

Como el valor p = 0,045 y 0,045 < 0,05 se afirma, con un 95% de confianza, que la confidencialidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, obteniendo una correlación positiva alta de 0,821.

Conclusión:

Se demostró que la hipótesis alterna es verdadera al hallar el valor p = 0,045 y ser menor a 0,05 teniendo una correlación positiva alta de 0,821 por lo que se acepta H1, por lo tanto, se puede afirmar que la confidencialidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Capítulo V. Discusión

5.1. Discusión de resultados

Para el desarrollo de la discusión de los resultados de la presente investigación, se tuvo en cuenta las investigaciones consideradas como la base y antecedentes de esta investigación y a las conclusiones a las que llegaron sus autores.

Con esta investigación quedó demostrado estadísticamente que existe una relación positiva alta entre el SGSI se relaciona y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, con un 95% de probabilidad, un coeficiente de 0,860 y una significancia de 0,028, al obtener una relación positiva alta coincidiendo con la investigación de Guardia (2020) quien realizó una investigación llamada "Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Publico Eleazar Guzmán Barrón - Huaraz - 2018", en que el SGSI permite la implementación de los mecanismos y controles para reducir el riesgo a un nivel mínimo o aceptable.

La presente investigación también coincide con la investigación de Valverde (2018) titulada "Seguridad de la información aplicando el ISO 27001:2013 para la oficina de Registros y archivos académicos de la Universidad Nacional del Callao 2017" quién demostró que la confidencialidad de la seguridad de la información aumentó de 67% a 97%, la disponibilidad aumentó de 28% a 95% y la integridad aumentó considerablemente de 17 % a 95%; con la investigación de Vegas (2019) titulada "Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001" quién concluyó con que es necesario la implementación de un SGSI; y con la investigación de Ponce (2023) titulada "Sistema de gestión de seguridad de la información para

la Protección de datos en una inmobiliaria, Lima 2022" quien demostró que un SGSI maximiza la protección de la data de una organización.

Además, con la investigación de Akly (2019) titulada "Modelo de Seguridad basado en la Norma ISO/IEC 27001/2013, para minimizar los riesgos en la seguridad lógica de la información" coincidimos con que la implementación de la seguridad de la información permite minimizar los riesgos de la seguridad lógica de la información, implementando controles como seguridad de contraseñas, contra código malicioso, seguridad de información, gestión de privilegios, contra manipulación de aplicaciones, capacitaciones y contra amenazas ambientales y naturales; y con la investigación de Arroyo (2019) titulada "Diseño de un plan de gestión de la seguridad y de la información para el sistema de intranet de la Prefectura de Esmeraldas, basado en estándares internacionales" quién también concluyó con que hay que implementar controles para el tratamiento de riesgos y así prevenir situaciones no deseadas con el manejo de la información.

Con Guerra (2020), quien desarrolló una tesis llamada "Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la biblioteca de la Universidad de la Costa", coincidimos con que implementar un SGSI permite identificar los riesgos asociados a cada proceso, así como conocer el nivel de su impacto para ser evaluado, de acuerdo a las amenazas y vulnerabilidades, además se deben implementar controles para reducir o mitigar los riesgos de los procesos.

Con la investigación de Chaverra (2021) titulada "Diseño del sistema de gestión de seguridad de la información para los procesos de administración de bases de datos y administración de hosting de aplicaciones de la Empresa Softdev LTDA., basado en la norma ISO IEC 27001:2013" coincidimos con que, mediante el SGSI se administra correctamente toda la información de los procesos internos y éste apoya el cumplimiento de los objetivos

estratégicos de la compañía, debido a que minimiza la afectación de la confidencialidad, integridad y disponibilidad de los activos de información críticos de la organización.

Capítulo VI. Conclusiones y recomendaciones

6.1. Conclusiones

Se afirma que el sistema de gestión de seguridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, debido a que los resultados que se obtuvieron demuestran, con un 95% de probabilidad, que si existe una correlación positiva alta entre ambas variables (R= 0,860; p=0,028 < 0,05).

Se afirma que la integridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, debido a que los resultados que se obtuvieron demuestran, con un 95% de probabilidad, que si existe una correlación positiva alta de 0,875 entre ambos.

Se afirma que la disponibilidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, debido a que los resultados que se obtuvieron demuestran, con un 95% de probabilidad, que si existe una correlación positiva alta de 0,857 entre ambos.

Se afirma que la confidencialidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, debido a que los resultados que se obtuvieron demuestran, con un 95% de probabilidad, que si existe una correlación positiva baja de 0,821 entre ambos.

6.2. Recomendaciones

Debido a que se llegó a la conclusión de que el sistema de gestión de seguridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, se recomienda supervisar constantemente el cumplimiento de los procedimientos y controles de seguridad de la base de datos como la actualización del análisis de riesgos y su tratamiento, de ésta manera podemos garantizar que la información que contiene la base de datos esté libre de cualquier incidente.

Debido a que se llegó a la conclusión de que la integridad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, se recomienda constante capacitación al personal acerca del uso de los sistemas de información y sobre los diferentes procedimientos y controles que debe cumplir para el óptimo manejo de la información, evitando incidentes contra la integridad de la información que pueden ser ocasionados por el descuido o error involuntario del propio personal, o causado por ataques informáticos externos.

Debido a que se llegó a la conclusión de que la disponibilidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023, se recomienda dar mantenimiento a los diferentes equipos y dispositivos donde se almacena y procesa la información que contiene la base de datos, además contar con planes de contingencia que garanticen tener siempre la disponibilidad de la información.

Debido a que se llegó a la conclusión de que la confidencialidad de la información se relaciona con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes

Indacochea Lozano en el 2023, se recomienda capacitar al personal que trata con información estratégica o sensible, acerca de los procedimientos y controles para el cuidado óptimo de la confidencialidad de la información, además de capacitarlos sobre la legislación nacional sobre protección de datos personales, que ellos deben de cumplir para no cometer ninguna infracción o delito.

Capítulo VII. Referencias

7.1. Fuentes bibliográficas

Akly, F. (2019). *Modelo de Seguridad basado en la Norma ISO/IEC 27001/2013, para minimizar los riesgos en la seguridad lógica de la información* (Tesis de posgrado). Universidad Autónoma Gabriel Rene Moreno, Santa Cruz, Bolivia.

Arias, E. (2019). *Plan de mejoramiento de la calidad del servicio y satisfacción de los usuarios del Gobierno Autónomo Descentralizado Municipal de Sucumbíos por el periodo septiembre 2018 – febrero 2019* (Tesis de pregrado). Universidad Central del Ecuador, Quito, Ecuador.

Arroyo, A. (2019). *Diseño de un plan de gestión de la seguridad y de la información para el sistema de intranet de la Prefectura de Esmeraldas, basado en estándares internacionales* (Tesis de pregrado). Pontificia Universidad Católica del Ecuador, Esmeraldas, Ecuador.

Blaz, N. y Miranda, R. (2017). *Sistema informático basado en plataforma web para mejorar el proceso de Gestión Documental en una Facultad de la Universidad Nacional de Ucayali* (Tesis de pregrado). Universidad Nacional de Ucayali, Ucayali, Perú.

Cáceda, C. (2021). *Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación* (Tesis de posgrado). Universidad Nacional Mayor de San Marcos, Lima, Perú.

Camapaza, A. (2019). *Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la Municipalidad del Centro Poblado de Salcedo - Puno* (Tesis de pregrado). Universidad Andina del Cusco, Cusco, Perú.

Carreño, M. (2019). *Inteligencia de negocios y el monitoreo de servidores en el Centro de Datos de una Empresa de Cloud, Lima - 2019* (Tesis de pregrado). Universidad Nacional José Faustino Sánchez Carrión, Huacho, Perú.

Castro, J. (2018). *Implementación de la NTP ISO/IEC 27001:2014 para mejorar la gestión de la seguridad en los sistemas de información de la autoridad Portuaria Nacional, Callao - 2017* (Tesis de pregrado). Universidad Autónoma del Perú, Lima, Perú.

Ccesa, M. (2017). *Diseño de un sistema de gestión de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016* (Tesis de pregrado). Universidad Nacional de San Cristóbal de Huamanga, Ayacucho, Perú.

Chaverra, J. (2021). *Implementación de sistema de gestión de la seguridad de la información para el aseguramiento del proceso de ingreso de notas en un portal web universitario* (Tesis de pregrado). Universidad de San Buenaventura, Medellín, Colombia.

Fuentes, R. (2020). *Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca* (Tesis de pregrado). Universidad Nacional de Cajamarca, Cajamarca, Perú.

Garcés, O. y Moreno, J. (2019). *Diseño del sistema de gestión de seguridad de la información para los procesos de administración de bases de datos y administración de hosting de aplicaciones de la Empresa Softdev LTDA., basado en la norma ISO IEC 27001:2013* (Tesis de posgrado). Universidad Piloto de Colombia, Bogotá, Colombia.

Godoy, R. (2014). Seguridad de Información. Guatemala: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica.

Guardia, R. (2020). *Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Publico Eleazar Guzmán Barrón - Huaraz - 2018* (Tesis de posgrado). Universidad Nacional Santiago Antúnez de Mayolo, Huaraz, Perú.

Guerra, E. (2020). *Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la Biblioteca de la Universidad de la Costa* (Tesis de pregrado). Universidad de la Costa, Barranquilla, Colombia.

Huincho, W. (2019). *Sistema de gestión de seguridad de la información para mejorar la protección informática de la Comisaria Región Huancavelica* (Tesis de pregrado). Universidad Nacional Daniel Alcides Carrión, Cerro de Pasco, Perú.

Jiménez, D. (2016). *Bases de datos multidimensionales y su incidencia en la Gestión Procesal para la toma de decisiones de la Fiscalía Provincial de Napo* (Tesis de posgrado). Universidad Técnica de Ambato, Ambato, Ecuador.

Méndez, M. (2021). *Diseño de un sistema gestión de seguridad de información para proteger los activos de información del servicio de administración tributaria de la zona norte del Perú* (Tesis de posgrado). Universidad Privada del Norte, Trujillo, Perú.

Monfil, A. (2018). *Análisis y diseño de técnicas de replicación de una base de datos híbrida y distribuida en un ambiente de ancho de banda limitado* (Tesis de pregrado). Instituto de Investigación y Desarrollo Tecnológico de la Armada de México, Veracruz, México.

Morejón, M. (2018). *La información en bases de datos NOSQL y su incidencia en la generación documental de la Secretaría General del Honorable Consejo*

Universitario (Tesis de posgrado). Universidad Técnica de Ambato, Ambato, Ecuador.

Narro, S. (2021). *El sistema de gestión de seguridad de la información y la gestión de riesgos en el área informática de una universidad pública, Región Cajamarca 2020* (Tesis de posgrado). Universidad Privada del Norte, Trujillo, Perú.

Osorio, L. (2016). *Gestión de Riesgos de Seguridad de la Información en el Sector Público*. Universidad Piloto de Colombia, Bogotá, Colombia.

Ponce, A. (2023). *Sistema de gestión de seguridad de la información para la Protección de datos en una inmobiliaria, Lima 2022* (Tesis de pregrado). Universidad César Vallejo, Trujillo, Perú.

Retuerto, A. (2017). *El compromiso organizacional y la calidad de servicio de los trabajadores de la municipalidad del distrito de Comas en el año 2016* (tesis de posgrado). Universidad Cesar Vallejo, Lima, Perú.

Sandoval, J. (2017). *Diseño de un plan de seguridad de la información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, periodo 2015.2018* (Tesis de pregrado). Universidad Nacional de Piura, Piura, Perú.

Silva, A. (2022). *Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021"* (Tesis de pregrado). Universidad Tecnológica del Perú, Lima, Perú.

Trinidad, M. (2019). *Sistema de Información Gerencial y la Gestión Administrativa de la Institución Educativa Honores del distrito de San Martin de Porres, 2018* (tesis de posgrado). Universidad Peruana de las Américas, Lima, Perú.

Trujillo, W. (2020). *Diseño de controles y políticas para la seguridad de la información en la red Lan en el Hotel Pipatón (*Tesis de pregrado). Universidad Nacional Abierta y a Distancia - UNAD, Santander, Colombia.

Valverde, I. (2018). *Seguridad de la información aplicando el ISO 27001:2013 para la oficina de Registros y archivos académicos de la Universidad Nacional del Callao 2017* (Tesis de pregrado). Universidad Nacional del Callao, Lima, Perú.

Vegas, I. (2019). *Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001* (Tesis de pregrado). Universidad Nacional de Piura, Piura, Perú.

Vergara, G. (2017). *Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016* (Tesis de posgrado). Universidad Nacional Federico Villarreal, Lima, Perú.

7.2. Fuentes hemerográficas

Arévalo, F., Cedillo, I., y Moscoso, S. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Revista Killkana Técnica*, 1(2), 31-42.

7.3. Fuentes electrónicas

Norma ISO 27001 (2013). *Sistema de Gestión de Seguridad de Información (SGSI)*. Recuperado de: https://www.iso27000.es/

Diario El Noticiero (2023). *Aumentan los detenidos por delitos informáticos en Perú*. Recuperado de: https://diarioelnoticiero.com/aumentan-los-detenidos-por-delitos-informaticos-en-peru/

ANEXOS

Anexo N°1: Matriz de consistencia

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS DE LA INSTITUCIÓN EDUCATIVA ESTATAL Nº20827 MERCEDES INDACOCHEA LOZANO - 2023

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIONES	INDICADORES	METODO Y TECNICAS
Problema General ¿Cuál es el nivel de relación entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023?	**Objetivos General** Determinar el nivel de relación que existe entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.	**Hipótesis General** El sistema de gestión de seguridad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.	Sistema de gestión de seguridad de la información (X)	X.1.- Integridad de la Información. X.2.- Disponibilidad de la Información. X.3.- Confidencialidad de la Información.	X.1.1.- Seguridad de la comunicación. X.1.2.- Gestión de incidentes. X.1.3.- Seguridad de los procedimientos. X.2.1.- Acceso a la información en el tiempo requerido. X.2.2.- Continuidad del negocio. X.2.3.- Procedimientos de respaldo. X.3.1.- Niveles de accesibilidad. X.3.2.- Autenticación. X.3.3.- Autorización.	**Población:** Los 06 Trabajadores que acceden a la base de datos. **Muestra:** Los 06 Trabajadores que acceden a la base de datos. **Nivel de la investigación:** Correlacional. **Tipo de investigación:** Esta investigación realiza un estudio aplicado . **Método de la investigación:** Deductivo. **Diseño de la investigación:** No experimental de tipo Transversal.
Problemas Específicos **1.** ¿Cuál es el nivel de relación entre la integridad de la información y la base de datos de la Institución	**Objetivos Específicos** **1.** Determinar el nivel de relación que existe entre la integridad de la información y la base de datos de la Institución Educativa	**Hipótesis Específicos** **1.** La integridad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal	Base de datos (Y)	Y.1.- Infraestructura tecnológica. Y.2.- Capacidad de respuesta.	Y.1.1.- Software. Y.1.2.- Hardware. Y.2.1.- Tiempo de respuesta. Y.2.2.- Mejora continua.	

Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023? **2.** ¿Cuál es el nivel de relación entre la disponibilidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023? **3.** ¿Cuál es el nivel de relación entre la confidencialidad de la información la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023?	Estatal Nº20827 Mercedes Indacochea Lozano en el 2023. **2.** Determinar el nivel de relación que existe entre la disponibilidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023. **3.** Determinar el nivel de relación que existe entre la confidencialidad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.	Nº20827 Mercedes Indacochea Lozano en el 2023. **2.** La disponibilidad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023. **3.** La confidencialidad de la información se relaciona significativamente con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.		Y.3.- Fiabilidad.	Y.3.1.- Eficiencia. Y.3.2.- Eficacia.	**Estadístico de prueba:** Pearson **Instrumento:** Cuestionario de encuesta.

Anexo N°2: Denuncias de Delitos Informáticos 2013-2020

Casi el 50% de las denuncias registradas en 7 años corresponden solamente a dos años: **6047 de delitos fueron captados solamente en 2019 y 2020. De esta forma, se visualiza la tendencia creciente** de los delitos, donde ***los registros del 2020*** **son un 846% más que los del 2013 (pasaron de 369 al pico histórico de 3491).**

Anexo N°3: Análisis de riesgos

Activo	Amenaza	Vulnerabilidad	Impacto			Probabilidad	Riesgo	Clasificación del riesgo
			Confidencialidad	Integridad	Disponibilidad			

Nota: La información referida al análisis de riesgo realizada a la Institución Educativa no se puede presentar por ser información confidencial.

Anexo N°4: Instrumento de recolecta de datos

UNIVERSIDAD NACIONAL

"JOSÉ FAUSTINO SÁNCHEZ CARRIÓN"

FACULTAD INGENIERÍA INDUSTRIAL, SISTEMAS E INFORMÁTICA

Escuela Profesional de Ingeniería de Sistemas

Cuestionario para evaluar la relación entre el sistema de gestión de seguridad de la información y la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en el 2023.

Estimado (a) trabajador, agradecemos su ayuda al responder con responsabilidad y honestidad este cuestionario. Por favor, responda a todas las preguntas sin dejar ningún sin contestar.

El objetivo es, recopilar datos para comprender el sistema de gestión de seguridad de la información y su relación con la base de datos de la Institución Educativa Estatal Nº20827 Mercedes Indacochea Lozano en 2023.

Instrucciones: Lea las preguntas cuidadosamente y marque la escala que crea conveniente con un aspa (x).

Escala valorativa.

Muy en desacuerdo	Algo en desacuerdo	Ni de acuerdo ni en desacuerdo	Algo de acuerdo	Muy de acuerdo
1	2	3	4	5

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (X)						
N°	**X.1.- Integridad de la información**	**1**	**2**	**3**	**4**	**5**
1	**X1.1.-** ¿Se documentan, revisan y actualizan adecuadamente los procedimientos para garantizar la integridad de la seguridad de la información?					
2	**X1.2.-** ¿Se mantiene la autenticidad de la información en la institución manteniendo la seguridad de la información?					
3	**X1.3.-** ¿Cumple la institución con los estándares de seguridad de la información para proteger la integridad de la información?					
	X.2.- Disponibilidad de la información					
4	**X2.1.-** ¿Se realizan procedimientos de respaldo de la información periódicamente?					
5	**X2.2.-** ¿La disponibilidad de datos garantiza la continuidad de la empresa?					

6	**X2.3.-** ¿La disponibilidad de la información garantiza el acceso rápido a la información?					
	X.3.- Confidencialidad de la información					
7	**X3.1.-** ¿Se han establecido claramente las responsabilidades y funciones para proteger la confidencialidad de la información?					
8	**X3.2.-** ¿Tienen controles para la autenticación de los usuarios para garantizar la confidencialidad de la información?					
9	**X3.3.-** ¿Es obligatorio obtener permiso para acceder a la información y mantener la confidencialidad?					
BASE DE DATOS (Y)						
	Y.1.- Infraestructura tecnológica					
10	**Y1.1.-** ¿El hardware que soporta la base de datos de la Institución es la adecuada?					
11	**Y1.2.-** ¿El software con que se maneja la base de datos de la Institución es adecuado?					
12	**Y.1.3.-** ¿Está la infraestructura tecnológica de la institución bien condicionada para brindar un servicio de calidad?					
	Y.2.- Capacidad de respuesta					
13	**Y2.1.-** ¿Es aceptable el plazo de respuesta a las solicitudes y requerimientos de información?					
14	**Y2.3.-** ¿Es posible ofrecer mejores servicios a través de la capacidad de respuesta de la base de datos, lo que conduce an una mejora continua de la institución?					
	Y.3.- Fiabilidad					
15	**Y3.1.-** ¿La base de datos ofrece los servicios que se requieren con una alta eficiencia?					
16	**Y3.2.-** ¿La base de datos proporciona los servicios que se requieren con alta eficacia?					

Muchas gracias por tu colaboración

Anexo N°5: Fichas de validación de juicio de expertos.

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS

TÍTULO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS DE LA INSTITUCIÓN EDUCATIVA ESTATAL Nº20827 MERCEDES INDACOCHEA LOZANO - 2023

AUTORES DEL INSTRUMENTO: ANA LIZBET DOMINGUEZ VILELA Y JOSÉ ALEXANDER OYOLA GOMEZ

I. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente 0 - 20				Regular 21 - 40				Bueno 41 - 60				Muy Bueno 61 - 80				Excelente 81 - 100			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulado con lenguaje apropiado																		X		
2. Objetividad	Está expresado en hechos observables																	X			
3. Actualidad	Adecuado al avance de la tecnología.																	X			
4. Organización	Existe una organización lógica																		X		
5. Suficiencia	Comprende los aspectos en cantidad y calidad																	X			
6. Intencionalidad	Adecuado para valorar los aspectos del sistema de gestión de seguridad de la información y la base de datos.																		X		
7. Consistencia	Basado en aspectos teóricos – científicos.																		X		
8. Coherencia	Establece coherencia entre las variables y los indicadores																		X		
9. Metodología	La estrategia responde a los objetivos																			X	
10. Pertinencia	Es útil y adecuado para la investigación																			X	

II. OPINIÓN DE APLICABILIDAD: Proceda a su aplicación.

III. PROMEDIO DE VALORACIÓN: 89,5

Lugar y fecha: Lima, 18 de diciembre del 2024

Firma del Experto Informante
Apellidos y nombres: Flores Cueto, Juan José
DNI N°09593196

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS

TÍTULO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS DE LA INSTITUCIÓN EDUCATIVA ESTATAL Nº20827 MERCEDES INDACOCHEA LOZANO - 2023

AUTORES DEL INSTRUMENTO: ANA LIZBET DOMINGUEZ VILELA Y JOSÉ ALEXANDER OYOLA GOMEZ

I. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente 0 - 20				Regular 21 - 40				Bueno 41 - 60				Muy Bueno 61 - 80				Excelente 81 - 100			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulado con lenguaje apropiado																		X		
2. Objetividad	Está expresado en hechos observables																			X	
3. Actualidad	Adecuado al avance de la tecnología.																	X			
4. Organización	Existe una organización lógica																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																		X		
6. Intencionalidad	Adecuado para valorar los aspectos del sistema de gestión de seguridad de la información y la base de datos.																			X	
7. Consistencia	Basado en aspectos teóricos – científicos.																		X		
8. Coherencia	Establece coherencia entre las variables y los indicadores																			X	
9. Metodología	La estrategia responde a los objetivos																		X		
10. Pertinencia	Es útil y adecuado para la investigación																			X	

II. OPINIÓN DE APLICABILIDAD: Proceda a su aplicación.

III. PROMEDIO DE VALORACIÓN: 91,0

Lugar y fecha: Huacho, 13 de diciembre del 2023

Firma del Experto Informante
Apellidos y nombres: Garrido Oyola, José Antonio
DNI N°15725918

INFORME DE JUICIO DE EXPERTOS DEL INSTRUMENTO DE INVESTIGACIÓN PARA MEDIR EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS

TÍTULO: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA BASE DE DATOS DE LA INSTITUCIÓN EDUCATIVA ESTATAL Nº20827 MERCEDES INDACOCHEA LOZANO - 2023

AUTORES DEL INSTRUMENTO: ANA LIZBET DOMINGUEZ VILELA Y JOSÉ ALEXANDER OYOLA GOMEZ

I. ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente 0 - 20				Regular 21 - 40				Bueno 41 - 60				Muy Bueno 61 - 80				Excelente 81 - 100			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Esta formulado con lenguaje apropiado																	X			
2. Objetividad	Está expresado en hechos observables																		X		
3. Actualidad	Adecuado al avance de la tecnología.																		X		
4. Organización	Existe una organización lógica																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																		X		
6. Intencionalidad	Adecuado para valorar los aspectos del sistema de gestión de seguridad de la información y la base de datos.																		X		
7. Consistencia	Basado en aspectos teóricos – científicos.																		X		
8. Coherencia	Establece coherencia entre las variables y los indicadores																			X	
9. Metodología	La estrategia responde a los objetivos																		X		
10. Pertinencia	Es útil y adecuado para la investigación																			X	

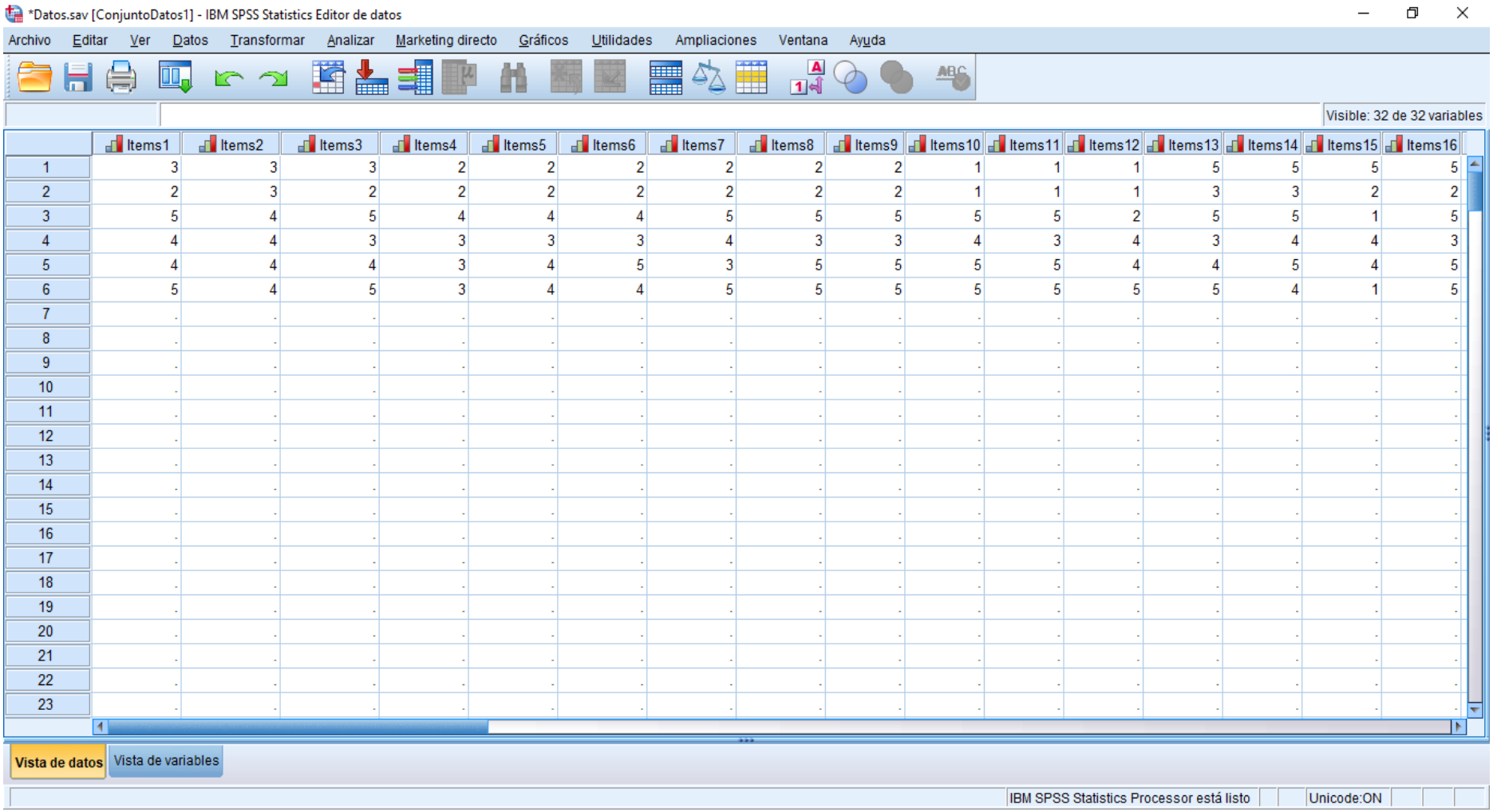
II. OPINIÓN DE APLICABILIDAD: Proceda a su aplicación.

III. PROMEDIO DE VALORACIÓN: 90,0

Firma del Experto Informante
Apellidos y nombres: Nicho Virú, Martín W.
DNI N°15759740

Lugar y fecha: Lima, 14 de diciembre del 2023

Anexo N°6: Tabla de datos en SPSS.



	Items1	Items2	Items3	Items4	Items5	Items6	Items7	Items8	Items9	Items10	Items11	Items12	Items13	Items14	Items15	Items16
1	3	3	3	2	2	2	2	2	2	1	1	1	5	5	5	5
2	2	3	2	2	2	2	2	2	2	1	1	1	3	3	2	2
3	5	4	5	4	4	4	5	5	5	5	5	2	5	5	1	5
4	4	4	3	3	3	3	4	3	3	4	3	4	3	4	4	3
5	4	4	4	3	4	5	3	5	5	5	5	4	4	5	4	5
6	5	4	5	3	4	4	5	5	5	5	5	5	5	4	1	5
7	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
8	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
9	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
10	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
11	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
12	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
13	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
14	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
15	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
17	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
18	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
19	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
20	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
21	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
22	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
23	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.