Universidad Nacional José Faustino Sánchez Carrión

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibri S.A.C. Lima - 2023

Tesis

Para optar el Título Profesional de Ingeniero de Sistemas

Autores

John Ruder Contador Minaya

Cristhian Andre Tapia Huaman

Asesor

Ing. Jorge Antonio Sánchez Guzmán

Huacho – Perú

2024

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

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

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

Facultad de Ingeniería Industrial, Sistemas e Informática

Escuela Profesional de Ingeniería de Sistemas

INFORMACIÓN

DATOS DEL AUTOR (ES):		
NOMBRES Y APELLIDOS	**DNI**	**FECHA DE SUSTENTACIÓN**
John Ruder Contador Minaya	45812505	19/12/2023
Cristhian Andre Tapia Huaman	72882908	19/12/2023
DATOS DEL ASESOR:		
NOMBRES Y APELLIDOS	**DNI**	**CÓDIGO ORCID**
Jorge Antonio Sanchez Guzman	17829652	0000-0002-2387-2296
DATOS DE LOS MIEMROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
NOMBRES Y APELLIDOS	**DNI**	**CODIGO ORCID**
Aldo Felipe Laos Bernal	15614107	0000-0002-5709-3901
Carlos Enrique Bernal Valladares	15614554	0000-0002-7421-9537
Ernesto Diaz Ronceros	46943961	0000-0002-2841-7014

DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA MINERA COLIBRI S.A.C. LIMA – 2023

INFORME DE ORIGINALIDAD

19%	18%	2%	12%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Jose Faustino Sanchez Carrion Trabajo del estudiante	3%
2	repositorio.unjfsc.edu.pe Fuente de Internet	3%
3	hdl.handle.net Fuente de Internet	2%
4	repositorio.uss.edu.pe Fuente de Internet	1%
5	repositorio.upn.edu.pe Fuente de Internet	1%
6	repositorio.udl.edu.pe Fuente de Internet	1%
7	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
8	repositorio.ucv.edu.pe Fuente de Internet	1%

Diseño e Implementación de la ISO 27001 para mejorar

la Seguridad de Información de la empresa minera

COLIBRÍ S.A.C. – Lima 2023

JOHN RUDER CONTADOR MINAYA
CRISTHIAN ANDRE TAPIA HUAMAN

Universidad Nacional José Faustino Sánchez Carrión

Nota del autor:

"Egresados de la Facultad de Ingeniería Industrial, Sistemas e Informática, de la Escuela Profesional de Ingeniería de Sistemas, presentamos la Tesis con la finalidad de obtener nuestro Título Profesional de Ingeniero de Sistemas, esta investigación ha sido desarrollada y financiada económicamente por aportes propios; agradecemos por las contribuciones y asesoría al Ing. Jorge Antonio Sánchez Guzmán en la elaboración de la presente tesis".

ASESOR Y MIEMBROS DE JURADO

_____	_____
Presidente	**Secretario**
_____	_____
Vocal	**Asesor**

DEDICATORIA

En primer lugar, quiero dedicar mi investigación a nuestro Dios que me ha conducido por este camino profesional y a mis padres por ayudarme en mis estudios y haber culminado con satisfacción mi carrera de ingeniero de Sistemas.

A mis abuelitos que siempre admiré por darnos la formación y compartir siempre conmigo muy buenos valores.

Jhon Ruder

DEDICATORIA

Dedicar la culminación de mi Tesis a los maestros que tuve en Ingeniería de Sistemas por inculcarnos sabidurías que hoy me sirven de mucho; a mis lindos padres, mi familia por siempre confiar en mi, para ellos y amistades que ayudaron a mi carrera como profesional.

Cristhian Andre

AGRADECIMIENTO

Nuestro agradecimiento por su contribución a los trabajadores, colaboradores y profesionales de la empresa minera Colibrí S.A.C. que con su contribución se ha logrado captar información y sobre todo porque nos proporcionaron los recursos fundamentales que necesitamos en la presente tesis.

"Agradecer al Ing. Jorge Antonio Sánchez Guzmán, por la asesoría de la tesis, por guiarnos en el proyecto de investigación. Certera y voluntaria gratitud por el interés presentado a nuestra investigación y las contribuciones dadas".

"A los ingenieros especialistas por las calificaciones, recomendaciones y su apoyo en el desarrollo de nuestra investigación, así como validar nuestro instrumento de recolección de información que fueron claves en la evaluación de las variables usadas".

Mencionamos también nuestro agradecimiento a nuestras familias y amistades que contribuyeron y ayudaron a la sabiduría, relaciones e información de la tesis.

Los Autores.

RESUMEN

Objetivo: Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad de Información de la Empresa Minera Colibrí S.A.C. – Lima 2023. **Métodos: "**La Población estuvo constituida por los 70 trabajadores de la Sede Central (oficina Lima de la empresa minera Colibrí S.A.C.) que tienen participación directa para la presente investigación"; en cuanto a la muestra se usó el mismo tamaño de la población; es decir los 70 trabajadores. Se utilizó la Técnica de Observación, Análisis Documental, Encuesta y Entrevista, para medir las mejoras y relación de variables: "Diseño e Implementación de la ISO 27001 para mejorar la Seguridad de Información de la empresa minera Colibrí S.A.C. Con este indicador de alfa de Cronbach se indica que el Cuestionario tiene un 82% de validez". **Resultados**: La empresa cuenta con 30 equipos de cómputo, 3 switch, 3 servidores, 4 router wifi, 1 firewall; faltándole a la empresa equipos certificados (router y switch) que puedan brindar la seguridad que necesita, ese es a nivel red, en nivel usuario falta también con las licencias originales donde es un riesgo alto (virus informáticos y malware) donde se vulnera la información confidencial que maneja dicha empresa y expuestos a multas; si bien es cierto todas las empresas deben estar licenciados en todos los software que puedan utilizar. **Conclusiones:** Con un 95% de confianza se comprobó que si se da una mejora con la implementación de la ISO 27001 y una buena relación con la variable Seguridad de Información de la empresa minera Colibrí S.A.C.

Palabras claves: Diseño e Implementación de la ISO 27001, Seguridad de Información, empresa minera Colibrí S.A.C.

ABSTRACT

Objective: Identify the influence of the Design and Implementation of ISO 27001 in improving the Information Security of the Mining Company Colibrí S.A.C. – Lima 2023. **Methods:** The Population was made up of the 70 workers at the Headquarters (Lima office of the mining company Colibrí S.A.C.) who have direct participation in this investigation; As for the sample, the same population size was used; that is, the 70 workers. The Observation Technique, Document Analysis, Survey and Interview were used to measure the improvements and relationship of variables: Design and Implementation of ISO 27001 to improve the Information Security of the mining company Colibrí S.A.C. This Cronbach's alpha indicator indicates that the Questionnaire has 82% validity. **Results:** The company has 30 computer equipment, 3 switches, 3 servers, 4 Wi-Fi routers, 1 firewall; The company lacks certified equipment (router and switch) that can provide the security it needs, that is at the network level, at the user level it also lacks the original licenses where it is a high risk (computer viruses and malware) where the information is violated confidential that this company manages and exposed to fines; While it is true, all companies must be licensed in all the software they can use. **Conclusions:** With 95% confidence it was proven that there is an improvement with the implementation of ISO 27001 and a good relationship with the Information Security variable of the mining company Colibrí S.A.C.

Keywords: Design and Implementation of ISO 27001, Information Security, mining company Colibrí S.A.C.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

Nuestro Perú es un país donde una de las actividades principales es la minería, logrando ingresos que sirven económicamente de apoyo a los pueblos implementando servicios básicos para su propio desarrollo, así también aportes a otras necesidades como obras y manejo de capacidad laboral a nuestros conciudadanos.

La presente tiene por objeto mejorar la seguridad de información de la empresa Colibrí S.A.C. inferir una relación de 2 variables importantes que resulta necesario para la minera como es el Diseño e Implementación de la ISO 27001 y la Seguridad de Información.

En el capítulo 1, se realizan las formulaciones problemáticas que se descubren cotejándolos a las fuentes de otros estudios donde se usan el diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la empresa minera Colibrí S.A.C. y/o bibliografías, análisis de exploración con herramientas serviles dirigidos a los problemas que se originan en la información confidencial de la minera.

En el capítulo 2, Se examinan y contrastan estudios locales e internacionales en el ámbito teórico para respaldar mi investigación, delineando así los fundamentos y teorías de las variables planteadas (el diseño e implementación de la norma ISO 27001 para fortalecer la seguridad de la información en la empresa minera Colibrí S.A.C.).

En el capítulo 3, Se profundiza en las teorías de compatibilidad, describiendo los elementos clave de los parámetros de investigación, como las hipótesis, variables, diseño y enfoque de investigación, métodos de estudio, población y muestra seleccionada, técnicas de recopilación de datos y método de análisis de contenido.

En el capítulo 4, Se examinan los resultados obtenidos a partir del detallado proceso de aplicación de la ISO 27001 en la empresa minera Colibrí S.A.C. de manera secuencial y fundamentada. Se analizan las implicaciones y descubrimientos derivados, presentándolos en tablas, gráficos y resúmenes estadísticos. Se complementa con pruebas de hipótesis, alineándolos con los

objetivos generales y específicos establecidos previamente. Posteriormente, se realiza la interpretación de estos resultados, validando su coherencia y su correspondencia con las referencias teóricas y hallazgos enunciados en el estudio.

En la sección final del estudio, se condensan las conclusiones destacadas de manera formal, junto con recomendaciones dirigidas a la empresa minera Colibrí S.A.C. y a otras entidades que requieran resguardar su información. Además, en los anexos se incluyen las pruebas y documentos que respaldan y enriquecen la credibilidad del trabajo de investigación.

Los Autores.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Desde la aparición del hombre siempre necesitó protección, cuidado personal por peligros en la naturaleza como los animales feroces, insectos dañinos y fuertes tempestades que de una forma lógica buscó protegerse de ataques y dejar de ser tan vulnerables le hizo frente con herramientas que poco a poco fue perfeccionando.

Con el transcurrir de los años y la multiplicación de la humanidad se presentaron muchas necesidades que el hombre fue superándolo día a día, con nuevas herramientas fue protegiéndose sobre todo para su seguridad. Y el avance de la tecnología brindó muchas mas herramientas, equipos sofisticados que ayudan mucho en las actividades cotidianas.

Hoy, son las empresas que buscan sostenimiento y progreso en este mundo globalizado y competitivo y mediante ésta búsqueda se presentan peligros, riesgos y daños sobre todo en las PCs, aparatos eléctricos que resultan sustanciales en el desempeño empresarial y laboral.

Basado en ello, la presente investigación trata de mostrar unas mejoras en la seguridad de información en la empresa Colibrí SAC de Lima; basado en la norma ISO 27001 que se presta inmejorablemente aplicada a dicha función.

La norma ISO 27001 formula buenas prácticas para la implementación de un sistema de gestión de seguridad de la información. Realizarlo permite proteger los datos de toda organización, que son el activo más importante, sino también genera mucha confianza entre los clientes, proveedores y empleados.

La realidad de la empresa minera Colibrí SAC es que no cuenta con equipo certificados (router y switch) que puedan brindar la seguridad que necesita, ese es a nivel red, en nivel usuario no cuenta con las licencias originales donde es un riesgo alto (virus informáticos y malware) en donde se está vulnerando la información confidencial que maneja dicha empresa y expuestos a una multa por indecopi si bien es cierto todas las empresas deben estar licenciados en todos los software que puedan utilizar.

Es por ello que buscamos aportar mediante este diseño e implementación de la norma ISO 27001 buscando mejorar la seguridad de información en la empresa minera Colibrí SAC de Lima.

En el presente trabajo de investigación con referencia a sistemas de cómputo es muy importante la protección informática, señalando y describiendo métodos de protección, tipos y medios de ataque a nuestro sistema de información en una red de datos de la empresa minera Colibrí SAC. Se pretende informar a los usuarios lo que deben saber para no caer fácilmente en ataques externos o virus informáticos.

1.2 FORMULACIÓN DEL PROBLEMA

1.2.1 Problema general

¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023?

1.2.2 Problemas específicos

- ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023?
- ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023?
- ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo general

Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023.

1.3.2 Objetivos específicos

- Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023.

- Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023.

- Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

La investigación, se justificó, acorde a los aspectos siguientes:

a) **Justificación Teórica:** Cuando se trata de seguridad de información es necesario basarse en fundamentos y teorías recomendadas y fiables que se espera resultados valederos, muy confiables con operaciones que permitan soluciones, trabajos fáciles, accesibles y sobre todo que satisfaga los requerimientos de usuarios o clientes.

En cuanto a la empresa minera Colibrí SAC en las oficinas de Lima, se justifica por aplicar las normas que da la ISO 27001 en el tema de seguridad de información por ser confidencial, disponible e integral.

b) **Justificación Práctica:** Planteamos la seguridad de información basado en la norma ISO 27001 primero en la red, luego en el software y por último en hardware; conocedores del funcionamiento de los equipos como conocemos lo vulnerable a peligros o riesgos de ataques que puede interferir o malograr equipos o la red.

Para ello, de forma práctica se puede ver o buscar la elección de soluciones o prevenciones en cada situación de peligro o daño.

c) **Justificación Económica:** El diseño e implementación que presentamos basado en la norma ISO 27001 busca mejorar la seguridad de información requerida para la empresa minera Colibrí SAC – Lima, que resulta ahorros económicos en cuanto se debe estar prevenido, preparado y operativo para cualquier operación normal porque cuenta con la estrategia necesaria y útil. Si no se aplica la correcta seguridad de información recomendada por ISO 27001, tendría gastos extras de recuperación, reparación, costos y sobre todo pérdida de tiempo que en estos tiempos resulta muy valioso.

d) **Justificación Social:** Nuestra sociedad necesita de un trabajo digno y seguro; además del confort donde labore. Es por ello que basado en reglamentos legales como la norma ISO 27001 muestra apoyo frontal a la seguridad de información previniendo de daños, pérdidas y sobre todo garantizar el normal funcionamiento de equipos, redes y software con la reglamentación o sugerencias cómo y qué debemos hacer. Es por ello que los trabajadores de la empresa minera Colibrí SAC de Lima y los usuarios podrán satisfactoriamente contar con total normalidad emplear y usar las comunicaciones e informaciones.

1.5 DELIMITACIÓN DE LA INVESTIGACIÓN

1.5.1 Delimitación Geográfica

La presente investigación es delimitada en el distrito de San Isidro – Lima. Perú.

1.5.2 Delimitación Temporal

El presente proyecto es desarrollado en el período o año 2023, formulando el diseño e implementación de la ISO 27001 para mejorar la seguridad de información en la empresa minera Colibrí S.A.C. – Lima 2023.

1.5.3 Delimitación de Recursos

Toda investigación necesita inversión tanto económico como tiempo, para ello solo contamos con el aporte de nosotros los investigadores que esforzadamente nos comprometemos a dar los alcances necesarios y poder terminar la presente asumiendo gastos y recursos que se necesitan en la elaboración del proyecto; que con la colaboración de nuestro asesor podemos salir de nuestras limitaciones de los recursos.

1.6 VIABILIDAD

Resulta viable porque, el nivel competitivo en las empresas que se presentan hoy en día, hace buscar nuevas estrategias para aplicarlas a la vanguardia en este mundo competitivo y globalizado; que habido de emprendimiento y sostenimiento es que busca seguridad de sus informaciones para sus usuarios y personal de trabajo, que sean confiables, estén disponibles y sean integrales así como nos recomienda la norma ISO 27001 y que en la presente investigación busca mejorar la seguridad de información basado en situaciones de riesgos y daños que se puedan presentar; pero que siguiendo nuestro planteamiento en el presente diseño e implementación de la ISO 27001 en la empresa minera Colibrí SAC de Lima logrará mejorar la seguridad de la información.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1 Investigaciones Internacionales:

Guano, M. & Jaramillo, M: (2020) realizaron la tesis titulada "Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio". "Escuela Politécnica Nacional – Facultad de Ingeniería de Sistemas. Quito – Ecuador". Para optar el título profesional de Ingeniera en Sistemas Informáticos y de Computación. Objetivo: "Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) para el Hospital de Especialidades Fuerzas Armadas N° 1 (H.E-1)" en base a estándares internacionales, acordes a la realidad de la institución, con el "fin de garantizar que los riesgos de seguridad que la aquejan sean minimizados en base a procedimientos adecuados para su tratamiento, además, lograr una gestión adecuada, de los activos de información a medida que la organización hace uso de nuevas tecnologías de información y comunicaciones para digitalizar y automatizar su información, para así mejorar la calidad de atención a sus usuarios" (p. 30).

Torres, C. (2020) realizó el trabajo de graduación titulado "Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada MEGAPROFER S.A.". "Universidad Técnica de Ambato" – "Facultad de Ingeniería en Sistemas, Electrónica e Industrial" – "Carrera de Ingeniería en Electrónica y Comunicaciones. Colombia. Para optar el título de Ingeniero en Sistemas Computacionales e Informáticos; objetivo: Desarrollar un modelo preventivo estructurado, el Sistema de Gestión de Seguridad de la Información (SGSI), basado en la normativa ISO

27001:2013, con el propósito de diseñar un plan de seguridad informática en la empresa privada Megaprofer S.A. La relevancia de esta acción reside en la información manejada por la empresa, abarcando aspectos como políticas de seguridad, sistemas de control de acceso, gestión de activos y seguridad del personal, entre otros" (p. 30). Se propone la implementación de políticas de seguridad actualizadas y congruentes, alineadas con los estándares institucionales, con el fin de establecer, implementar, mantener y mejorar un SGSI mediante un proceso de mejora continua.

Barrera, J. (2019) realizó la tesis titulada "Propuesta de Sistema de Gestión de Seguridad de la Información utilizando la Norma ISO 27001 para la Unidad Educativa Nuestra Señora de Fátima". Universidad Tecnológica Israel. Quito – Ecuador. Para optar el título profesional de Ingeniero en Sistemas Informáticos. Objetivo: "Proponer un Sistema para la gestión de la Seguridad de la Información basado en la Norma ISO 27001:2013, para esto, se realizó una caracterización del estado de la institución en base a los elementos requeridos por la ISO 27001:2013, se verifico la factibilidad técnica y operacional para materializar la implementación y se generó la propuesta de implementación" (p. 20). "Se observó un 72% de incumplimiento con los requisitos formales de la norma y 78% de incumplimiento de los recaudos asociados al ANEXO A de la misma". Por su parte, "la mayoría de los riesgos detectados se ubicaron dentro de la categoría de Alto y muy alto riesgo, así como un elevado índice de vulnerabilidad de los elementos asociados a el mantenimiento y trasferencia de la información, y de falta de documentación para controlar los procesos asociados al tema, por lo cual se terminó proponiendo un SGI apropiado a las condiciones observadas" (p. 28).

Maureira, D. (2017) realizó la tesis titulada "Norma ISO/IEC 27001 aplicada a una carrera universitaria". Universidad Andrés Bello –

Facultad de Ingeniería. Santiago de Chile. Para optar el título profesional de Ingeniero Civil Informático. Objetivo: ‘‘Pretender plantear las fortalezas y las falencias a la que están expuestos los datos y la información perteneciente a la Universidad, administrativos, académicos y estudiantes, con motivo de entregar y asegurar que se minimicen las vulnerabilidades y riesgos que se pueden presentar” (p. 30). “Esto aumenta cada año a medida que el número de los estudiantes crece, se torna cada vez más difícil la gestión, orden y resguardo de los datos, esto afecta directamente a la continuidad de las actividades que realiza nuestra Universidad, es por este motivo que los encargados del resguardo de estos activos deben tomar conciencia sobre la evaluación, análisis y tratamiento del nivel de riesgo, lo cual permitirá no tener sorpresas inesperadas y en caso de que ocurran llevarlos a valores aceptables” (Pessolani, 2007). “Además, el almacenamiento y el recurrente uso de estos datos deben estar actualizados y seguros. Es así como también se debe tener un especial cuidado con respecto a los documentos generados impresos o electrónicos, los cuales deben ser almacenados de forma segura para evitar que su contenido se revele, manipule o se altere ya que esto puede afectar directamente a la institución tanto a nivel de imagen pública o confianza antes sus alumnos, dañando la credibilidad de la Universidad en relación al manejo de la información o incluso puede llegar dañar la legitimidad en cuanto a la validez de los títulos obtenidos por sus estudiantes” (p. 35).

Yañez, N. (2017) realizó la tesis titulada “Sistema de Gestión de Seguridad de Información para la Subsecretaría de Economía y Empresas de Menor Tamaño”. “Universidad de Chile” – “Facultad de Ciencias Físicas y Matemáticas” – “Departamento de Ciencias de la Computación. Chile. Para optar el grado de Magister en Tecnologías de la Información”. Objetivo: ‘‘Proponer que la metodología de implementación de SGSI se apoye en la gestión de riesgos, utilizando

las guías y buenas prácticas de la norma ISO31000. Con ello los procesos estratégicos de la subsecretaría son clasificados por prioridad según su exposición a los riesgos y su impacto" (p. 32). De este modo se optimiza la asignación de recursos a los proyectos de seguridad de la información, se favorece el aprendizaje y la creación de equipos de trabajo orientados a los objetivos prioritarios, sin que ellos perdieran la visión de conjunto y objetivo final. La presente tesis no cubre la implementación de los 114 objetivos de control de la norma ISO27001, pero cierra las principales brechas de seguridad de la información existentes en la organización al cubrir en forma completa el primer ciclo PDCA del SGSI, escogiendo un subconjunto de 44 objetivos de control priorizados por una análisis de brechas, incorporando las recomendaciones de DIPRES y cuya selección se realizó por un comité de seguridad de la Información constituido en el presente trabajo Las políticas y procedimientos son mantenidos en régimen mediante los seis sistemas que forman el SGSI y cuyo objetivo es administrar, monitorear, documentar y mejorar en forma continua la seguridad de la información La metodología que se utiliza esta tesis, se centra en ciclos de aprobación que permitan establecer consensos y conciliar visiones en torno a un fuerte sentimiento de trabajo en equipo para facilitar la implementación de las políticas y procedimientos de seguridad de la información.

2.1.2 Investigaciones Nacionales:

López, J. (2022) realizó la tesis titulada "Implementación del SGSI, basado en la ISO/IEC 27001 para dar tratamiento al riesgo en una empresa constructora". "Universidad San Ignacio de Loyola – Facultad de Ingeniería – Carrera de Ingeniería Empresarial y de Sistemas. Lima – Perú". Para optar el título de Ingeniero Empresarial y de Sistemas. Objetivo: "El propósito de este proyecto consistía en instaurar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a las pautas de ISO/IEC 27001, específicamente

diseñado para una compañía del sector de la construcción. El enfoque era proteger los recursos de información ante amenazas tanto internas como externas, garantizando su confidencialidad, integridad y disponibilidad" (p. 40). Se buscaba resguardar la información como un activo primordial de la empresa. Esta iniciativa se proyectaba para beneficiar a diversos departamentos, como logística, recursos humanos, finanzas, contabilidad, adquisiciones, operaciones, aspectos legales, ventas y tecnologías de la información.

Reyes, F. (2021) realizó la tesis titulada "Implementación de recomendaciones y el fortalecimiento en el sistema de gestión de seguridad y salud laboral en la empresa minera Yanacocha S.R.L. período 2017 – 2019". "Universidad Nacional de Cajamarca – Escuela de posgrado – Unidad de posgrado de la Facultad de Ciencias Económicas, Contables y Administrativas – Programa de Maestría en Ciencias. Para optar el grado académico de Maestro en Ciencias mención en Auditoría. Cajamarca – Perú". Objetivo: "Determinar si la implementación de recomendaciones realizada por la empresa auditora, fortalece el Sistema de Gestión de Seguridad y Salud laboral en la empresa minera Yanacocha S.R.L., en los periodos comprendidos del 2017 al 2019; diseñado como una investigación aplicada de corte longitudinal y correlacional, utilizando los métodos deductivo- inductivo y analítico-sintético" (p. 45). "En el caso puntual de esta investigación, minera Yanacocha S.R.L. contrató a la empresa auditora Técnica Hurtado E.I.R.L. y con el apoyo del investigador se realizó el seguimiento y el reforzamiento de su sistema de seguridad" (p. 45). "La empresa minera Yanacocha S.R.L dentro de sus políticas de sistema de gestión de riesgos seguridad y salud laboral se administra en cumplimiento de la norma internacional OHSAS 18001, la política corporativa de Newmont y el marco de la legislación peruana como la Ley N° 29783, estos sistemas de gestión periódicamente son sometidos a auditorías" (p. 48).

Ticona, H. (2021) realizó la tesis titulada "Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa ICO el año 2021". "Universidad Privada del Norte – Facultad de Ingeniería – Carrera de Ingeniería de Sistemas Computacionales. Lima – Perú". Para optar el título profesional de Ingeniero de Sistemas Computacionales. Objetivo: "Determinar en qué medida el uso de norma ISO 27001 influye en la seguridad de la información de la empresa ICO, año 2021. En el cuestionario los responsables de los sistemas de recursos empresariales (ERP) proporcionaron información sobre la variable dependiente ISO 27001 y la variable independiente seguridad de la información, mediante la evaluación de sus distintas dimensiones" (p. 50). Ahora bien, "la presente investigación determina que el uso de la ISO 27001 no influye de manera significativa en la mejora la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021 con un nivel de significancia" (p. 65).

Delgado, M. & Vásquez, J. (2019) realizaron una tesis titulada "Modelo de seguridad informática aplicando la norma ISO/IEC 27001 para proteger los activos de información en la empresa Berendson Natación S.R.L.". "Universidad de Lambayeque. Facultad de Ciencias de Ingeniería – Escuela profesional de Ingeniería de Sistemas. Perú. Para optar el Título de Ingeniero de Sistemas". Objetivo: Identificar las deficiencias en la seguridad de la información para desarrollar un modelo alineado con la normativa ISO/IEC 27001, destinado a proteger los activos de la organización y a evaluar tanto riesgos financieros como la confidencialidad y accesibilidad de los datos. "El objetivo principal es establecer un modelo basado en la ISO/IEC 27001 para fortalecer la seguridad informática en BERENDSON NATACION S.R.L. Los objetivos específicos incluyen diagnosticar la situación actual de la empresa en cuanto a amenazas a sus activos, crear un modelo personalizado basado en la norma mencionada y evaluar los resultados tras la implementación de dicho modelo" (p.

40). “La hipótesis plantea que el modelo adaptado de la norma ISO/IEC 27001 mejora la seguridad de los activos de información en BERENDSON NATACION S.R.L” (p. 52).

Vásquez, J. (2018) realizó la tesis titulada “Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI”. “Universidad Nacional Mayor de San Marcos – Facultad de Ingeniería Industrial – Escuela Profesional de Ingeniería Industrial – Perú”. Para optar el Título Profesional de Ingeniero Industrial; objetivo: Establecer directrices y controles para salvaguardar la información crucial dentro de una organización. Garantizar la seguridad de la información en sus tres aspectos: confidencialidad, integridad y disponibilidad, a través de la aplicación de una metodología de evaluación de riesgos que identifique las amenazas que puedan afectar la seguridad de la información en los procesos de Tecnologías de la Información (TI) de GMD®, responsable de gestionar la plataforma tecnológica y el soporte técnico para su cliente "ONP". “La adopción del sistema de gestión ISO 27001:2013 contribuye a proteger la información en los procesos de TI mediante la implementación de directrices y medidas de seguridad. Se detallan las acciones necesarias para implementar adecuadamente este sistema de gestión de seguridad de la información, enfatizando la importancia de concienciar al personal sobre la relevancia de proteger la información que manejan en sus labores diarias” (p. 48).

2.2 BASES TEÓRICAS

2.2.1 Diseño e Implementación de la ISO 27001

La definición más clara de la ISO 27001. Según el blog Advisera (2023):

> "ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2" (p. 24).

Implementar ISO 27001, significa proporcionar metodologías para la seguridad de la información. Según el blog Advisera (2023):

> ISO 27001 "puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización" (p. 28). "También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001" (p. 36).

La norma ISO 27001 es a nivel mundial. Según el blog Advisera (2023), "ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento".

La función principal de la ISO 27001. Según la academia Pirani (2014):

> "La norma ISO 27001 establece buenas prácticas para implementar un sistema de gestión de seguridad de la información. Hacerlo no solo permite proteger los datos de tu organización, que son el activo más importante, sino también generar mayor confianza entre tus clientes, proveedores y empleados" (p. 48).

Figura 01:

ISO 27001: Qué es, para qué sirve y aplicación.

Fuente: Copias de seguridad en la nube

El almacenamiento de información se ve transformado. Según la academia Pirani (2014), "Desde hace algunos años, muchas empresas han comenzado a implementar un proceso de transformación digital, que entre otras cosas requiere del uso de nuevas tecnologías y almacenamiento de la información en la nube y en diferentes dispositivos electrónicos".

Contar con un sistema de gestión de seguridad es vital. Según la academia Pirani (2014):

> Y aunque esto, sin duda, trae muchas ventajas, también genera más exposición a riesgos cibernéticos, "por eso cada vez es más importante contar con un sistema de gestión de seguridad de la

información basado en la norma ISO 27001 para proteger los datos y prevenir las consecuencias que traería la materialización de un riesgo de este tipo".

Como herramienta asegura muy confidencialmente toda la información. Según la academia Pirani (2014):

> En general, esta norma ofrece herramientas que permiten asegurar, integrar y tener de manera confidencial toda la información de la compañía y los sistemas que la almacenan, evitando así que un ciberataque se materialice y así mismo, hacer más competitiva a la empresa y cuidar su reputación.

Confidencialidad de la información

En cuanto a la confidencialidad de la información. Según OSTEC BLOG (2023):

> "Con la creciente cantidad de información almacenada en plataformas digitales, es fundamental que las empresas y organizaciones adopten medidas de protección adecuadas para evitar filtraciones y brechas de seguridad" (p. 31). "Además, la legislación en materia de protección de datos se ha vuelto cada vez más estricta en todo el mundo, lo que refuerza la importancia de la confidencialidad" (p. 32).

Vemos entonces, que hoy en día es muy importante las medidas de protección.

Además, en cuanto a la accesibilidad. Según la norma ISO 27001 (actualización 2022):

> La confidencialidad es uno de los pilares fundamentales de la seguridad de la información según la norma ISO 27001. Este pilar tiene como objetivo garantizar que la información sea

> “accesible solo para personas autorizadas, protegiéndola contra la divulgación no autorizada y el uso indebido. La confidencialidad es especialmente importante para la información confidencial, como los datos personales y financieros” (p. 28).

Muy importante sea confidencial sobre todo en el campo financiero como confidencial en los datos personales.

Como políticas de protección y garantía de la confidencialidad. Según la norma ISO 27001 (actualización 2022):

> “Para garantizar la confidencialidad de la información, la ISO 27001 establece requisitos como el control de acceso, cifrado, implementación de políticas de seguridad de datos y la verificación periódica de los sistemas de seguridad” (p. 55). “Además, es importante que las empresas cuenten con un plan de contingencia para enfrentar incidentes de seguridad que puedan comprometer la confidencialidad de la información” (p. 56).

“La implementación de sistemas con políticas de seguridad y el control de acceso es vital en la confidencialidad de la información”.

Por otro lado, son los usuarios que debe proteger la información. Según OSTEC BLOG (2023):

> También, se debe concientizar a los usuarios sobre la importancia de la confidencialidad y la necesidad de mantener la información protegida. Y establecer políticas claras para el uso y acceso a la información, capacitar a los empleados sobre los riesgos de seguridad y monitorear constantemente el comportamiento de los usuarios.

Podemos decir entonces, que el agente involucrado son los usuarios mantener la información protegida y que cuente con capacidad para ésta importante tarea.

Consecuentemente, se debe garantizar la confidencialidad de la información. Según OSTEC BLOG (2023):

> "La violación de la confidencialidad puede traer serios daños financieros, legales y de imagen a las empresas, además de comprometer la privacidad de los usuarios. Por lo tanto, es fundamental adoptar un enfoque proactivo y sistemático para garantizar la protección de la información y generar confianza en los usuarios y clientes" (p. 78). "La confidencialidad es un pilar esencial para la seguridad de la información y debe ser tratada con la debida importancia y seriedad" (p. 79).

El enfoque debe ser la adopción de un buen diseño sistémico e implantar la seguridad en la información.

En cuanto a los activos. Según pmg-ssi.com (2015), "Los activos son los recursos del Sistema de Seguridad de la Información ISO 27001, necesarios para que la empresa funcione y consiga los objetivos que se ha propuesto la alta dirección".

Se observa que en ISO 27001 valora mucho los activos. Según pmg-ssi.com (2015):

> "Un proyecto de Seguridad tiene como principal objetivo de seguridad los activos que generan el dominio en estudio del proyecto. El límite del conjunto de activos del dominio no imposibilita la consideración de las relaciones en materia de seguridad de dichos activos con el entorno" (p. 86).

Claramente, podemos entender que los activos sirven de mucha relación con la seguridad.

En cuanto a la variedad de los activos. Según pmg-ssi.com (2015), “Cada activo o grupo de activos conlleva diferentes tipos de indicadores de valoración que ofrecen una orientación con lo que poder calibrar el impacto que materializa la amenaza que puede provocar”.

Aspectos de SGSI para la mejora continua:

- La directriz sobre seguridad de la información.
- Los propósitos en materia de seguridad de la información.
- Los desenlaces de las revisiones de auditoría.
- La evaluación de sucesos acontecidos.
- Las medidas correctivas y de anticipación.
- El examen ejecutivo.

Figura 02:

Confidencialidad norma ISO/IEC 27001

Fuente: Blog Kantan Software

Disponibilidad de la Información

“En referencia al campo de la seguridad informática y de la información, la disponibilidad informática es

la característica o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados".

Se debe poner énfasis, inmediata en la disposición y acceso a los datos. Según itconsultors.com (2020):

> "Una gran parte de la gestión de datos es lograr un equilibrio entre la seguridad de los datos y el fácil acceso o disponibilidad a los datos que su equipo necesita para hacer su trabajo. Por ejemplo, los agentes de servicio al cliente necesitan acceso inmediato a los datos del cliente" (p. 75). "Configure permisos de datos basados en roles para que los miembros del equipo obtengan lo que necesitan sin comprometer la seguridad de todo su inventario de datos" (p. 76).

También brindar las herramientas suficientes para disponer de la información. Según itconsultors.com (2020):

> "Brinde a los empleados herramientas para que puedan encontrar rápidamente los datos que necesitan. Por ejemplo, una interfaz de lenguaje natural permite a los empleados preguntar" (p. 16): "¿Qué porcentaje de nuestras ventas fueron widgets increíbles?" Otras herramientas útiles le permiten agregar fácilmente paneles basados en roles.

Deberá siempre revisar o administrar periódicamente. Según itconsultors.com (2020):

> La gestión de datos no es un procedimiento de "configúrelo y olvídese". Revise su plan de administración de datos regularmente para asegurarse de que aún satisfaga las necesidades de su empresa. Las revisiones periódicas también son cruciales para la seguridad de los datos, ya que las amenazas externas solo se vuelven más sofisticadas. Estas técnicas

principales de administración de datos pueden ayudarlo a mantener sus datos accesibles, confiables y seguros.

Figura 03:

Disponibilidad de Información y Almacenamiento

Fuente: Blog Endeavor Technologies Systems

Asegure la calidad revisando y manteniendo datos

El mantenimiento de datos deberá ser un proceso continuo. Según itconsultors.com (2020):

> Es importante revisar y mantener los datos para asegurarse de que está trabajando con conjuntos de datos de calidad. "A diferencia de la limpieza de datos, el mantenimiento de datos es un proceso continuo. Revise y verifique periódicamente sus datos para asegurarse de que sigan siendo confiables y utilizables. Revisar y mantener los datos también hace que su base de datos se ejecute más rápido al eliminar archivos innecesarios" (p. 42).

La base de datos siempre debe ser reconstruida. Según itconsultors.com (2020):

> "Reconstruir los índices de su base de datos es una parte importante del mantenimiento de datos. A medida que elimine

> datos irrelevantes y los verifique, creará fragmentación de índice, lo que provocará lagunas en sus datos y ralentizará el acceso a sus datos" (p. 52).

La administración de datos. Según itconsultors.com (2020): "Use estas técnicas de administración de datos para mantener sus datos limpios y utilizables. Se debe aprender sobre las mejores prácticas de administración de datos, incluida la privacidad, el almacenamiento y el archivado de datos".

Elija el almacenamiento de datos correcto

En cuanto al almacenamiento de información. Según itconsultors.com (2020):

> "La forma en que almacene sus datos afectará qué tan bien los administra. Cuando elige una solución de almacenamiento de datos, puede seleccionar servidores locales, una solución basada en la nube o una combinación de ambos, conocida como almacenamiento híbrido". "El almacenamiento en la nube es una forma asequible de almacenar grandes volúmenes de datos sin comprar servidores caros" (p. 26).

Además, existen varios tipos de almacenamiento de información. Según itconsultors.com (2020):

> También hay varios tipos de almacenamiento local disponibles. El almacenamiento conectado directo, como unidades USB y discos duros externos, se puede conectar directamente a sus computadoras. El almacenamiento conectado a la red (NAS) es el modelo de almacenamiento del servidor central, donde todo se guarda en los servidores y se comparte a través de la red. Algunas compañías todavía usan almacenamiento fuera de línea como copias de seguridad de discos ópticos (CD o DVD) también.

El almacenamiento de información debe ser completamente disponible y seguro. Según itconsultors.com (2020):

> Lo que debe tener en cuenta, independientemente del método de almacenamiento que elija, es la disponibilidad de sus datos y su seguridad. Busque almacenamiento con un alto tiempo de actividad (disponibilidad del 99.999 por ciento), así como respaldo automático y recuperación ante desastres. También necesitará saber cuánto costará obtener más almacenamiento, así como qué tan seguro es. Esto incluye cómo se encripta, tanto cuando se almacena como cuando está en tránsito.

Integridad

La información debe ser intacta y completa. Según blog FIRMA-e (2023):

> El diccionario define el término como "estado de lo que está completo o tiene todas sus partes". "La integridad hace referencia a la cualidad de la información para ser correcta y no haber sido modificada, manteniendo sus datos exactamente tal cual fueron generados, sin manipulaciones ni alteraciones por parte de terceros" (p. 26). "Esta integridad se pierde cuando la información se modifica o cuando parte de ella se elimina, y una gran garantía para mantenerla intacta es, la firma digital" (p. 27).

La información debe ser autentica siendo muy segura. Según blog FIRMA-e (2023):

> Un aspecto relacionado con la integridad es la autentificación, cualidad que permite identificar al generador de la información y que se logra con los correctos accesos de usuario y con otros sistemas como la recientemente mencionada firma electrónica. Para algunos, incluso, la autentificación sería el "cuarto pilar" de la Seguridad de la Información.

Figura 04:

Integridad de datos: definición y problemas

Fuente: Blog Tecnologías – Información

2.2.2 Seguridad de la Información

El cuidado y salvaguarda de la información es fundamental. Según blog pmg-ssi.com (2021):

La seguridad de la información comprende el conjunto de estrategias y procedimientos empleados para supervisar y proteger la totalidad de los datos manipulados en una entidad, asegurando que dicha información permanezca dentro del sistema establecido por la organización. Constituye un elemento fundamental que permite a las empresas llevar a cabo sus operaciones, dado que los datos manejados resultan

Toda organización debe establecer medidas de seguridad. Según blog pmg-ssi.com (2021):

> Es crucial tener presente que toda entidad, sin importar su escala, maneja información confidencial, ya sea de clientes, empleados o de ambas partes, por lo que debe

implementar medidas de seguridad en protección de datos para asegurar su correcto manejo. Esto se convierte, tras la implementación inicial de la LOPD y posteriormente del RGPD, no en una elección, sino en una obligación que deben cumplir.

Figura 05:

La Seguridad de la información: Historia, Terminología y Campo de acción.

Fuente: Blog Desde Linux

Seguridad de la red

"La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos".

- Engloba tecnologías tanto físicas como lógicas.
- Está dirigida hacia diferentes tipos de riesgos.
- Impide la entrada o la difusión a través de la red.
- Un sistema de seguridad de red competente gestiona la entrada a la red.

¿Cómo funciona la seguridad de red?

La seguridad de la red es la aplicación de políticas y control de la defensa. Según blog cisco.com (2023):

> La seguridad de red combina varias capas de defensa en el perímetro y la red. Cada capa de seguridad de red implementa políticas y controles. Los usuarios autorizados tienen acceso a los recursos de red, mientras que se bloquea a los usuarios maliciosos para evitar que ataquen vulnerabilidades y amenacen la seguridad.

¿En qué me beneficia la seguridad de red?

En que los servicios de red a usuarios están protegidos. Según blog cisco.com (2023):

> La digitalización ha transformado al mundo. Ha cambiado nuestra manera de vivir, trabajar, aprender y entretenernos. Todas las organizaciones que quieren prestar los servicios que exigen los clientes y los empleados deben proteger su red. La seguridad de red también ayuda a proteger la información confidencial de los ataques. En última instancia, protege su reputación.

Segmentación de la red

Mucho importa categorizar o segmentar y clasificar. Según blog cisco.com (2023):

> La segmentación definida por software clasifica el tráfico de red en distintas categorías y facilita la aplicación de políticas de seguridad. Lo ideal es que las clasificaciones se basen en la identidad de los EndPoints, no solo en las direcciones IP. Puede asignar derechos de acceso basados en roles, ubicación y demás, de modo que se otorgue el nivel de acceso correcto a las

personas adecuadas y se contengan y reparen los dispositivos sospechosos.

Control de acceso

Debe definirse quienes son los usuarios. Según blog cisco.com (2023):

> No todos los usuarios deben tener acceso a la red. Para evitar posibles ataques, debe reconocer a todos los usuarios y dispositivos. Entonces podrá aplicar las políticas de seguridad. Puede bloquear dispositivos de EndPoint que no cumplen las políticas o proporcionarles acceso limitado. Este proceso se denomina control de acceso a la red (NAC).

Análisis del comportamiento

Se debe contar con herramientas de comportamientos. Según blog cisco.com (2023):

> Para detectar el comportamiento anómalo de la red, primero debe conocer el comportamiento normal. Las herramientas de análisis de comportamiento detectan automáticamente las actividades que se desvían de la norma. El equipo de seguridad entonces puede identificar mejor los indicadores de infiltración que pueden traer problemas y reaccionar rápidamente ante las amenazas.

Seguridad de dispositivos móviles

Tenemos que establecer medidas de seguridad contra los ciberdelincuentes. Según blog cisco.com (2023):

> Los ciberdelincuentes cada vez se centran más en los dispositivos y las aplicaciones móviles. En los próximos 3 años, el 90 por ciento de las organizaciones de TI tendrá aplicaciones

corporativas para dispositivos móviles. Obviamente, debe controlar qué dispositivos pueden acceder a la red. También debe configurar las conexiones para preservar la privacidad del tráfico de red.

Figura 06:

Conoce qué es la seguridad de redes

Fuente: Postgrado UCSP

Seguridad del Software

La seguridad en el software puede ser complejo. Según cpl.thalesgroup.com (2023):

> "Toda empresa de software quiere asegurarse de que sus protocolos de seguridad del software sean de primera categoría. No hay debate en torno a eso" (p. 37). "Pero en el complejo mundo de las tecnologías de la información de hoy, con empresas que utilizan cada vez más software que nunca y ciberataques desenfrenados, asegurarse de que el software sea verdaderamente seguro puede resultar complicado" (p. 38).

La disponibilidad de los softwares hace que elijas la más segura. Según cpl.thalesgroup.com (2023), "El software de seguridad informática está ampliamente disponible en la actualidad y ayuda a las empresas y a los usuarios finales a asegurarse de que están utilizando

el software correcto con las herramientas adecuadas para mantenerse protegidos".

¿Qué es la seguridad del software?

Implementación de mecanismos de seguridad. Según cpl.thalesgroup.com (2023):

> La seguridad de un programa informático implica la integración de medidas durante su desarrollo para mantener su funcionalidad o resistencia ante posibles ataques. Esto implica someter el software a pruebas de seguridad antes de su lanzamiento al mercado, con el fin de evaluar su capacidad para defenderse de potenciales ataques malintencionados.

El software debe ser seguro desde el principio. Según cpl.thalesgroup.com (2023):

> "La idea detrás de la seguridad del software es crear software que sea seguro desde el principio sin tener que agregar elementos de seguridad adicionales para agregar capas adicionales de seguridad (aunque en muchos casos, esto todavía sucede)" (p. 49). "El siguiente paso es enseñar a los usuarios a usar el software de la manera correcta para evitar ser propensos o estar expuestos a ataques" (p. 50).

La buena programación evita daños posteriores. Según cpl.thalesgroup.com (2023):

> La importancia de la seguridad del software radica en que un ataque de software malicioso puede ocasionar graves daños, comprometiendo la integridad, autenticidad y disponibilidad de la pieza de software. Si los desarrolladores consideran esto durante la fase de programación, en lugar de abordarlo más tarde, pueden prevenir los daños antes de que ocurran.

Seguridad del software frente a la seguridad de las aplicaciones

La confianza va generando seguridad primero en el software luego en las aplicaciones. Según cpl.thalesgroup.com (2023), "Los conceptos de seguridad del software y seguridad de aplicaciones a menudo van juntos. De hecho, muchas empresas hoy optan por poner su énfasis en la seguridad de las aplicaciones, como ocurre después del proceso de desarrollo".

La seguridad tiene que ser muy bien manejada por expertos, ingenieros en la programación. Según cpl.thalesgroup.com (2023):

> Esa es la diferenciación importante entre la seguridad de las aplicaciones y la del software. Se deben solucionar las vulnerabilidades de seguridad del software antes de implementarlo y enviarlo a los usuarios finales. Esto requiere esfuerzo y compromiso por parte de programadores e ingenieros en la etapa de desarrollo. Una vez que el producto llega al mercado, puede ser demasiado tarde (o requerir cambios sustanciales en futuras actualizaciones, situación que la mayoría de las empresas prefieren evitar).

¿Por qué es importante la seguridad del software?

La seguridad del software comienza con los desarrolladores para no dañar la empresa. Según cpl.thalesgroup.com (2023):

> Sin un plan establecido, la seguridad del software puede dañar gravemente a una empresa. Como se mencionó, la seguridad del software comienza con los desarrolladores, asegurándose de que el software esté preparado para ataques o cualquier cosa que intente derribarlo. Este proceso está fuera del alcance del usuario final, pero debería ser una parte importante a la hora de decidir en qué piezas de software confiar.

Una vez elegido el software estamos listo para la mejor seguridad. Según cpl.thalesgroup.com (2023), “Después de elegir el software adecuado, es hora de implementar las mejores prácticas de seguridad de software discutidas. Para hacer esto, las organizaciones deben recurrir a soluciones de seguridad de software”.

Figura 07:

Políticas de Seguridad

Fuente: Blog Evaluando Software

Seguridad de Hardware

Su definición de Seguridad de Hardware. Según Grupo Atico34 (2021), “La seguridad informática de hardware es aquella que se refiere a la parte física de los equipos. Es decir, suele tratarse de dispositivos que se conectan al ordenador u otros aparatos informáticos para aumentar su grado de seguridad”.

Es el complemento de la seguridad de software. Según Grupo Atico34 (2021):

> Es uno de los tipos de seguridad informática más importantes, y generalmente se suele utilizar como complemento a la seguridad por software. Gracias a ella, se puede adoptar un enfoque multidimensional de la seguridad informática, basándola no solo en la protección de las aplicaciones, sino también de la infraestructura de los equipos.

Ayuda a detectar y analizar las vulnerabilidades de los equipos y sistemas. Según Grupo Atico34 (2021):

> Algunos de los ejemplos de seguridad de hardware son los firewalls por hardware, los servidores proxy o los módulos de seguridad. También se suele encargar de detectar y analizar las vulnerabilidades de equipos y sistemas, y de establecer las medidas para protegerse frente a cualquier amenaza.

Estrategia de seguridad basada en hardware

Debe estar encaminada a estrategias de protección. Según Grupo Atico34 (2021), "Las medidas de seguridad del hardware deben estar encaminadas a la creación de una estrategia de protección integral, en la que se evite totalmente la vulnerabilidad de los equipos".

La Seguridad de Hardware está en el punto final. Según Grupo Atico34 (2021):

> "Uno de los objetivos de esta estrategia debe ser mejorar la seguridad en el punto final**.** Los ordenadores o dispositivos de un sistema informático son el principal foco de atención de los ciberdelincuentes. Es habitual que los hackers utilicen las vulnerabilidades del software de seguridad para insertar malware en el cortafuegos de los equipos" (p. 58). "Sin embargo, hay sistemas avanzados que ya utilizan la inteligencia artificial y la telemetría del hardware para evitar ataques que de otras formas no podían ser detectados" (p. 59).

La Seguridad de Hardware debe presentar la máxima garantía. Según Grupo Atico34 (2021):

> Otra medida a implementar es garantizar la instalación de un firmware seguro, transparente y que ofrezca las máximas garantías. "Gracias a ello se pueden eliminar los puntos ciegos

> que permiten mayor visibilidad y accesibilidad a las plataformas del sistema. Esto permite crear una infraestructura de IT más fiable y que ofrece un mayor conocimiento de todos los equipos de una misma plataforma" (p. 36).

También es posible control de forma remota. Según Grupo Atico34 (2021):

> Las estrategias de seguridad por hardware también deben estar encaminadas a la creación de entornos gestionados a distancia. Por ejemplo, que se pueda controlar de forma remota el teclado, el ratón o el monitor, para aplicar los parches de seguridad cuando sea necesario, a pesar de no estar físicamente en la ubicación del equipo. Esto supone una gran ventaja a la hora de responder frente a amenazas o para recuperarse más rápidamente frente a posible errores o ataques de denegación de servicio.

La seguridad física del hardware

Su previsión a imprevistos de daños. Según Grupo Atico34 (2021):

> La seguridad física del hardware es crucial para proteger los componentes físicos de un sistema informático o electrónico contra accesos no autorizados, daños o manipulaciones indebidas. Incluye medidas como el control de acceso a las instalaciones donde se encuentra el hardware, el uso de cerraduras, sistemas de alarmas, vigilancia por cámaras, y la implementación de gabinetes o cajas fuertes para resguardar los dispositivos.

Es importante ubicar los equipos en zonas muy seguras. Según Grupo Atico34 (2021):

> Es esencial considerar otros riesgos externos, como la manipulación de dispositivos o el hurto de equipos informáticos. Por esta razón, ubicar los dispositivos en entornos seguros, inaccesibles para personas no autorizadas, resulta fundamental.

La seguridad física también de señales. Según Grupo Atico34 (2021):

> Incluso yendo un paso adicional, podríamos referirnos a lo conocido como seguridad física de emisión. Esto implica resguardar las señales emitidas por el hardware, como la visualización de pantallas de computadoras desde ventanas o la captación de ondas electromagnéticas generadas por los dispositivos, las cuales podrían convertirse en datos accesibles para personas no autorizadas.

La Seguridad de Hardware crea entornos TI. Según Grupo Atico34 (2021), "En definitiva, la seguridad de hardware es imprescindible para crear entornos TI más seguros y garantizar la protección e integridad de los equipos informáticos".

Figura 08:

Seguridad de Hardware para ordenadores de empresas

Fuente: Blog Grupo Atico34

2.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

Amenaza: Según Glosario de términos ISO 27001 (2013), "Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización".

Ataque: Según Glosario de términos ISO 27001 (2013), "Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo".

Autenticación: Según Glosario de términos ISO 27001 (2013), "Es un proceso que garantiza y confirma la identidad de un usuario. La autenticación es uno de los aspectos básicos en la seguridad de la información, junto con los tres pilares, a saber: la integridad, disponibilidad, y confidencialidad".

Autenticidad: Según Glosario de términos ISO 27001 (2013), "Es la seguridad de que un mensaje, una transacción u otro intercambio de información proviene de la fuente de la que afirma ser. Autenticidad implica prueba de identidad".

Confiabilidad: Según Glosario de términos ISO 27001 (2013), "Es un atributo de cualquier sistema de información (software, hardware o una red, por ejemplo) que nos garantiza que el sistema en cuestión tiene un desempeño de acuerdo con sus especificaciones".

Confidencialidad: Según Glosario de términos ISO 27001 (2013), "Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados".

Control de acceso: Según Glosario de términos ISO 27001 (2013), "Medios para garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad".

Control de seguridad: Según Glosario de términos ISO 27001 (2013), "Es una medida de seguridad técnica o administrativa para evitar, contrarrestar o

minimizar la pérdida o falta de disponibilidad debido a las amenazas que actúan por una vulnerabilidad asociada a la amenaza".

Disponibilidad: Según Glosario de términos ISO 27001 (2013), "En el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto".

Estándar e Implementación de Seguridad: Según Glosario de términos ISO 27001 (2013), "Documento que especifica formas autorizadas para realizar la seguridad. La norma ISO/IEC 27001. Esta norma establece los requisitos para que el sistema de gestión de seguridad de la información (SGSI) de una organización pueda ser auditado y certificado".

Evento de Seguridad de la Información: Según Glosario de términos ISO 27001 (2013), "Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad".

Gobernanza de la Seguridad de la Información: Según Glosario de términos ISO 27001 (2013), "Sistema por el cual las actividades de seguridad de la información de una organización son dirigidas y controladas".

Información Documentada: Según Glosario de términos ISO 27001 (2013), "Se refiere a la información necesaria que una organización debe controlar y mantener actualizada tomando en cuenta y el soporte en que se encuentra. Puede estar en cualquier formato (audio, video, ficheros de texto etc.)".

Instalaciones de Procesamiento de Información: Según Glosario de términos ISO 27001 (2013), "Cualquier sistema de procesamiento de información, servicio o infraestructura, o la ubicación física que lo alberga".

Integridad de la información: Según Glosario de términos ISO 27001 (2013), "Es la exactitud y consistencia generales de los datos o expresado de

otra forma, la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios".

Mejora continua: Según Glosario de términos ISO 27001 (2013), "Es simplemente identificar y realizar cambios enfocados a conseguir la mejora del rendimiento y resultados de una organización. Es un concepto fundamental para las teorías y programas de gestión de la calidad y de la seguridad de la información".

Nivel de Riesgo: Según Glosario de términos ISO 27001 (2013), "Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad".

Órgano Rector: Según Glosario de términos ISO 27001 (2013), "Persona o grupo de personas que son responsables del desempeño de la organización. El órgano rector puede ser una junta directiva o consejo de administración".

Parte Interesada: Según Glosario de términos ISO 27001 (2013), "Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad".

Riesgo: Según Glosario de términos ISO 27001 (2013), "Efecto de la incertidumbre sobre los objetivos. Una desviación de lo esperado - positivo o negativo. La incertidumbre es el estado de la deficiencia de la información, la comprensión o el conocimiento de un evento, su consecuencia o probabilidad".

Seguridad de Información: Según Glosario de términos ISO 27001 (2013), "Preservación de la confidencialidad, integridad y disponibilidad de la información".

Sistema de Gestión: Según Glosario de términos ISO 27001 (2013), "Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos".

Sistema de Gestión de Seguridad de la Información (SGSI): Según Glosario de términos ISO 27001 (2013), "Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de administración de seguridad de la información. En sistemas más grandes, es aconsejable asignar este cometido a un grupo de personas".

Sistema de Información: Según Glosario de términos ISO 27001 (2013), "Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información".

Vulnerabilidad: Según Glosario de términos ISO 27001 (2013), "Debilidad de un activo o control que puede ser explotado por una o más amenazas. Puede ser un fallo en un sistema que puede dejarlo accesible a los atacantes".

2.4 FORMULACIÓN DE HIPÓTESIS

2.4.1 Hipótesis General

El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023.

2.4.2 Hipótesis Específica

- El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023.
- El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023.
- El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023.

2.5 OPERACIONALIZACIÓN DE VARIABLES E INDICADORES

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES
1. DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001.	"La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI)".	"La norma ISO 27001 permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización".	Confidencialidad	• Activos • Valores • Mejoras
			Disponibilidad	• Procesamiento de datos • Almacenamiento de datos • Partes interesadas
			Integridad	• Legal • Reglamentos • Contractuales
2: SEGURIDAD DE LA INFORMACIÓN	"La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización".	"Los sistemas de seguridad de la información deben ser capaces de gestionar el riesgo existente y superarlo con el menor impacto para la organización, es decir, tienen que ser capaces de garantizar la resiliencia de la organización y sus sistemas de seguridad con lo que prevenir, evitar y solucionar cualquier riesgo o ataque que se derive del tratamiento de la información y los datos".	De la red	• Controles • Acceso • Tratamientos
			Del software	• Adquisición • Diseño • Mantenimiento
			Del hardware	• Fabricación • Protección • Auditoría

CAPÍTULO III

METODOLOGÍA

3.1 DISEÑO METODOLÓGICO

3.1.1 Tipo de Investigación

La presente investigación es de tipo aplicada, puesto que se dedica a contrastar la teoría con lo real, Por otro lado, se considera una investigación descriptiva porque enfoca elementos de estudio de un fenómeno en este caso el diseño e implementación de la ISO 27001.

3.1.2 Diseño de la Investigación

Nuestra investigación es de diseño no experimental y transversal, debido a que está basado elementalmente en observar los hechos sin intervenir en un solo momento las variables en estudio, para luego analizarlo con los instrumentos que medirán nuestras hipótesis.

3.1.3 Nivel

El enfoque de la investigación es de naturaleza correlacional, ya que se centra en evaluar cómo la implementación de la norma ISO 27001 contribuye a mejorar la seguridad de la información en la empresa minera Colibrí S.A.C. en Lima durante el año 2023.

3.1.4 Enfoque

Un enfoque mixto en la investigación implica la combinación de metodologías cualitativas y cuantitativas para obtener una comprensión más completa del tema en estudio. Esta aproximación busca aprovechar tanto la recolección de datos cualitativos, que se enfoca en comprender contextos, percepciones y experiencias, como la recopilación de datos cuantitativos, que se centra en mediciones numéricas y estadísticas.

3.2 POBLACIÓN Y MUESTRA

3.2.1 Población

Tomando en cuenta a la población como el universo de la investigación, la población de la presente investigación son los 70 participantes o trabajadores administrativos que de la oficina central de Lima de la empresa minera Colibrí SAC.

3.2.2 Muestra

Es la parte de la totalidad del fenómeno o actividad que se considera representativa. Siendo el tamaño de la muestra que representa, en esta investigación es igual al tamaño de la población (70 participantes) que pertenecen a los administrativos de la central Lima de la empresa minera Colibrí SAC.

3.2.3 Técnicas

Criterios de técnicas de muestreo no probabilístico, especialmente se analiza a las poblaciones que existen en la actividad tales como los trabajadores administrativos o intervinientes de la empresa Colibrí SAC – Lima 2023.

3.3 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.3.1 Técnicas a Emplear

"Las técnicas para la obtención de la información que se necesitó para el desarrollo de esta investigación fueron":

- ✓ Observación.
- ✓ Análisis documental
- ✓ Entrevista

- ✓ Encuestas

3.3.2 Descripción de los Instrumentos

Observación: Se aplicó para observar todo lo relacionado con el diseño e implementación de la ISO 27001 para mejorar la seguridad de información en la empresa minera Colibrí SAC - Lima.

Análisis Documental: Con la finalidad de obtener un fundamento del problema de investigación para el presente trabajo de estudio, se revisó las fuentes escritas (textos, tesis, etc.) vinculadas al tema de estudio.

Entrevista: Se entrevistó a los participantes en general a los trabajadores administrativos de la investigación; diseño e implementación de la ISO 27001 para mejorar la seguridad de información en la empresa minera Colibrí SAC - Lima.

Encuesta: Se elaboró un cuestionario de preguntas tipo Likert que fueron respondidas por participantes sobre el diseño e implementación de la ISO 27001 para mejorar la seguridad de información en la empresa minera Colibrí SAC - Lima.

3.3.3 Validez de los Instrumentos

En el instrumento se usó la escala tipo Likert (también llamada método de evaluaciones sumatorias) que es una escala psicotécnica que después se pudo validar y poder medir su confiabilidad del cuestionario. Ver Anexo (Cuestionario N° 1 - Encuesta).

El criterio de validez tiene que ver con la validez del contenido y la validez del conocimiento. La validez establece la relación del instrumento con la variable que se pretende medir y la validez de construcción de relacionar los ítems del cuestionario aplicado.

La confiabilidad se refiere al grado en que su aplicación repetida al mismo sujeto, produce iguales resultados.

3.4 TÉCNICAS PARA EL PROCESAMIENTO DE LA INFORMACIÓN

Después de la recolección de datos por medio de las técnicas de recolección se realizó el procesamiento de la información por medio del instrumento cuestionario.

La información se procesó por medio de las siguientes herramientas:

- **MS WORD 2019**, con este procesador de textos se procedió a realizar los distintos informes, cuadros y el cuestionario.
- **SPSS VERSIÓN 23,** sirvió pues ver los resultados del instrumento de una manera cuantitativa y cualitativa de los datos para luego interpretar a través de este programa.

Se utilizó una prueba estadística para examinar y establecer la conexión entre las variables. Los datos recolectados se sometieron a análisis estadístico descriptivo, lo que posibilitó la verificación de la hipótesis pertinente.

3.5 MATRIZ DE CONSISTENCIA

DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA MINERA COLIBRÍ SAC. – LIMA 2023

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES - DIMENSIONES	INDICADORES	METODOLOGÍA
PROBLEMA GENERAL: ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023?	**OBJETIVO GENERAL:** "Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023".	**HIPÓTESIS GENERAL:** El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023.	**Variable: (1)** - DISEÑO E IMPLEMENTA-CIÓN DE LA ISO 27001 **Dimensiones:** - Confidencialidad - Disponibilidad - Integridad	Indicadores de Variable 1: Activos, valores y mejoras Procesamiento de datos, almacenamiento de datos y partes interesadas. Legal, reglamentos y contractuales.	**Tipo de Investigación** La investigación será de tipo no experimental, y transaccional o transversal ya que se tomará los datos a través del tiempo. **Nivel** La investigación será relacional. **Enfoque** Para desarrollar la investigación se sigue el modelo cualitativo y cuantitativo. **Población y Muestra** **Población:** La población está constituida por 70 trabajadores administrativos de la oficina central de la empresa minera Colibrí SAC – Lima.. **Muestra:** La muestra será la totalidad de los trabajadores (70 personas). **Técnicas:** Criterios de técnicas de muestreo no probabilístico.
PROBLEMAS ESPECÍFICOS: • ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023? • ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023? • ¿De qué manera el Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023?	OBJETIVOS ESPECÍFICOS: • "Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023". • "Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023". • "Identificar la influencia del Diseño e Implementación de la ISO 27001 en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023".	HIPÓTESIS ESPECÍFICAS: • El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023. • El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023. • El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023.	**Variable: (2)** - SEGURIDAD DE INFORMACIÓN **Dimensiones:** - De la red - Del software - Del hardware	Indicadores de Variable 2: Controles, acceso y tratamientos. Adquisición, diseño y mantenimiento. Fabricación, protección y auditoría.	

CAPÍTULO IV

RESULTADOS

4.1 RESULTADOS TEÓRICOS:

"¿Cómo influye la aplicación del ISO 27001 en la confidencialidad de la seguridad de la información de una empresa?" Según www.scielo.org.pe la Biblioteca Científica Electrónica en Línea (2020):

> Las empresas necesitan salvaguardar su información de posibles competidores. Mantener la confidencialidad de estos datos es fundamental para el progreso y la estabilidad empresarial, por lo que se debe evitar la divulgación no autorizada de información corporativa. Resulta pertinente que empresas de distintos tamaños implementen normativas como la ISO 27001 o la 27002, adaptándolas a sus respectivos ámbitos, ya que estas directrices orientan la gestión de la seguridad de la información y permiten evaluar la situación actual, así como planificar su progreso a lo largo del tiempo. Todo tipo de empresa maneja información confidencial, por lo que es crucial protegerla incluso de sus propios empleados, quienes deben ser conscientes de la relevancia de gestionar adecuadamente la información generada en su trabajo diario. Numerosas empresas, independientemente de su tamaño, aplican estándares internacionales para analizar su estado actual en relación con un ideal, teniendo como base los principios fundamentales de la seguridad informática, entre los que se destaca la confidencialidad.

"¿Cómo influye la aplicación del ISO 27001 en la integridad de la seguridad de la información?" Según www.scielo.org.pe la Biblioteca Científica Electrónica en Línea (2020):

> Al implementar la norma ISO 27001 en una empresa y considerando sus diferentes dominios, se examina la integridad de la seguridad de la información. Esto conlleva la necesidad de establecer mecanismos,

políticas y directrices comunicadas a todos los empleados de distintos departamentos, con el objetivo de evitar alteraciones no autorizadas en los datos manejados.

La ISO 27001 permite evaluar que estrategias, políticas, directivas se aplican. Según www.scielo.org.pe la Biblioteca Científica Electrónica en Línea (2020):

> Evidentemente, "los resultados obtenidos en relación a la integridad de la seguridad de la información, validan lo expuesto anteriormente; ya que, si una organización no implementa políticas o normas para el desarrollo de sus procesos, éstos marcharán a la deriva y expuestos a altos riesgos. Asimismo, que la aplicación de ISO 27001 si influye en la integridad de la información porque permite evaluar que estrategias, políticas, directivas se están aplicando para evitar que la información sea alterada sin autorización".

"¿Cómo influye la aplicación del ISO 27001 en la disponibilidad de la seguridad de la información?" Según www.scielo.org.pe la Biblioteca Científica Electrónica en Línea (2020):

> El aplicar el ISO 27001 en una organización impacta en la disponibilidad de la seguridad de la información, ya que "es uno de los pilares de la seguridad de la información y sostiene que es necesario que la información debe ser accedida por usuarios autorizados. Se comenta también que la información de la organización se encuentra vulnerable a ataques, modificaciones y otros tipos de daños. La disponibilidad hace referencia a que los datos, información debe estar a disposición de los usuarios de forma oportuna y según los privilegios o accesos que se les haya asignado".

La ISO 27001 permite evaluar que estrategias, políticas, directivas se aplican. Según www.scielo.org.pe la Biblioteca Científica Electrónica en Línea (2020):

> En relación a los resultados obtenidos, se encontró la influencia de la aplicación del ISO 27001 en la seguridad de la información; que la aplicación de planes de mejora garantiza la integridad, disponibilidad y accesibilidad de la información haciendo referencia al ISO 27001. En tal sentido, se demuestra que el estudio realizado posee una valía teórica y metodológica ya que se conoció la eficiencia del modelo ISO en la solución y mejora continua de la seguridad de la información. Los sistemas de seguridad han ido progresando a través del tiempo. En ese contexto los sistemas ISO han ido aportando elementos importantes a la seguridad desde la planificación de la misma hasta el monitoreo permanente. La influencia existente permite establecer un horizonte seguro y confiable para los usuarios.

También en relación a los resultados específicos obtenidos, se encontró "la influencia de la aplicación del ISO 27001 en la confidencialidad, integridad y la disponibilidad de la seguridad de la información de la empresa colibrí SAC, se encontró la existencia de esa influencia. La aplicación la norma ISO reduce el costo de tiempo. En tal sentido, la seguridad de manera íntegra puede verse reflejada en la confidencialidad de la información; la reserva de los activos de la empresa se convierte en un componente esencial para el logro de los objetivos estratégicos ya que mucha de esa información será útil para la toma de decisiones. Con respecto a la integridad y la disponibilidad, el fácil acceso y la credibilidad de los recursos se convierte en una creciente demanda de usuarios y gestores". A partir de estos elementos, se garantiza la fluidez de la seguridad de la información.

La importancia de la Informática y las TICs. Según peritoinformatico.es (2023):

> La informática y las tecnologías de la información (TI) se han convertido en herramientas fundamentales para que personas, empresas y administraciones puedan realizar sus tareas y procesos habituales. En este entorno, los fallos de seguridad en informática son

> uno de los mayores riesgos a los que se enfrenta un negocio, teniendo un gran impacto en su actividad e imagen cuando se producen.

Según peritoinformatico.es (2023), “Una brecha de seguridad en una empresa puede implicar, desde interrupciones en su actividad diaria, pasando por pérdida de clientes y ventas, hasta sanciones económicas por exponer información sensible”.

Principales fallos de seguridad informática

Los fallos se dan habitualmente en las empresas. Según peritoinformatico.es (2023):

> Sufrir un fallo de seguridad es una situación que sufren habitualmente las empresas, por lo que es importante contar con medidas de protección, prevención y actuación para poder estar preparados. Veamos cuáles son las principales amenazas de seguridad informática que existen.

Contraseñas débiles

Según peritoinformatico.es (2023), “Uno de los mayores fallos en ciberseguridad está relacionado con el uso de contraseñas poco seguras o débiles”.

Usar las contraseñas seguras. Según peritoinformatico.es (2023), “Las empresas deben obligar al uso de contraseñas seguras por parte de sus trabajadores y clientes. Es decir, forzar la creación de contraseñas largas, que intercalen mayúsculas y minúsculas, que contengan números y que incluyan algún símbolo”.

Según peritoinformatico.es (2023), “Con una contraseña sólida, los ciberdelincuentes tendrán muchas más dificultades para poder descifrarlas”.

Actualización de sistemas y software

Actualizar siempre los sistemas operativos y software. Según peritoinformatico.es (2023):

> Otra de las principales amenazas de seguridad en una empresa está relacionada con la no actualización de sus sistemas operativos y software. Las últimas versiones siempre incluyen parches y actualizaciones que corrigen vulnerabilidades conocidas e implementan nuevas medidas de protección y seguridad.

No utilizar herramientas de protección

Según peritoinformatico.es (2023), "Existen muchas herramientas especialmente diseñadas para la protección de la infraestructura TI de una empresa, tanto a nivel de *hardware* (*firewalls*, por ejemplo), como de *software* (antivirus, *antimalware*…)".

Según peritoinformatico.es (2023), "No implementar este tipo de sistemas de protección hace que la empresa sufra mayores fallos de seguridad informática, recibiendo ciberataques contra sus servidores y sistemas (*ransomware*, denegación de servicio, inyección SQL y similares)".

No disponer de un sistema de copias de seguridad

Una gran falla de las empresas es no contar con un buen sistema de copias de seguridad. Según peritoinformatico.es (2023):

> Un fallo en seguridad informática que cometen muchas empresas es no contar con un buen sistema de copias de seguridad. Con una copia de seguridad automatizada y periódico, la empresa puede recuperar sus sistemas e información de forma rápida y eficiente cuando sea necesario.

Mala formación en seguridad de los trabajadores

Los culpables de los fallos en su mayoría son los usuarios. Según peritoinformatico.es (2023):

> Los usuarios "son los culpables de la mayoría de los fallos informáticos relacionados con la seguridad de una empresa. Por este motivo, es muy importante implementar en la empresa una cultura de ciberseguridad**.** Esta debe ir acompañada con un buen plan de formación de los trabajadores en materia de seguridad informática".

Según peritoinformatico.es (2023), "Si los empleados de un negocio son conscientes de los riesgos informáticos existentes y cuentan con los conocimientos y habilidades en seguridad necesarios, las amenazas de seguridad para el negocio serán mucho menores".

Política de seguridad poco eficiente

Con una mala política de seguridad se presentan los fallos informáticos. Según peritoinformatico.es (2023):

> Los fallos informáticos de seguridad vienen muchas veces relacionados con una mala política de ciberseguridad. Desarrollar una política moderna y eficiente de seguridad debe ser una de las prioridades de cualquier negocio, pues ayuda a minimizar los riesgos y actúa como una guía a seguir en caso de ser víctimas de un ataque.

Asignación de permisos de usuarios

En cuanto a la asignación de permisos de usuario. Según peritoinformatico.es (2023):

> Otro punto clave para la seguridad informática es la asignación de permisos de usuario. Si la empresa no da los permisos de acceso a datos y sistemas teniendo en cuenta el rol de cada empleado o usuario, los riesgos de que se vean expuestos son mucho mayores**.**

Según peritoinformatico.es (2023), "Una correcta asignación de permisos permitirá que los trabajadores y usuarios solo accedan a aquellas herramientas e información necesaria para realizar sus actividades o tareas, minimizando los riesgos en seguridad (evitando robos internos, por ejemplo)".

Deficiente protección de las redes

Según peritoinformatico.es (2023), "Las redes empresariales son fundamentales para el funcionamiento del negocio (redes wifi, acceso a internet por cable, red interna…). Una mala protección de estas redes eleva el riesgo en ciberseguridad del negocio".

Según peritoinformatico.es (2023), "Por ejemplo, es importante implementar un sistema de acceso vía VPN para los teletrabajadores. Así podrán realizar su trabajo de forma remota sin poner en riesgo los datos y sistemas de la empresa".

Dispositivos ocultos

Según peritoinformatico.es (2023), "Muchos fallos de seguridad se producen por la presencia en las redes empresariales de equipos ocultos a los ojos de los administradores. Es decir, dispositivos que utilizan los usuarios sin permiso de los administradores (móviles, tabletas, portátiles, etc.)".

Según peritoinformatico.es (2023), "Gestionar de forma eficiente los accesos a red de todos los dispositivos y utilizar una consola de ciberseguridad son imprescindibles para evitar que existan equipos conectados a la red de la empresa que no estén supervisados por los administradores".

Según peritoinformatico.es (2023), "Los fallos de seguridad informática producen grandes pérdidas a las empresas y las sitúan en posiciones de debilidad ante sus principales competidores".

La informática forma parte de nuestro día a día. Según www.imagar.com (2020):

> La computación es una parte cotidiana de nuestras vidas. Realizamos actividades como abrir correos electrónicos, descargar archivos y acceder a diversas redes sin mayores inquietudes ni precauciones. Rara vez consideramos que estas acciones, tan habituales para nosotros, puedan representar un riesgo.

Según www.imagar.com (2020), "Es importante tenerlo en cuenta en tu vida personal, porque puedes estar poniendo en peligro tus datos íntimos. Pero aún más si cabe en tu empresa, porque ahí ya entran muchas más cosas en juego".

Exposición de las entrañas de la empresa

Los problemas de seguridad informática en la empresa. Según www.imagar.com (2020):

> Un problema de seguridad informática en la empresa puede hacer que se expongan datos de tus clientes, tu propia organización o del funcionamiento de sus sistemas. Sin contar que si alguien accede a ellos puede vulnerarlos y alterar o modificar el trabajo que se realiza.

Grietas por las que colarse

Según www.imagar.com (2020), "La facilidad que tenemos a la hora de manejar y conectar cualquier servicio de sistemas informáticos nos hace olvidarnos que también puede ser muy sencillo colarse en ellos y generar mucho daño".

Los principales problemas de seguridad informática, precisamente de los que menos consciente somos:

- Redes: Conjunto de dispositivos interconectados que se comunican entre sí, permitiendo compartir recursos y datos. Pueden ser redes locales (LAN), redes de área extensa (WAN) o redes inalámbricas (Wi-Fi), entre otros tipos.

- Antivirus y firewall: “El antivirus es un software diseñado para detectar, prevenir y eliminar software malicioso, como virus, gusanos, troyanos, etc”. Por otro lado, un firewall es una barrera de seguridad que controla el flujo de datos entre una red privada y otras redes, permitiendo o bloqueando el tráfico según reglas predefinidas para prevenir accesos no autorizados.
- Accesos: Hace referencia a la entrada o interacción autorizada a recursos, datos o áreas específicas. En el ámbito digital, se refiere a la capacidad de ingresar o utilizar información o servicios protegidos mediante credenciales o permisos otorgados.
- Confianza: En el contexto de la seguridad informática, se refiere al grado de certeza o fiabilidad que se tiene en un sistema, proceso o entidad para manejar datos o realizar operaciones de manera segura, confiable y conforme a ciertos estándares.
- Dispositivos: Elementos físicos o virtuales utilizados para procesar, almacenar o transmitir datos. Incluyen computadoras, teléfonos móviles, tablets, servidores, enrutadores, entre otros equipos tecnológicos.

Según www.imagar.com (2020), “Para mejorar la seguridad informática tener en cuenta que no solo se ha de prestar atención a los equipos y sistemas informáticos. Es importante concienciar a los propios trabajadores de los peligros que existen. Así, se minimizarán al máximo”.

LA EMPRESA

La “Empresa Minera de Capitales Sudafricanos” comenzó su trayectoria en el país con una Planta de Tratamiento de Minerales Auríferos de pequeña escala, con una capacidad inicial de 40 toneladas por día. A día de hoy, ha experimentado un crecimiento considerable en sus instalaciones, alcanzando una capacidad actual de 200 toneladas por día. Su producción mensual supera los 90 kilogramos de oro. La labor de MINERA COLIBRI SAC ha generado progreso en los pueblos cercanos, beneficiando a numerosas familias gracias a las actividades desarrolladas en su Planta de Beneficio, localizada en los

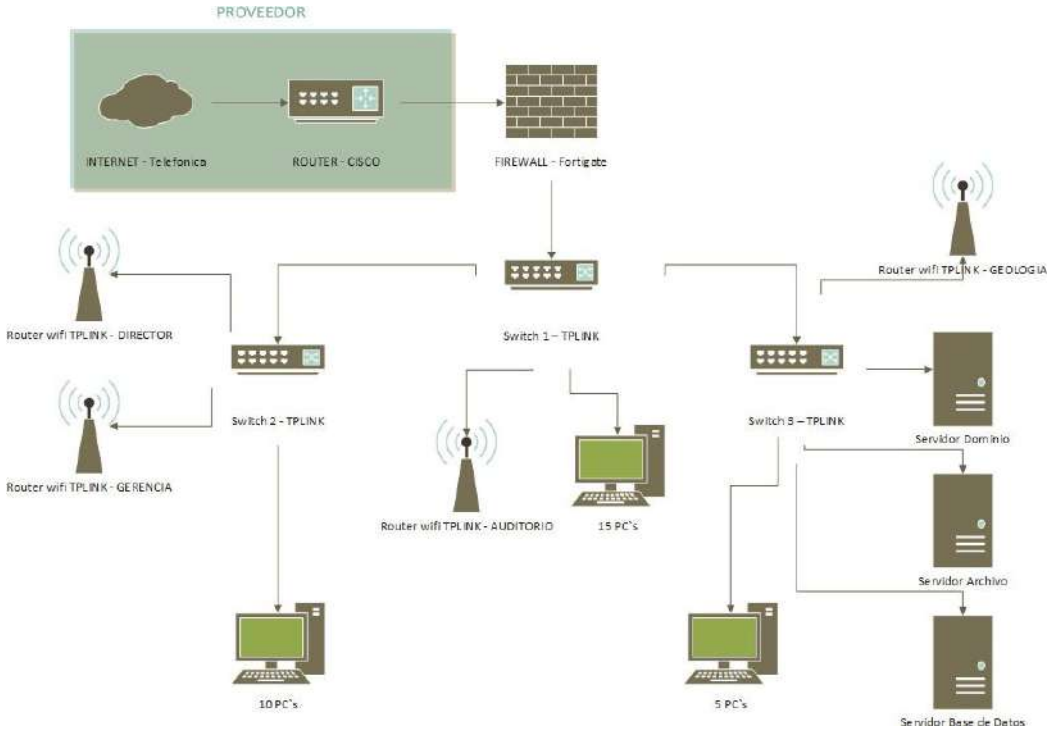
Distritos de Cháparra – Achanizo, Provincia de Caravelí, Departamento de Arequipa.

ESTADO ACTUAL NIVEL SEGURIDAD

La empresa cuenta con 30 equipos de cómputo, 3 switch, 3 servidores, 4 router wifi, 1 firewall.

Figura 09:

Equipos de cómputo de la Empresa Colibrí SAC



Fuente: Oficina Central – Lima Colibrí SAC

Como se puede observar en la realidad de la empresa le falta equipos certificados (router y switch) que puedan brindar la seguridad que necesita, ese es a nivel red, en nivel usuario también faltan licencias originales donde

es un riesgo alto (virus informáticos y malware) donde se está vulnerando la información confidencial que maneja dicha empresa y expuestos a multas; si bien es cierto todas las empresas deben estar licenciados en todos los software que puedan utilizar.

4.2 RESULTADOS METODOLÓGICOS:

4.2.1 Validez del Instrumento

La validación de un instrumento en investigación se refiere al proceso de evaluar la calidad, precisión y eficacia del instrumento utilizado para recopilar datos.

NÚMERO ÓPTIMO DE EXPERTOS:

La validación de un cuestionario mediante la revisión de tres expertos es una etapa crucial en la investigación. Este proceso implica presentar el cuestionario a estos especialistas para obtener su evaluación detallada sobre la coherencia, relevancia y claridad de cada ítem. Los expertos proporcionan retroalimentación, señalando posibles ambigüedades, preguntas poco claras o sugerencias para mejorar la validez del instrumento en relación con los objetivos de la investigación.

La participación de tres expertos ofrece una perspectiva más amplia y diversa, lo que contribuye a identificar posibles deficiencias o áreas de mejora en el cuestionario. A través de sus comentarios y sugerencias, se busca fortalecer la calidad y fiabilidad del instrumento, asegurando que las preguntas sean adecuadas y efectivas para medir con precisión los aspectos que se investigan.

CONFECCIÓN DEL LISTADO DE EXPERTOS:

Contactar a estos especialistas implica presentarles el propósito de la investigación, detallar la importancia de su participación en la validación del cuestionario y solicitar su colaboración para revisar y proporcionar retroalimentación sobre la efectividad y pertinencia de las preguntas planteadas en el instrumento. Su aporte resulta esencial para garantizar la validez y fiabilidad del cuestionario en la medición de los aspectos investigativos.

"En la presente investigación existe 01 experto de vasta experiencia y enseñan las áreas de METODOLOGÍA DE LA INVESTIGACIÓN, los dos siguientes expertos se eligió ingenieros de la FIISI y de la FIC. Los expertos que realizaron fueron los siguiente":

Experto 1: Ing. Químico	Robert Ocrospoma Dueñas
Experto 2: Ing. Civil	Manuel Alfredo Mora Morales
Experto 3: Ing. Industrial	Jorge Sánchez Guzman

Las calificaciones para los criterios de validación, que se mencionan en la hoja de juicio de experto (Juicio de Expertos) con respecto al contenido del instrumento, se muestra en la siguiente tabla:

Tabla 01
Calificación de los Expertos

N° "PREGUNTA Y ALTERNATIVAS"	**EXPERTOS**			**Punt.**
	E1	**E2**	**E3**	
"Pregunta N° 1 y su valoración"	4	5	5	**14**
"Pregunta N° 2 y su valoración"	5	4	5	**14**
"Pregunta N° 3 y su valoración"	4	4	5	**13**
"Pregunta N° 4 y su valoración"	5	5	5	**15**
"Pregunta N° 5 y su valoración"	5	5	4	**14**
"Pregunta N° 6 y su valoración"	5	4	5	**14**
"Pregunta N° 7 y su valoración"	4	5	5	**14**
"Pregunta N° 8 y su valoración"	5	5	5	**15**
"Pregunta N° 9 y su valoración"	5	4	5	**14**
"Pregunta N° 10 y su valoración"	4	5	5	**14**
"Pregunta N° 11 y su valoración"	5	5	4	**14**
"Pregunta N° 12 y su valoración"	4	4	5	**13**
"Pregunta N° 13 y su valoración"	5	5	4	**14**
"Pregunta N° 14 y su valoración"	5	4	5	**14**
"Pregunta N° 15 y su valoración"	5	5	5	**15**
"Pregunta N° 16 y su valoración"	4	5	4	**13**
"Pregunta N° 17 y su valoración"	5	5	4	**14**
"Pregunta N° 18 y su valoración"	5	5	5	**15**
Puntaje total	**84**	**84**	**85**	**253**

Donde: 1 = "Totalmente en Desacuerdo (TD)"
2 = "En Desacuerdo (ED)"

3 = “Ni de Acuerdo ni en Desacuerdo (NA-ND)”
4 = “De Acuerdo (DA)”
5 = “Totalmente de Acuerdo (TA)”

“CÁLCULO DEL COEFICIENTE DE VALIDEZ”:

$$Validez = \frac{Puntaje\ obtenido}{Máxima\ valoración}$$

$$Validez = \frac{253}{270} = 0{,}937 = 93{,}7\%$$

Con una validez general de 93,7% según la escala de validez el instrumento tiene muy alta validez; el “*DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA MINERA COLIBRÍ S.A.C. – LIMA 2023”* (Ver Tabla 2), de acuerdo al criterio de los expertos.

Tabla 02

Calificación de los Expertos

ESCALA	INDICADOR
0,01 – 0,20	“Muy baja validez”
0,21 – 0,40	“Validez baja”
0,41 – 0,60	“Moderada validez”
0,61 – 0,80	“Alta validez”
0,81 – 1,00	“Muy alta validez”

4.2.2 Confiabilidad del Instrumento

"Se realizó el análisis de fiabilidad en el programa estadístico SPSS Statistics 23.0 al instrumento aplicado a todos los participantes" (70 trabajadores de la empresa Colibrí S.A.C. Lima). "Se obtuvo una fiabilidad de 0,820 (ver Tabla 3), este instrumento estuvo conformado por 18 items, distribuidos para": la **variable 1:** DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001 en 3 dimensiones (Confidencialidad, Disponibilidad e Integridad) y para la **variable 2:** SEGURIDAD DE INFORMACIÓN, en 3 dimensiones (De la red, Del software y Del hardware).

Tabla 03

"Alpha de Cronbach aplicado al Instrumento"

Alpha de Cronbach	N° de elementos
0,820	18

Fuente: "Elaboración propia"

"Esto quiere decir que el instrumento tiene una valoración de muy alta validez según la escala de expertos, como se muestra a continuación en la tabla 4".

Tabla 04

"Escala de confiabilidad"

ESCALA	INDICADOR
0,01 – 0,20	"Muy baja validez"
0,21 – 0,40	"Validez baja"
0,41 – 0,60	"Moderada validez"
0,61 – 0,80	"Alta validez"
0,81 – 1,00	"Muy alta validez"

4.2.3 Tablas y Gráficos Estadísticos

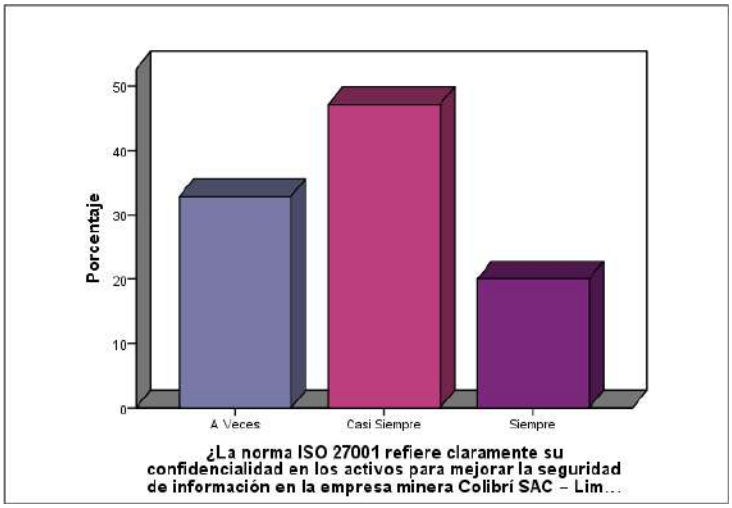
Tabla 05

¿La norma ISO 27001 refiere claramente su confidencialidad en los activos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	23	31,5	32,9	32,9
	Casi Siempre	33	45,2	47,1	80,0
	Siempre	14	19,2	20,0	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 10

Respuesta si la norma ISO 27001 refiere claramente su confidencialidad en los activos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 47,1% afirmó que Casi Siempre la norma ISO 27001 refiere claramente su confidencialidad en los activos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

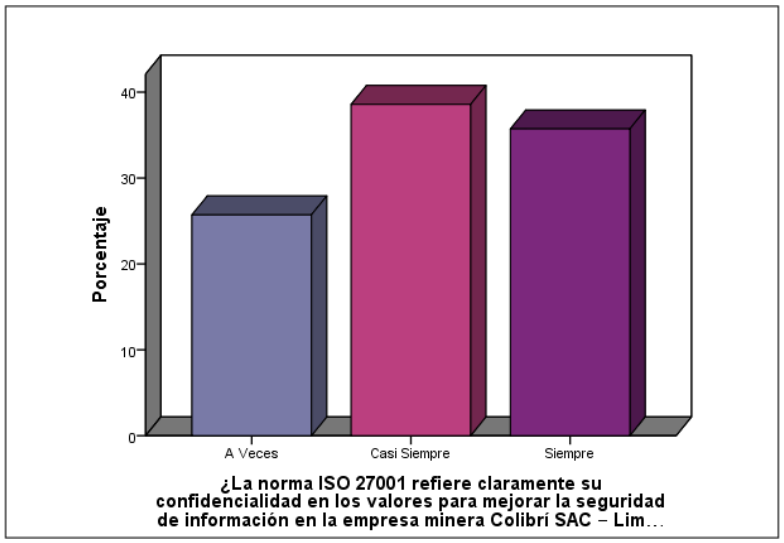
Tabla 06

¿La norma ISO 27001 refiere claramente su confidencialidad en los valores para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	18	24,7	25,7	25,7
	Casi Siempre	27	37,0	38,6	64,3
	Siempre	25	34,2	35,7	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 11

Respuesta si la norma ISO 27001 refiere claramente su confidencialidad en los valores para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 38,6% afirmó que Casi Siempre la norma ISO 27001 refiere claramente su confidencialidad en los valores para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

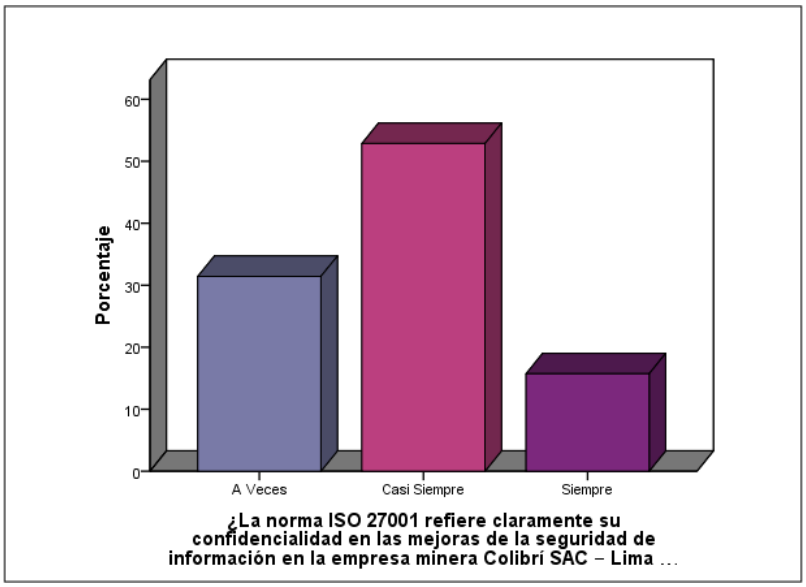
Tabla 07

¿La norma ISO 27001 refiere claramente su confidencialidad en las mejoras de la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	22	30,1	31,4	31,4
	Casi Siempre	37	50,7	52,9	84,3
	Siempre	11	15,1	15,7	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 12

Respuesta si la norma ISO 27001 refiere claramente su confidencialidad en las mejoras de la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 52,9% afirmó que Casi Siempre la norma ISO 27001 refiere claramente su confidencialidad en las mejoras de la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

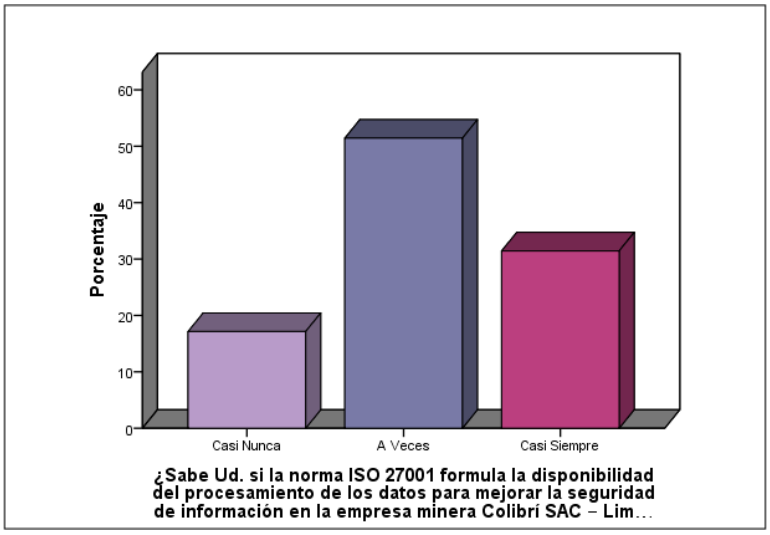
Tabla 08

¿Sabe Ud. si la norma ISO 27001 formula la disponibilidad del procesamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Nunca	12	16,4	17,1	17,1
	A Veces	36	49,3	51,4	68,6
	Casi Siempre	22	30,1	31,4	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 13

Respuesta si sabe que la norma ISO 27001 formula la disponibilidad del procesamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.



Nota: Un 51,4% afirmó que A Veces sabe que la norma ISO 27001 formula la disponibilidad del procesamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

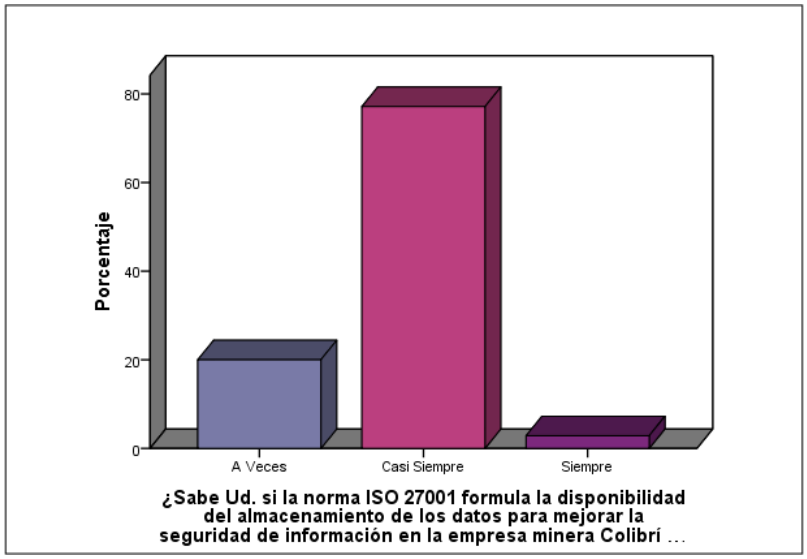
Tabla 09

¿Sabe Ud. si la norma ISO 27001 formula la disponibilidad del almacenamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	14	19,2	20,0	20,0
	Casi Siempre	54	74,0	77,1	97,1
	Siempre	2	2,7	2,9	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 14

Respuesta si sabe que la norma ISO 27001 formula la disponibilidad del almacenamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 77,1% afirmó que Casi Siempre sabe que la norma ISO 27001 formula la disponibilidad del almacenamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

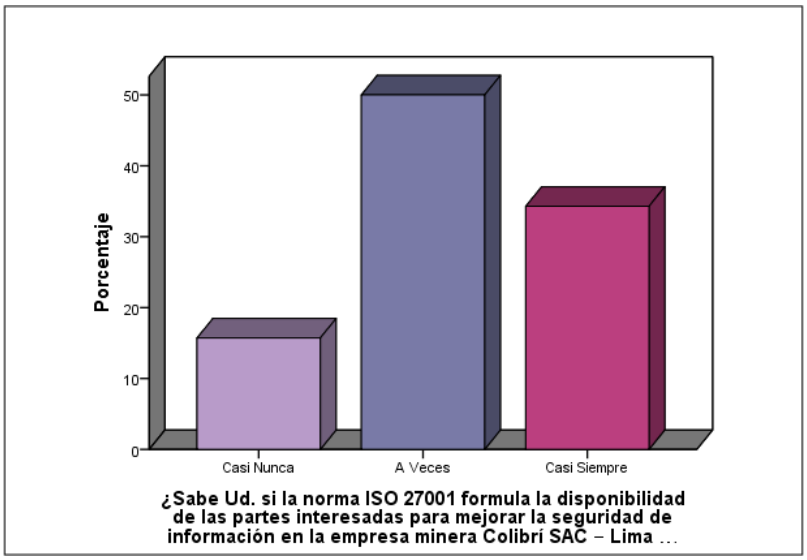
Tabla 10

¿Sabe Ud. si la norma ISO 27001 formula la disponibilidad de las partes interesadas para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Nunca	11	15,1	15,7	15,7
	A Veces	35	47,9	50,0	65,7
	Casi Siempre	24	32,9	34,3	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 15

Respuesta si sabe que la norma ISO 27001 formula la disponibilidad de las partes interesadas para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 50% afirmó que A Veces sabe que la norma ISO 27001 formula la disponibilidad de las partes interesadas para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

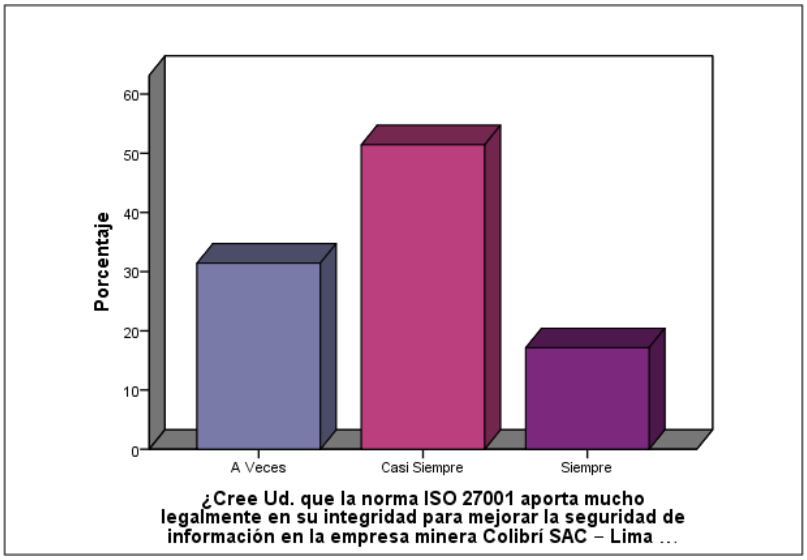
Tabla 11

¿Cree Ud. que la norma ISO 27001 aporta mucho legalmente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	22	30,1	31,4	31,4
	Casi Siempre	36	49,3	51,4	82,9
	Siempre	12	16,4	17,1	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 16

Respuesta si cree que la norma ISO 27001 aporta mucho legalmente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 51,4% afirmó que Casi Siempre cree que la norma ISO 27001 aporta mucho legalmente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

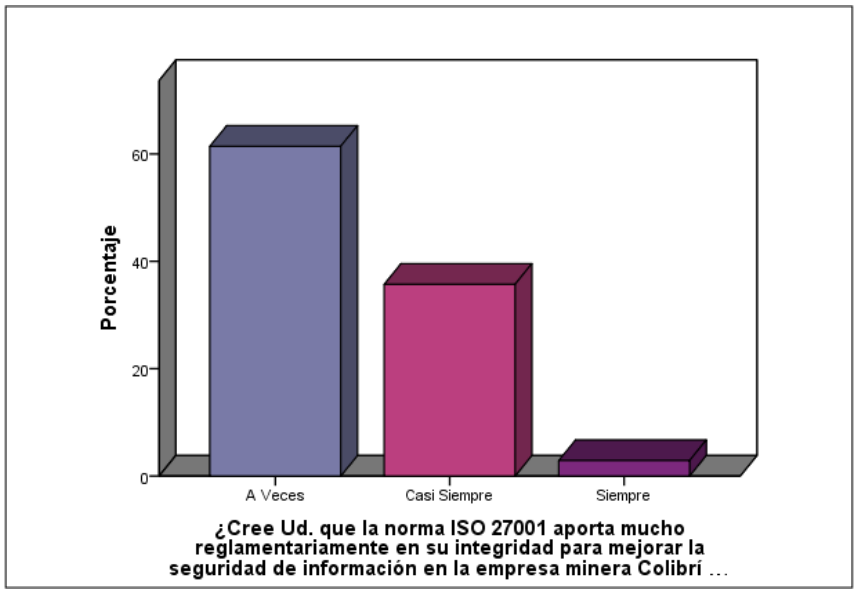
Tabla 12

¿Cree Ud. que la norma ISO 27001 aporta mucho reglamentariamente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	43	58,9	61,4	61,4
	Casi Siempre	25	34,2	35,7	97,1
	Siempre	2	2,7	2,9	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 17

Respuesta si cree que la norma ISO 27001 aporta mucho reglamentariamente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 61,4% afirmó que A Veces cree que la norma ISO 27001 aporta mucho reglamentariamente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

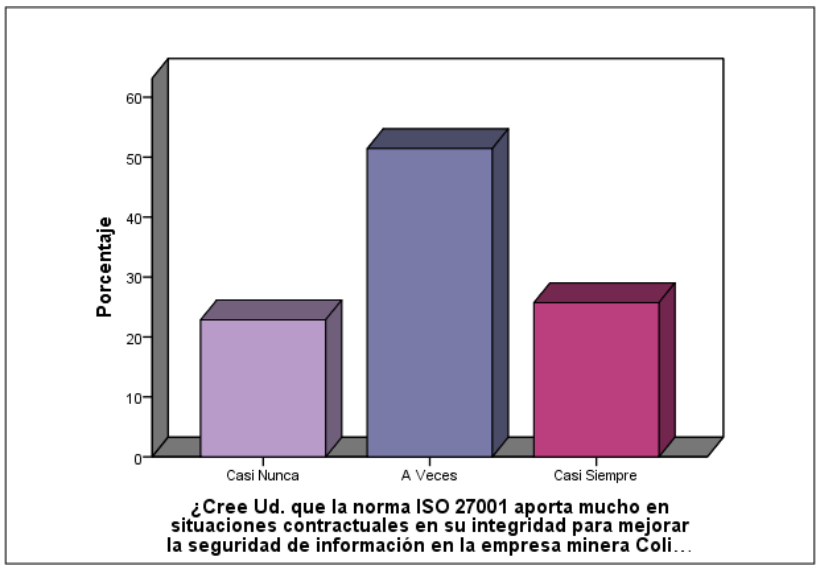
Tabla 13

¿Cree Ud. que la norma ISO 27001 aporta mucho en situaciones contractuales en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Nunca	16	21,9	22,9	22,9
	A Veces	36	49,3	51,4	74,3
	Casi Siempre	18	24,7	25,7	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 18

Respuesta si cree que la norma ISO 27001 aporta mucho en situaciones contractuales en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 51,4% afirmó que A Veces cree que la norma ISO 27001 aporta mucho en situaciones contractuales en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023.

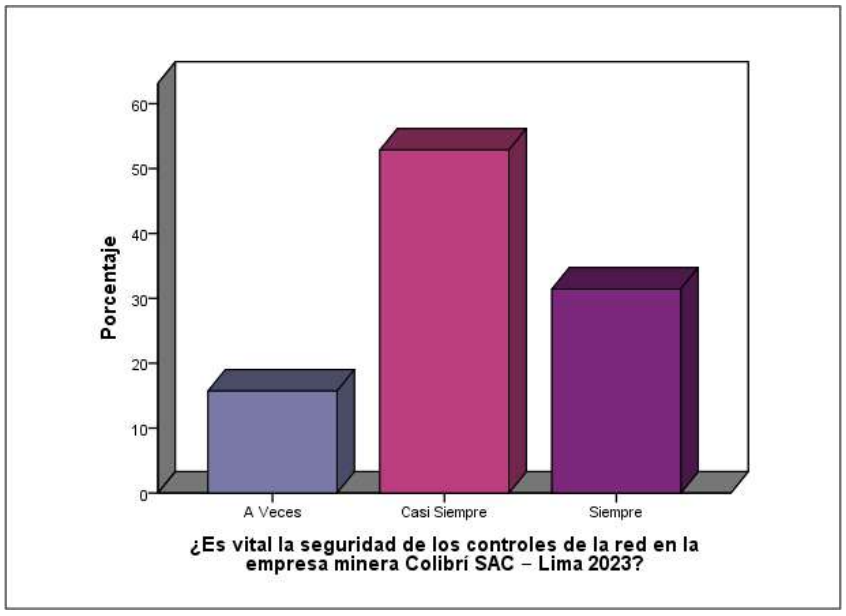
Tabla 14

¿Es vital la seguridad de los controles de la red en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	11	15,1	15,7	15,7
	Casi Siempre	37	50,7	52,9	68,6
	Siempre	22	30,1	31,4	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 19

Respuesta si es vital la seguridad de los controles de la red en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 52,9% afirmó que Casi Siempre es vital la seguridad de los controles de la red en la empresa minera Colibrí SAC – Lima 2023.

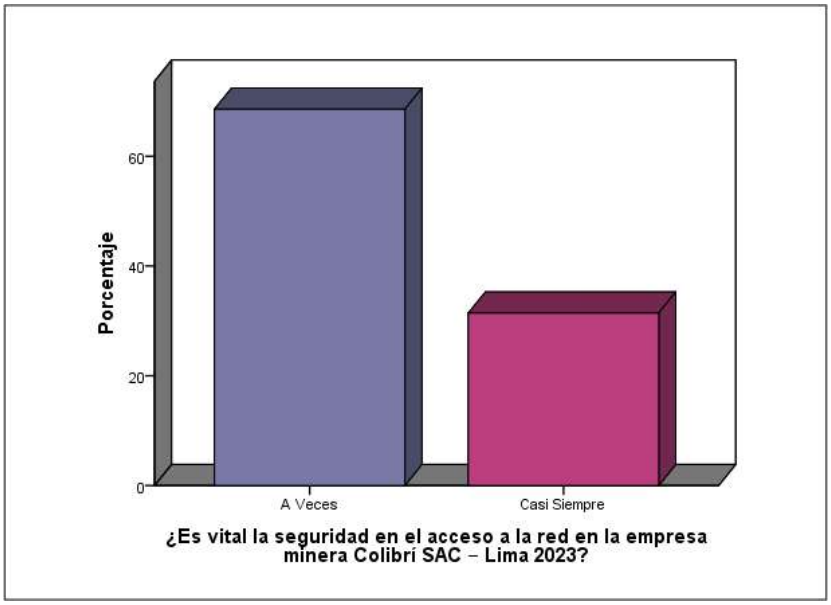
Tabla 15

¿Es vital la seguridad en el acceso a la red en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	48	65,8	68,6	68,6
	Casi Siempre	22	30,1	31,4	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 20

Respuesta si es vital la seguridad en el acceso a la red en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 68,6% afirmó que A Veces es vital la seguridad en el acceso a la red en la empresa minera Colibrí SAC – Lima 2023.

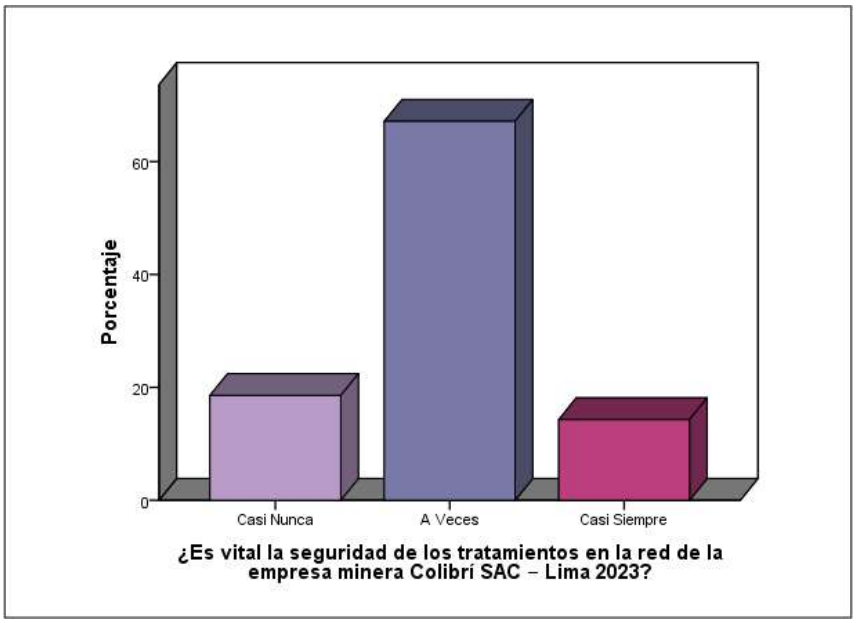
Tabla 16

¿Es vital la seguridad de los tratamientos en la red de la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Nunca	13	17,8	18,6	18,6
	A Veces	47	64,4	67,1	85,7
	Casi Siempre	10	13,7	14,3	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 21

Respuesta si es vital la seguridad de los tratamientos en la red de la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 67,1% afirmó que A Veces es vital la seguridad de los tratamientos en la red de la empresa minera Colibrí SAC – Lima 2023.

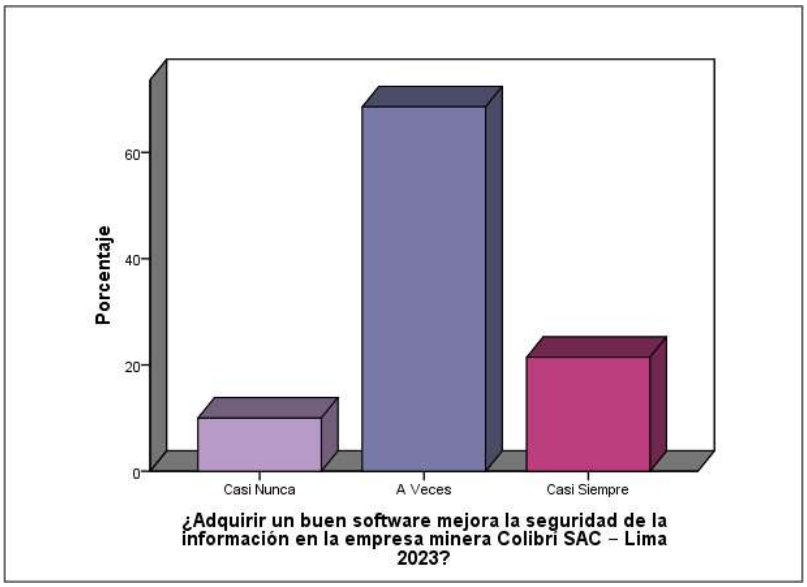
Tabla 17

¿Adquirir un buen software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Nunca	7	9,6	10,0	10,0
	A Veces	48	65,8	68,6	78,6
	Casi Siempre	15	20,5	21,4	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 22

Respuesta si adquirir un buen software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 68,6% afirmó que A Veces adquirir un buen software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.

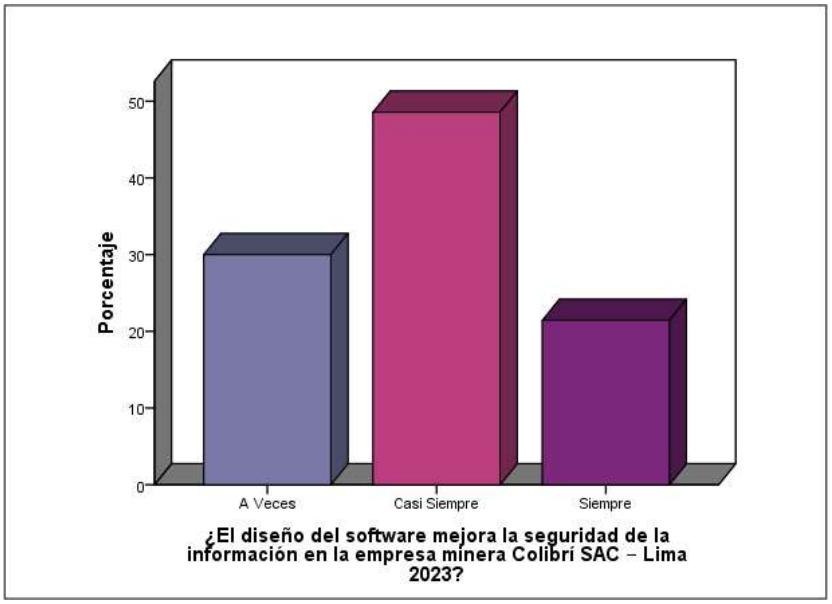
Tabla 18

¿El diseño del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	21	28,8	30,0	30,0
	Casi Siempre	34	46,6	48,6	78,6
	Siempre	15	20,5	21,4	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 23

Respuesta si el diseño del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 48,6% afirmó que Casi Siempre el diseño del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.

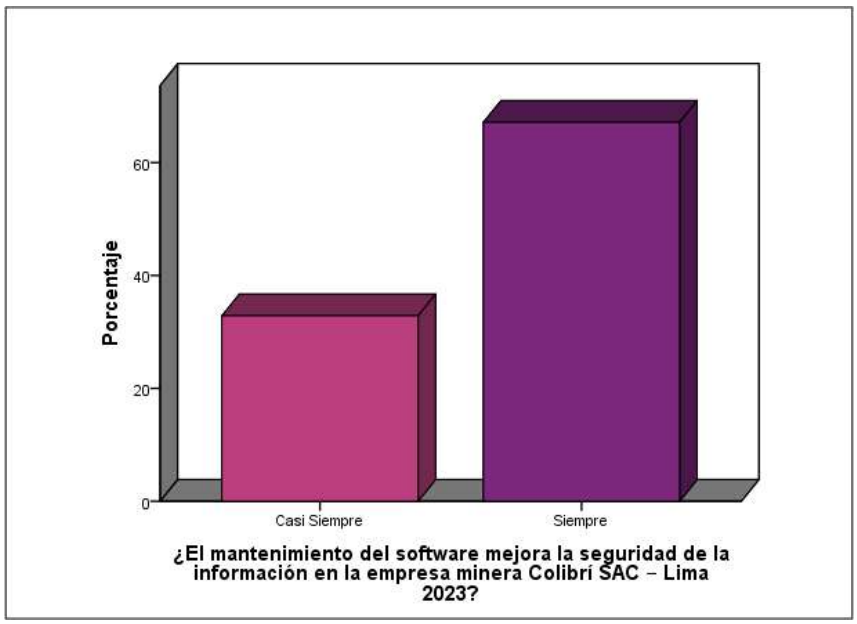
Tabla 19

¿El mantenimiento del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Siempre	23	31,5	32,9	32,9
	Siempre	47	64,4	67,1	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 24

Respuesta si el mantenimiento del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 67,1% afirmó que Siempre el mantenimiento del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.

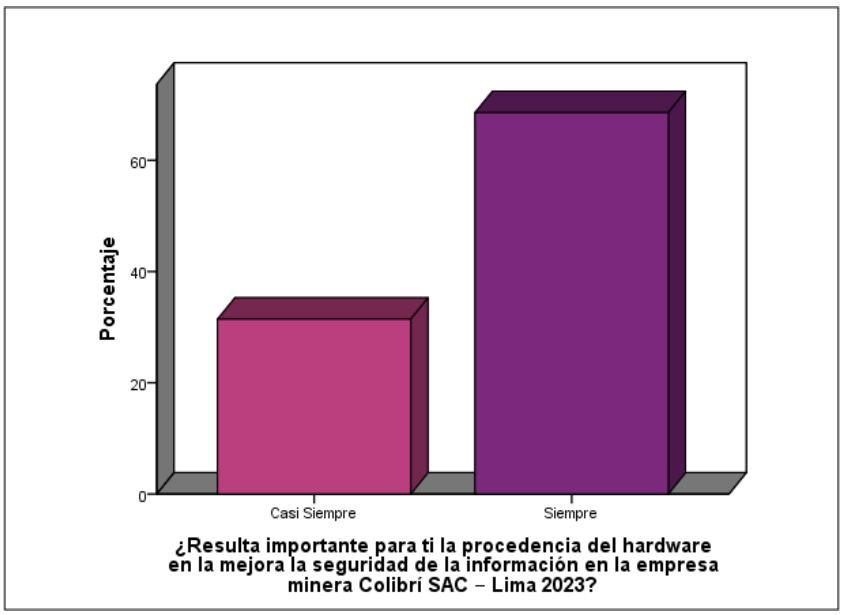
Tabla 20

¿Resulta importante para ti la procedencia del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Siempre	22	30,1	31,4	31,4
	Siempre	48	65,8	68,6	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 25

Respuesta si resulta importante para ti la procedencia del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 68,6% afirmó que Siempre resulta importante la procedencia del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.

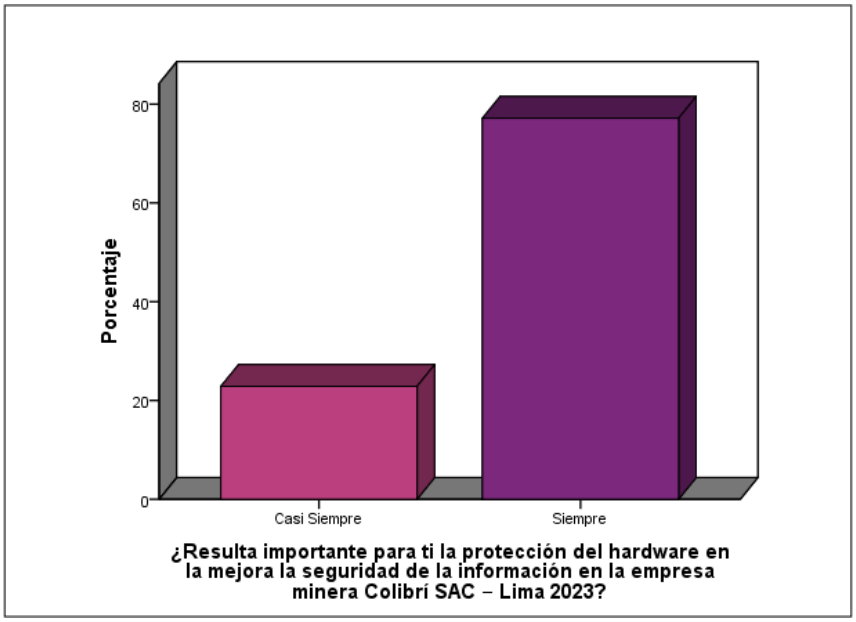
Tabla 21

¿Resulta importante para ti la protección del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Casi Siempre	16	21,9	22,9	22,9
	Siempre	54	74,0	77,1	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 26

Respuesta si resulta importante para ti la protección del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 77,1% afirmó que Siempre resulta importante para ti la protección del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.

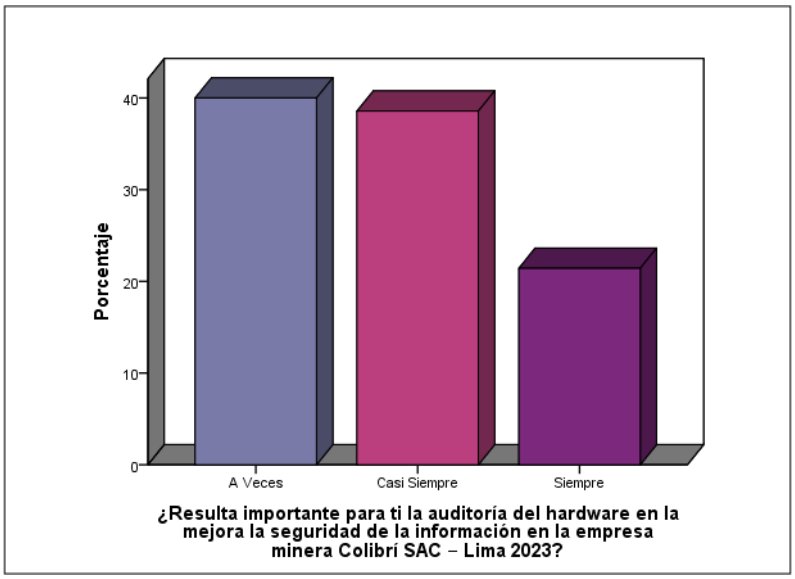
Tabla 22

¿Resulta importante para ti la auditoría del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	A Veces	28	38,4	40,0	40,0
	Casi Siempre	27	37,0	38,6	78,6
	Siempre	15	20,5	21,4	100,0
	Total	70	95,9	100,0	
Perdidos	Sistema	3	4,1		
Total		73	100,0		

Figura 27

Respuesta si resulta importante para ti la auditoría del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.



Nota: Un 40% afirmó que A Veces resulta importante para mi la auditoría del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023.

4.2.4 Contrastación de Hipótesis

"En la realización de la contrastación de hipótesis se empleó la información obtenida del cuestionario": DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA MINERA COLIBRÍ S.A.C. – LIMA 2023, "*donde se obtuvo las respuestas a las 18 preguntas planteadas, contestadas según escala de Likert, siendo (1) Nunca (2) Casi Nunca (3) A Veces (4) Casi Siempre y (5) Siempre".*

1. PRUEBA DE HIPÓTESIS DE INDICADORES X – Y1

Hn: El Diseño e Implementación de la ISO 27001, no influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Ha: El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Nivel de Significancia: a = 0,05

Tabla 23

*"De contingencia RESUMEN X (agrupado) * Y1 (agrupado)"*

		Y1 (agrupado)			Total
		A Veces	Casi Siempre	Siempre	
X (agrupado)	A Veces	2	3	0	5
	Casi Siempre	15	37	0	52
	Siempre	0	11	2	13
Total		17	51	2	70

Variable 1: X
Diseño e Implementación de la ISO 27001
X:
Valoración del promedio de las 3 dimensiones de la V1. (X1, X2, X3)

Variable 2: Y
Seguridad de la Información
Y1:
Valoración de la 1ra. dimensión de la V2 (Seguridad de la Red)

Tabla 24

Pruebas de chi-cuadrado

	Valor	Gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	13,261[a]	4	,010
Razón de verosimilitud	14,269	4	,006
Asociación lineal por lineal	8,354	1	,004
N de casos válidos	70		

a. "6 casillas (66.7%) han esperado un recuento menor que 5. El recuento mínimo esperado es .14".

Nota: Como el Nivel de Significación de muestra es **0,010**, menor al **0,05**, se Rechaza la Hipótesis Nula y en su lugar se Acepta la Hipótesis Alternativa, es decir: El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023.

2. PRUEBA DE HIPÓTESIS DE INDICADORES X – Y2

Hn: "El Diseño e Implementación de la ISO 27001, no influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023".

Ha: El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Nivel de Significancia: a = 0,05

Tabla 25

*"De contingencia RESUMEN X (agrupado) * Y2 (agrupado)"*

		Y2 (agrupado)			
		A Veces	Casi Siempre	Siempre	Total
X (agrupado)	A Veces	1	3	1	5
	Casi Siempre	2	39	11	52
	Siempre	0	6	7	13
Total		3	48	19	70

Variable 1: X
Diseño e Implementación de la ISO 27001
X:
Valoración del promedio de las 3 dimensiones de la V1. (X1, X2, X3)

Variable 2: Y
Seguridad de la Información

Y2:
Valoración de la 2da. dimensión de la V2 (Seguridad del Software)

Tabla 26

Pruebas de chi-cuadrado

	Valor	Gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	8,978[a]	4	,062
Razón de verosimilitud	7,581	4	,108
Asociación lineal por lineal	5,888	1	,015
N de casos válidos	70		

a. 6 casillas (66.7%) han esperado un recuento menor que 5. El recuento mínimo esperado es .21.

Nota: Como el Nivel de Significación de muestra es **0,062**, mayor al **0,05**, se Rechaza la Hipótesis Alternativa y en su lugar Acepta la Hipótesis Nula, es decir: El Diseño e Implementación de la ISO 27001, no influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023.

3. PRUEBA DE HIPÓTESIS DE INDICADORES X – Y3

Hn: El Diseño e Implementación de la ISO 27001, no influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Ha: El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Nivel de Significancia: a = 0,05

Tabla 27

*"De contingencia RESUMEN X (agrupado) * Y3 (agrupado)"*

		Y3 (agrupado)		
		Casi Siempre	Siempre	Total
X (agrupado)	A Veces	4	1	5
	Casi Siempre	17	35	52
	Siempre	0	13	13
Total		21	49	70

Variable 1: X
Diseño e Implementación de la ISO 27001
X:
Valoración del promedio de las 3 dimensiones de la V1. (X1, X2, X3)

Variable 2: Y
Seguridad de la Información
Y3:
Valoración de la 3ra. dimensión de la V2 (Seguridad del Hardware)

Tabla 28

Pruebas de chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	11,703[a]	2	,003
Razón de verosimilitud	14,791	2	,001
Asociación lineal por lineal	11,253	1	,001
N de casos válidos	70		

a. "3 casillas (50.0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 1.50".

Nota: Como el Nivel de Significación de muestra es **0,003**, menor al **0,05**, se Acepta la Hipótesis Alternativa y en su lugar se Rechaza la Hipótesis Nula, es decir: El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023.

4. PRUEBA DE HIPÓTESIS DE INDICADORES X – Y

Hn: El Diseño e Implementación de la ISO 27001, no influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Ha: El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023.

Nivel de Significancia: a = 0,05

Tabla 29

*De contingencia RESUMEN_X (agrupado) * RESUMEN_Y (agrupado)*

		Y (agrupado)		
		Casi Siempre	Siempre	Total
X (agrupado)	A Veces	5	0	5
	Casi Siempre	35	17	52
	Siempre	2	11	13
Total		42	28	70

Variable 1: X
Diseño e Implementación de la ISO 27001
X:
Valoración del promedio de las 3 dimensiones de la V1. (X1, X2, X3)

Variable 2: Y
Seguridad de la Información
Y:
Valoración del promedio de las 3 dimensiones de la V2. (Y1, Y2, Y3)

Tabla 30

Pruebas de chi-cuadrado

	Valor	gl	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	15,272[a]	2	,000
Razón de verosimilitud	17,334	2	,000
Asociación lineal por lineal	14,625	1	,000
N de casos válidos	70		

a. 2 casillas (33.3%) han esperado un recuento menor que 5. El recuento mínimo esperado es 2.00.

Nota: "Como el Nivel de Significación de muestra es **0,000**, menor al **0,05**, se Rechaza la Hipótesis Nula y en su lugar Acepta la Hipótesis Alternativa", es decir: "El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023".

Tabla 31

"RESUMEN, ANÁLISIS E INTERPRETACIÓN DE LA PRUEBA DE HIPÓTESIS ESTADÍSTICA"

CONTRASTACIONES	DECISIÓN	
	H. NULA	**H. ALTERNATIVA**
"El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de la Red en la Empresa Minera Colibrí S.A.C. – Lima 2023".	. . . . .	Se Acepta
"El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Software en la Empresa Minera Colibrí S.A.C. – Lima 2023".	Se Acepta	. . . . .
"El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad del Hardware en la Empresa Minera Colibrí S.A.C. – Lima 2023".	. . . . .	Se Acepta

Nota: "Sobre los Indicadores establecidos en nuestra Investigación, se encuentra que entre ellos si existe **Relación**, es decir con una Probabilidad del **95%,** de las tres pruebas de hipótesis, en dos se Acepta la hipótesis alternativa y en una se Rechaza la hipótesis alternativa, lo que nos conduce a una Aceptación por mayoría de relación entre variables".

POR LO TANTO:

"Dos de las Tres pruebas de hipótesis, se encuentra que se Acepta la Hipótesis Alternativa, dando paso al Rechazo de la Hipótesis Nula (Ver Tabla 31), con lo que se confirma la ACEPTACIÓN DE LA HIPÓTESIS PRINCIPAL", es decir que: "El Diseño e Implementación de la ISO 27001, influye en la mejora de la Seguridad de Información en la Empresa Minera Colibrí S.A.C. – Lima 2023". (ver Tabla 30).

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se evaluó que “la implementación de la ISO 27001 impacta la mejora de la seguridad de la red en la empresa minera Colibrí S.A.C. - Lima 2023”. Esto se evidencia en la tabla 24 de chi cuadrado, donde se halló un valor de significancia (p) de 0,010, inferior a 0,05, lo que llevó al rechazo de la hipótesis nula.

- Se examinó “el impacto del Diseño e Implementación de la ISO 27001 en la mejora de la seguridad del software en la empresa minera Colibrí S.A.C. - Lima 2023”. En la tabla 26 de chi cuadrado, se identificó un p valor de significancia de 0,062, superior a 0,05, lo que llevó al rechazo de la hipótesis alternativa.

- Se analizó “el impacto del Diseño e Implementación de la ISO 27001 en la mejora de la seguridad del hardware en la empresa minera Colibrí S.A.C. - Lima 2023”. En la tabla 28 de chi cuadrado, se obtuvo un p valor de significancia de 0,003, inferior a 0,05, conduciendo al rechazo de la hipótesis nula.

- Se investigó cómo “la implementación de la ISO 27001 influye en la mejora de la seguridad de la información en la empresa minera Colibrí S.A.C. - Lima 2023”. Esto se evidenció en la tabla 30 de chi cuadrado, donde se encontró un valor de significancia (p) de 0,000, menor a 0,05, lo que llevó al rechazo de la hipótesis nula.

5.2 RECOMENDACIONES

- La normativa está diseñada para instruirnos en la implementación de un Sistema de Gestión que incorpore los mecanismos necesarios para reducir los riesgos asociados con la confidencialidad, integridad y disponibilidad de la información en la organización. Esta información circula a través de los procesos internos de la empresa, incluyendo aquellos que agregan valor al interactuar con clientes y otras partes interesadas, así como los procesos de apoyo que, por su naturaleza, facilitan el funcionamiento de los procesos de valor en la empresa minera Colibrí S.A.C. A pesar de que podemos asegurar la seguridad del área de TI, a menudo descuidamos los procesos que tienen un contacto directo con el cliente, donde realmente se recopila la información. El área de Tecnologías de la Información en una empresa debe ser análoga al sistema nervioso del cuerpo humano; es crucial ya que por allí se canaliza una cantidad significativa de información vital.

- Las amenazas de la ciberseguridad son el gran problema de la empresa minera S.A.C. en manejar bien su información en la que recomendamos principalmente lo siguiente: Activa la protección de seguridad, practica la navegación segura, cuida lo que publicas en redes sociales, comprobar si tu conexión en red está protegida, ten cuidado con lo que descargas, crea contraseñas seguras y mantén actualizado el antivirus.

- Cuando se emplean accesos gratuitos en internet, la empresa que los ofrece suele obtener beneficios a través de publicidad, siendo esta una forma común de generar ingresos mientras se proporciona un servicio al usuario. Al conectar un dispositivo a una red de wi-fi abierta, en muchos casos, se pierde el control directo sobre la seguridad en la empresa minera Colibrí S.A.C. Cuando se utiliza una red wi-fi pública, es aconsejable evitar acceder a cuentas bancarias u otros servicios críticos a menos que se esté conectado a través de una red privada

virtual (VPN). Una alternativa recomendada es optar por la conexión a Internet móvil a través de un paquete de datos.

- Uno de los principales objetivos de los delincuentes cibernéticos consiste en inducirte a descargar software malicioso, es decir, programas o aplicaciones que contienen virus y buscan sustraer información. Habitualmente, estos programas maliciosos se presentan como aplicaciones populares, como juegos, informes de tráfico, pronósticos del clima o servicios de entretenimiento, como películas, series o música. La empresa minera debe contar con un software de seguridad que resguarde los dispositivos de todas las amenazas, detectando y eliminando los virus. Es crucial mantener actualizado tanto el sistema operativo como las aplicaciones utilizadas con frecuencia.

CAPÍTULO VI

REFERENCIAS

6.1 FUENTES BIBLIOGRÁFICAS

Barrera, J. tesis "Propuesta de Sistema de Gestión de Seguridad de la Información utilizando la Norma ISO 27001 para la Unidad Educativa Nuestra Señora de Fátima". Universidad Tecnológica Israel. Quito – Ecuador. 2019.

Delgado, M. & Vásquez, J. tesis "Modelo de seguridad informática aplicando la norma ISO/IEC 27001 para proteger los activos de información en la empresa Berendson Natación S.R.L.". Universidad de Lambayeque. Facultad de Ciencias de Ingeniería – Escuela profesional de Ingeniería de Sistemas. Perú. 2019.

Guano, M. & Jaramillo, M. tesis "Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio". Escuela Politécnica Nacional – Facultad de Ingeniería de Sistemas. Quito – Ecuador. 2020.

López, J. tesis "Implementación del SGSI, basado en la ISO/IEC 27001 para dar tratamiento al riesgo en una empresa constructora". Universidad San Ignacio de Loyola – Facultad de Ingeniería – Carrera de Ingeniería Empresarial y de Sistemas. Lima – Perú. 2022.

Maureira, D. tesis "Norma ISO/IEC 27001 aplicada a una carrera universitaria". Universidad Andrés Bello – Facultad de Ingeniería. Santiago de Chile. 2017.

Reyes, F. tesis "Implementación de recomendaciones y el fortalecimiento en el sistema de gestión de seguridad y salud laboral en la empresa minera Yanacocha S.R.L. período 2017 – 2019". Universidad Nacional de Cajamarca – Escuela de posgrado – Unidad de posgrado

de la Facultad de Ciencias Económicas, Contables y Administrativas – Programa de Maestría en Ciencias. Perú. 2021.

Ticona, H. tesis "Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa ICO el año 2021". Universidad Privada del Norte – Facultad de Ingeniería – Carrera de Ingeniería de Sistemas Computacionales. Lima – Perú. 2021.

Torres, C. trabajo de graduación "Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada MEGAPROFER S.A.". Universidad Técnica de Ambato – Facultad de Ingeniería en Sistemas, Electrónica e Industrial – Carrera de Ingeniería en Electrónica y Comunicaciones. Colombia. 2020.

Vásquez, J. tesis "Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI". Universidad Nacional Mayor de San Marcos – Facultad de Ingeniería Industrial – Escuela Profesional de Ingeniería Industrial – Perú. 2018.

Yañez, N. tesis "Sistema de Gestión de Seguridad de Información para la Subsecretaría de Economía y Empresas de Menor Tamaño". Universidad de Chile – Facultad de Ciencias Físicas y Matemáticas – Departamento de Ciencias de la Computación. Chile. 2017.

6.2 FUENTES ELECTRÓNICAS

https://advisera.com/27001academy/es/que-es-iso-27001/

https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla

https://ostec.blog/es/aprendizaje-descubrimiento/los-pilares-de-la-seguridad-de-la-informacion-segun-la-norma-iso-27001/

https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/

https://www.itconsultors.com/que-es-la-gestion-de-datos

https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html

https://cpl.thalesgroup.com/es/software-monetization/what-is-software-security

https://protecciondatos-lopd.com/empresas/seguridad-hardware/

https://www.iso27000.es/glosario.html

http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992020000400011

https://peritoinformatico.es/cuales-son-los-fallos-de-seguridad-informatica-mas-frecuentes/

https://www.imagar.com/blog-desarrollo-web/principales-problemas-de-seguridad-informatica/

ANEXOS

Anexo N° 1

Cuestionario N° 01 - ENCUESTA

UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

CUESTIONARIO DE ENCUESTA PARA MEDIR EL "DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA MINERA COLIBRI S.A.C. – LIMA 2023
".

A.- Presentación:

Estimado (a) señor (a), el presente cuestionario es parte de una investigación que tiene por finalidad obtener información, acerca del "Diseño e implementación de la ISO 27001 para mejorar la Seguridad de Información de la empresa minera Colibrí S.A.C. – Lima 2023". Respuestas personales que solamente, son de gran importancia para mi investigación y que serán procesadas con toda confidencialidad, respetando el anonimato en la presentación de los resultados.

B.- Indicaciones:

- ✓ Este cuestionario es anónimo. Por favor responda con sinceridad.
- ✓ Lea detenidamente cada ítem. Cada uno tiene cinco respuestas, de las cuales sólo seleccione una.
- ✓ Conteste a las preguntas marcando con una "X" en un solo recuadro que, según su opinión. La escala de calificación es la siguiente:
  1 = Nunca, 2 = Casi Nunca, 3 = A Veces, 4 = Casi Siempre, 5 = Siempre

Ítem	DISEÑO E IMPLEMENTACIÓN DE LA ISO 27001	1	2	3	4	5
1	¿La norma ISO 27001 refiere claramente su confidencialidad en los activos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?					
2	¿La norma ISO 27001 refiere claramente su confidencialidad en los valores para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?					
3	¿La norma ISO 27001 refiere claramente su confidencialidad en las mejoras de la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?					
4	¿Sabe Ud. si la norma ISO 27001 formula la disponibilidad del procesamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.					
5	¿Sabe Ud. si la norma ISO 27001 formula la disponibilidad del almacenamiento de los datos para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.					
6	¿Sabe Ud. si la norma ISO 27001 formula la disponibilidad de las partes interesadas para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.					

7	¿Cree Ud. que la norma ISO 27001 aporta mucho legalmente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.					
8	¿Cree Ud. que la norma ISO 27001 aporta mucho reglamentariamente en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.					
9	¿Cree Ud. que la norma ISO 27001 aporta mucho en situaciones contractuales en su integridad para mejorar la seguridad de información en la empresa minera Colibrí SAC – Lima 2023?.					
Ítem	**SEGURIDAD DE LA INFORMACIÓN**	**1**	**2**	**3**	**4**	**5**
10	¿Es vital la seguridad de los controles de la red en la empresa minera Colibrí SAC – Lima 2023?					
11	¿Es vital la seguridad en el acceso a la red en la empresa minera Colibrí SAC – Lima 2023?					
12	¿Es vital la seguridad de los tratamientos en la red de la empresa minera Colibrí SAC – Lima 2023?					
13	¿Adquirir un buen software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?					
14	¿El diseño del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?					
15	¿El mantenimiento del software mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?					
16	¿Resulta importante para ti la procedencia del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?					
17	¿Resulta importante para ti la protección del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?					
18	¿Resulta importante para ti la auditoría del hardware en la mejora la seguridad de la información en la empresa minera Colibrí SAC – Lima 2023?					

Gracias por tu colaboración