Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Trabajo de Suficiencia Profesional

ISO 27001 para mejorar la seguridad de la información en una empresa tecnológica, Lima 2024

Para optar el Título Profesional de

Ingeniero de Sistemas e Informática

Presentado por:

Autor: Cruz Cordova, Harold

Código ORCID: https://orcid.org/0000-0001-7143-6395

Autor: Gamarra Chumbes, Christian Arturo

Código ORCID: https://orcid.org/0009-0002-8001-3225

Asesor: Mg. Chávez Alvarado, Walter Amador

Código ORCID: https://orcid.org/0000-0001-8614-482X

Lima – Perú

2026

Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, **Cruz Córdova Harold y Gamarra Chumbes Christian Arturo**, egresados de la **Facultad de Ingeniería y Negocios** y Escuela Académica Profesional de **Ingenierías** de la Universidad privada Norbert Wiener declaro que el trabajo de investigación "ISO 27001 para mejorar la seguridad de la información en una empresa tecnológica, Lima 2024". Asesorado por el docente: Mg. Walter Amador Chávez Alvarado DNI 09731774 ORCID 0000-0001-8614-482X, tiene un índice de similitud de **17 (diecisiete) %** con código oid: 14912:542228311 verificable en el reporte de originalidad del software Turnitin.

Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.

…… ……

Firma de autor 1
Harold Cruz Córdova
DNI: 42559460

Firma de autor 2
Christian Arturo Gamarra chumbes
DNI: 40953245

……

Firma del Asesor
Walter Amador Chávez Alvarado
DNI: 09731774

Lima, 24 de julio de 2025

Dedicatoria

Este proyecto está dedicado a nuestras madres que día a día están y estuvieron cuando las necesitamos gracias a ellas somos personas correctas y de gran corazón.

Agradecimiento

Agradecemos en primer lugar a Dios nuestro creador y guía en el camino diario, un agradecimiento a nuestra familia que es el empuje que necesitamos para embarcarnos en esta etapa en ser profesional y no podemos olvidar de nuestros docentes quienes nos inculcan los valores a la profesión y de nuestros compañeros que se convirtieron en amigos de carrera y de la vida.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

Resumen

El presente estudio permite precisar en qué medida la ISO 27001 aumenta la seguridad de la información de la compañía en estudio, como es el de implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información que pueda mantener la confidencialidad, integridad y disponibilidad de la información.

Para el estudio se utilizó el método hipotético-deductivo y analítico con enfoque de investigación cuantitativa, con diseño no experimental, asimismo, para la muestra representativa se tomó 20 controles a evaluar de un total de 114 que conforman los criterios de la ISO 27001. Además, se usó una ficha de observación, la cual permitió realizar una validación de los eventos con posible riesgo que afecte la seguridad de la información.

Así mismo se dividió en tres aspectos donde la primera fue la confidencialidad dentro de ella está el pretest y el post-test, ambas muestran que existe una diferencia del 40%, se evidencia en la reducción de eventos de riesgo con el post-test. Para el aspecto de la disponibilidad donde el pretest y el post-test existe una diferencia del 27 %, de la misma forma, presentó disminución de los eventos de riesgo con el post-test. Y en el tercer punto de la integridad entre el pretest y el post-test existe una diferencia del 30%, al verificar, se comprueba que la diferencia es menor en los eventos de riesgo con el post-test.

Por consiguiente, las pruebas demostraron que ISO 27001 aumenta la seguridad de la información al reducir significativamente las tasas de incidentes, con una reducción del 75 % en la confidencialidad, el 50 % en la integridad y el 50 % en la disponibilidad.

***Palabras claves**: ISO 27001, seguridad de la información, disponibilidad, confidencialidad e integridad.*

Abstract

The present study allows us to specify to what extent ISO 27001 increases the information security of the company under study, such as implementing, maintaining and continuously improving an information security management system that can maintain the confidentiality, integrity and availability of the information.

For the study, the hypothetical-deductive and analytical method was used with a quantitative research approach, with a non-experimental design. Also, for the representative sample, 20 controls were taken to be reviewed from a total of 114 that make up the ISO 27001 criteria. In addition, an observation form was used, which allowed a validation of the events with possible risk that affect the security of the information.

Likewise, it was divided into three aspects where the first was confidentiality within it is the pre-test and the post-test, both showing that there is a difference of 40%, which is evidenced in the reduction of risk events with the post-test. For the availability aspect, where there is a difference of 27% between the pre-test and the post-test, there is also a decrease in risk events with the post-test. And in the third point of integrity, there is a difference of 30% between the pre-test and the post-test. When verified, it is found that the difference is smaller in risk events with the post-test.

Therefore, the results showed that ISO 27001 improves information security by significantly reducing incident rates, with a 75% reduction in confidentiality, 50% in integrity and 50% in availability

Key words: *ISO 27001, information security, availability, confidentiality and integrity.*

Introducción

En la actualidad, la tecnología y la ciencia de los datos han evolucionado a pasos agigantados considerando los eventos acontecidos en estos últimos tiempos, por ende, la ciberdelincuencia quienes se aprovechan de la falta de seguridad de información implementada por las compañías, en aspectos de la privacidad, integridad y acceso de la información Por lo tanto, la norma ISO 27001 nos permitirá corregir y mejorar los activos de la información de las empresas que lo necesiten, de tal forma, la empresa tecnológica conformada por su directorio tomó una excelente decisión en verificar la norma y realizar un contraste y mejorar las políticas que presentan, para la reducción de los eventos de riesgo, conforme se fue desarrollando el proyecto en detalle a continuación en 5 capítulos.

Capítulo I: En el problema a tratar, se desglosa la problemática del proyecto. Por lo tanto, se llegó a formular cuál es el problema y los posibles objetivos de la solución.

Capítulo II: Se relata lo que conforma al marco teórico, donde se realizó la búsqueda de los acontecimientos nacionales e internacionales y las posibles teorías, para el sustento de la investigación.

Capítulo III: En el caso de la metodología, se identificó, la forma, el modelo, el patrón, la población y el prototipo de nuestra tesis. De tal forma, se continuó con el manejo de las variables.

Capítulo IV: En los resultados y las discusiones, se consideró el análisis descriptivo. Asimismo, al trabajar con las hipótesis, se consideró, usar la prueba de consistencia, la prueba de normalidad y la prueba de contraste.

Capítulo V: En la Conclusiones y recomendaciones, se tomó en cuenta tres conclusiones de cada problema hallado y tres recomendaciones contando con la evaluación de la compañía tecnológica para la mejorar la forma de tomar las decisiones.

CAPÍTULO I: EL PROBLEMA

1.1 Planteamiento del problema

La seguridad de la información es un aspecto crítico por el gran manejo de datos y de la protección que estos requieren, así también como la competitividad de las empresas y organizaciones, requieren información para la toma de decisiones; sabiendo ello, debemos de tener en cuenta que la confidencialidad nos garantiza la privacidad de los datos mediante la restricción en diferentes aspectos, por otro lado la integridad nos garantiza que la información sea confiable, además, al hablar de la disponibilidad, como la misma palabra lo indica debe de facilitar la información o tenerla disponible para personas que están autorizadas para su administración. Asimismo, se enfrenta a una variedad de retos a nivel mundial, regional y local. En Europa, se ha reportado un aumento de los ciberataques y la ciberdelincuencia, que ponen en riesgo la privacidad, la veracidad y el uso de la información, así como la confianza en los servicios y herramientas digitales (Pontijas, 2023)En Europa el costo promedio de un ciberataque es de 1,4 millones de euros, un alza del 36% en comparación con el año anterior (Culot et al. 2021) Además, se prevé que para el año 2025, el efecto económico de la ciberdelincuencia en dicha región alcance los 2,5 billones de euros. En Latinoamérica, se ha observado una brecha en las capacidades de ciberseguridad de los países, que se refleja al no contar con políticas, normas, arquitecturas y gente especializada para prevenir y responder a las ciber amenazas (Aguilar, 2020). Se estima que el impacto económico de los incidentes vinculados con la seguridad de la información alcanza los 90.000 millones de dólares anuales, lo que equivale al 0,5% del PIB regional. Asimismo, se proyecta que el riesgo cibernético podría reducir el crecimiento potencial de la región en un 0,3% anual Organización de Estados Americanos (OEA, 2020). En el Perú, se ha evidenciado una baja inversión y una escasa cultura en la protección de la información en las empresas privadas, en

donde se hacen vulnerables a incidentes como la infección de malware, el robo de información, los accesos no autorizados y el secuestro de datos Banco Internacional de Desarrollo (BID, 2020), donde existe reportes que el 70% de las compañías que presentaron algún tipo de ataque informático en los últimos dos años, lo que ha generado pérdidas de hasta 10 millones de soles por cada evento. Igualmente, se estima que la ciberdelincuencia ha generado una pérdida anual de 1.500 millones de dólares, lo que sería en porcentajes un 0,7% del PBI nacional (Pueblo, 2023).

Por ello, se hace necesario mejorar las capacidades de ciberseguridad y ciber resiliencia a nivel global y regional, mediante la implementación de políticas, normas, infraestructura y recursos humanos especializados para prevenir y controlar a las ciber amenazas.

Respecto a la problemática local que se presenta en la compañía tecnológica, donde se encontró pérdida de información en casi todos sus accesos, además de que la información era manipulada por personas externas y no el personal autorizado o correspondiente al área, generando muy poca confianza, por ello se elaboró con una herramienta llamada árbol del problema (anexo 9), la cual nos permitió determinar las causas y el resultado de los problemas. Los problemas de la organización son: (i) confidencialidad de la información, el mayor riesgo de tener ataques cibernéticos, debido a que, al no adoptar controles para proteger los datos y la información, las empresas pasarían dificultades para identificar y mitigar los eventos de riesgo para la información; (ii) integridad de la información, con pérdidas financieras a causa de los ataques cibernéticos provocando pérdidas financieras significativas para la empresa. Estas pérdidas incluyen la pérdida de datos, interrupción de las operaciones y los costes de recuperación; (iii) disponibilidad de la información, generando la interrupción de las operaciones por los ataques cibernéticos generan pérdida de ingresos, clientes y reputación según la magnitud del problema.

1.2 Formulación del problema

1.2.1 Problema general

¿En qué medida la implementación de la ISO 27001 aumenta la seguridad de la información en una empresa tecnológica, Lima 2024?

1.2.2 Problemas específicos

¿En qué medida la implementación de la ISO 27001 aumenta el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024?

¿En qué medida la implementación de la ISO 27001 aumenta el nivel disponibilidad de la información en una empresa tecnológica, Lima 2024?

¿En qué medida la implementación de la ISO 27001 aumenta el nivel de integridad de la información en una empresa tecnológica Lima 2024?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Determinar en qué medida la implementación de la ISO 27001 aumenta la seguridad de la información en una empresa tecnológica, Lima 2024.

1.3.2 Objetivos específicos

OE1: Determinar en qué medida la implementación de la ISO 27001 aumenta el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024.

OE2: Determinar en qué medida la implementación de la ISO 27001 aumenta el nivel disponibilidad de la información en una empresa tecnológica, Lima 2024.

OE3: Determinar en qué medida la implementación de la ISO 27001 aumenta el nivel de integridad de la información en una empresa tecnológica, Lima 2024.

1.4 Justificación de la investigación

1.4.1 Teórico

El siguiente estudio, con respecto a la variable de investigación denominada ISO 27001, se utilizó cuatro teorías: (i) la teoría general de sistemas, también se le conoce como teoría de sistemas o teoría General de Sistemas en los estudios de los sistemas en general, viéndolo desde una forma interdisciplinaria, el biólogo alemán (Von Bertalanffy, 1968) desarrolló la teoría general de sistemas como una herramienta útil para diversas ciencias. No obstante, contribuyó a la creación de un nuevo paradigma científico basado en la interconexión de los componentes que tienen los sistemas. La teoría general de sistemas se ha utilizado en muchas ciencias desde su creación, en el contexto del análisis de interacciones (Business School, 2018). En nuestra investigación la teoría general de sistemas (TGS) nos permitió estudiar los principios aplicables en cualquier nivel en todos los campos de la investigación, ya que en la teoría nos habla de que el sistema de seguridad debe ser entendido como un todo y no como la suma de sus partes; (ii) la teoría de contingencias, que fue diseñada por primera vez en 1950 (Woodward, 1965). Que no solo hay una forma de organizar o gestionar una empresa para que sea universalmente efectiva. La base organizativa y las prácticas de gestión deben adecuarse conforme las contingencias o situaciones específicas en las que se encuentre la organización. Lo cual, implica que no solo hay un único enfoque para las empresas, sino que se debe acomodar a las circunstancias cambiantes del mundo empresarial (Narváez et al. 2022). Esta teoría nos permite la innovación y la transformación de la seguridad de información regida por el ISO 27001, donde este enfoque garantiza que los controles de seguridad sean efectivos, relevantes y proporcionales a las necesidades y riesgos específicos de cada organización; (iii) la teoría Z del liderazgo, según Ouchi (1981), quien publicó un estudio comparando las prácticas de gestión tanto en estadounidenses como también con los japoneses. En

su afán (Saeckel, 2023). de lograr un poco más que las aportaciones dadas por el empresario Douglas McGregor en los años cuarenta, de acuerdo a ello podemos decir que “La teoría Z promueve el trabajo en equipo, la confianza y la toma de decisiones colectivas. De ese modo, una empresa eleva su productividad y los empleados se sienten más satisfechos y motivados”. Esta teoría nos ayuda a verificar la confianza y toma de decisiones en los trabajadores con referencia al uso del ISO 27001, ya que deben diseñarse de manera que sean eficaces, pero también convenientes para los empleados, asegurando que se mantenga un buen equilibrio entre la seguridad y la facilidad de uso.; y (iv) la teoría de la calidad total, en 1960 un administrador y químico industrial de una empresa japonesa, que sustenta la teoría creada por Kaoru Ishikawa quien dijo que era una filosofía de la organización, en la que todos sus integrantes estudian, practican, participan y fomentan la mejora continua (Viteri Quishpi, et al. 2022). Esto quiere decir que se centra en la producción de productos y servicios de calidad para satisfacer las necesidades de cada uno de los clientes.

Con respecto a la variable dependiente referido a la seguridad de la información, se consideran las siguientes teorías: (i) teoría de la seguridad de la información, en 1949, la teoría es también conocida como la teoría matemática de la comunicación, ya que su enfoque está orientado a analizar, cómo procesar y medir datos (Claude, 1948). Esto se relaciona con el proyecto que se realiza al emplear los 20 controles para analizar el nivel de seguridad de la organización. (ii) teoría general de sistemas, se definen por la naturaleza del intercambio de información que se maneje en su entorno, al enfocarlo con el proyecto, podemos señalar que en el intercambio de información existe ciertas vulnerabilidades en el transcurso del manejo de los datos (Von Bertalanffy,1968). En esta parte entra a tallar lo que es la seguridad de la información.

1.4.2 Metodológica

En la metodología se empleó un enfoque cuantitativo de tipo aplicado, con un diseño experimental, con el propósito de mejorar la seguridad de la información manejada en la empresa tecnológica y desarrollar la solución óptima que satisfaga las expectativas de la dirección institucional. El objetivo de esta investigación es brindar tanto conocimientos teóricos como prácticos a los investigadores interesados en profundizar en el tema de estudio. Asimismo, para la metodología de la implementación del sistema de gestión de seguridad de la información (SGSI), se consideró sus tres pilares:

Confidencialidad

En este punto se reconoce que la información manejada en la empresa es confidencial y no debe divulgarse a terceros. Con este entendimiento, se proporcionó a la empresa la información requerida para implementar los controles pertinentes, específicamente relacionados con la norma ISO 27001 (Unir, 2023). De esta manera, los empleados comprenden que la información es propiedad exclusiva de la empresa y solo puede ser utilizada por el personal autorizado.

Disponibilidad

En este punto se alude a la disponibilidad de que individuos, empresas o procesos autorizados puedan acceder a la información empresarial, a pesar de que esto pueda parecer contradictorio con la confidencialidad. Sin embargo, al incorporar los controles de la norma ISO 27001 y brindar una capacitación breve al personal, se les explica que al permitir este acceso se evita cualquier robo de información en la empresa, asegurando la integridad de los datos (Unir, 2023).

Integridad

En esta fase se reconoce que los datos no deben ser modificados o alterados sin la autorización justificada de la empresa. Tras identificar deficiencias en la integridad de la empresa, se enfatizó

la importancia de mantener íntegros los controles de la norma ISO 27001, especialmente en este aspecto. La constante modificación de los datos podría ocasionar fallos en el sistema y facilitar el robo de información (Unir, 2023).

1.4.3 Práctica

Este estudio experimental tiene como propósito ayudar a la organización a identificar y reducir los riesgos de seguridad de la información, protegiendo la información confidenciales e importantes. De esta manera, reduce los costos de incidentes de seguridad de datos y mejora su reputación y credibilidad ante clientes, proveedores y socios comerciales. En ese sentido, la norma ISO 27001 es una herramienta útil para resguardar la seguridad de la información en las organizaciones. De igual manera el uso de un Sistema de Gestión de la Seguridad de la Información (SGSI) el cual es un conjunto de políticas de administración de la información, utilizado principalmente por la ISO/IEC 27001, así mismo en un estándar internacional, el Objetivo de un Sistema de Gestión de la Seguridad de la Información es garantizar que los riesgos sean conocidos, asumidos, gestionados, haciendo que estos sean minimizados por la organización de una forma documentada, sistemática y estructurada (González, 2021).

1.5 Limitaciones de la investigación

El estudio se llevó a cabo de agosto de 2023 a enero de 2024. El estudio se hizo en una compañía tecnológica, que pertenece al distrito de Lince, en la provincia y departamento de Lima. Una de las grandes limitaciones que encontramos en esta empresa es que no tiene implementado al 100% los controles de SGSI (sistema de gestión de seguridad de la información) el cual hace que esta empresa sea vulnerable por no asegurar la integridad y confidencialidad de los datos de la misma. Asimismo, el estudio también se enfocó en la industria de TI como parte de su alcance. El estudio

tuvo un valor estimado de S/ 15,000.00, en donde, el 50% fue invertido por los expertos del tema y la compañía con el otro porcentaje faltante.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

Nacionales:

Asqui y Torres (2023) según su investigación realizada en Lima, tuvo como objetivo "Evidenciar como la ISO 27001 aumentaría la confianza, integridad y la disponibilidad de la información en una organización". Por cuanto, este estudio utilizó una metodología cuantitativa con un diseño experimental que convergen en un alineamiento deductivo, hipotético y analítico en una población de 24 controles considerando los parámetros de ISO 27001. Con respecto a la técnica, se empleó la observación, y el instrumento, que se usó, es la guía de observación. Asimismo, en el caso de los resultados, se utilizó, el ciclo de Deming, para poder mejorar de forma general las normas de seguridad, mientras que la prueba de T-Student se utilizó con indicadores paramétricos. Esta prueba demostró que las dos tasas de incidentes de confidencialidad eran notables en promedio, con un promedio en el pre-test del 88,9 % y un promedio en el post-test del 27,6 % e. De esta manera, se llegó al nivel que se necesitaba con el uso de la prueba T-Student y se encontró, que en el caso del resultado del valor "Sig." fue menor que 0.05 en el caso de los eventos relacionados con la confidencialidad. Como resultado, aceptaron los controles de ISO 27001 para mejorar la institución educativa de la cual están tratando. La ISO 27001 mejora la seguridad de la información, reduciendo significativamente las tasas de incidentes en la confidencialidad, la integridad y la disponibilidad, respectivamente. Se ha llegado a la conclusión de que la aplicación de la norma ISO 27001 ha mejorado la confidencialidad, la seguridad y la integridad de la

institución educativa, lo que ha permitido disminuir la tasa de incidentes que afectan la disponibilidad. Antes, la institución manejaba un promedio de 130 incidentes, pero al implementar la ISO 27001, se han reducido a 20 sucesos, lo que ha beneficiado a la compañía.

Moron (2023) en su investigación en Lambayeque, buscó: "Diseñar un Sistema de Seguridad de la Información para una empresa privada orientada a los nuevos estándares internacionales de las TI". De esta manera, utilizaron una técnica conocida como el ciclo de Deming, basándose en la ISO 27001, y encuestaron a 100 trabajadores con un cuestionario de 14 preguntas. La observación directa fue el método utilizado, y la entrevista se utilizó como ayuda para el estudio. Y como constancia escrita en la investigación, se utilizó la ficha técnica. Como resultado, el valor promedio del análisis previo fue del 69.90%, mientras que el valor promedio del análisis posterior fue del 14.00%. Sin embargo, el valor menor del pre-test fue de 50%, mientras que el valor mayor fue de 88%, por otra parte, el valor menor del post-test es de 0% y el valor mayor es de 27%. Finalmente, el nivel de significancia en el examen previo fue de 0.265, mientras que en el examen posterior fue de 0.108. Determinando si el indicador es compatible con una distribución normal paramétrica ($P > 0.05$). Para la constatación de la hipótesis, se aplicó la prueba t de Student. En conclusión, mientras la compañía evidencia deficiencias como, falta de conocimiento en políticas de seguridad, acceso a personal no autorizado, deficiencia en los procedimientos de eliminación de acceso a usuarios y falta de orientación y concientización en la seguridad de la información.

Balladares (2023) de acuerdo con su investigación realizada en Lima, encontró como objetivo: "Establecer en qué medida afecta la implementación de la norma ISO 27001 en el control de la seguridad de la informática en una consultoría particular". Por lo tanto, se utilizó un enfoque cuantitativo correlacional para el diseño preexperimental y la investigación de tipo aplicada. Por

otra parte, el tipo de población fue finita empleando 27 personas de la parte administrativa. Usando el método de recolección de datos y los cuestionarios, validados por tres expertos. Los resultados del análisis descriptivo confirmaron que el pre-test tuvo un valor promedio de 0.1863 mientras que el post-test tuvo un valor promedio de 0.163. También hubo un valor de significancia entre los dos valores. es de 0.00($p<0.05$). Asimismo, para el cálculo del valor del coeficiente de confiabilidad se usó el alfa de Cronbach, ya que se usa una escala politómica. Por lo tanto, los resultados muestran que la hipótesis alternativa está en línea y la hipótesis nula está descartada. Razonando que la norma ISO 27001 controla adecuadamente la adaptación de datos en su control de seguridad de datos. Se encontró que la evidencia de la implementación de la norma ISO 27001 mejoró la protección de la información de las consultoras privadas. Además, gracias a la implementación de la norma la organización se encuentra protegida acorde con las exigencias del mercado. Sin lugar a duda mejoró considerablemente la accesibilidad de su información, seguridad de encriptación de datos y los usuarios con privilegios para la obtención de la información de la empresa.

Medina (2023) conforme a su investigación realizada en Lima, se tuvo como objetivo: "Encontrar de qué forma el ISO 27001 afecta en la gestión de la seguridad de la información en el área de TI en una industria". Sin embargo, la técnica utilizada fue cuantitativa y de tipo correlacional causal. Se utilizó una muestra de 31 empleados de TI como muestra total, con una posición de muestreo censal no probabilística. La técnica de recolección de datos utilizada fue la encuesta y su instrumento fue el cuestionario. Se descubrió que la ISO 27001 aumentó la seguridad de la comunicación, la criptografía y el manejo de activos en un 35 % y la eficacia de las gestiones operativas de los sistemas en un 29 %., de tal forma se reflejó una $p<0.05$. Se usó la prueba de confiabilidad de alfa de Cronbach con un resultado de 0.803, obteniendo un instrumento confiable. Se descubrió que la métrica ISO 27001 tiene un impacto significativo en la seguridad de la

información en el sector de TI. Demostrando cambios significativos en la gestión de procesos de la organización.

Internacionales:

Torres (2020) en su investigación realizada en el país de Ecuador, donde su objetivo fue: "Determinar un plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A". Con un enfoque analítico, y sus métodos de investigación incluyeron observación, encuesta y entrevista. La población empleada fueron los trabajadores siendo un total de 4 empleados. Como resultado pudieron observar con relación a la implantación del SGSI en base a la norma ISO 27001, tuvo una gestión de manera favorable siendo esta de mejora. Como conclusión se toma conocimiento sobre la importancia que tiene la seguridad de la información en la actualidad, dándonos a conocer de esta manera que en una institución es fundamental contar un sistema de gestión de la seguridad de la información aplicado mediante la norma internacional ISO 27001.

Alvarez (2019) de acuerdo con su investigación realizada en Ecuador, donde su objetivo fue: "Emplear un plan de seguridad informática colaborando con la norma ISO 27001 en una empresa de calzado". Su enfoque de empleo fue analítico, y sus métodos de investigación incluyeron observación, encuesta y entrevista. La población empleada fue todo el personal de la empresa de calzado. Como resultado, la empresa sufre constantes pérdidas económicas, por las insuficiencias en el uso de la información. Por lo tanto, como conclusión se debe considerar la elaboración de un plan informático que indique clara y eficientemente como llevar los procesos en la empresa a tratar.

Arévalo et al. (2015), de acuerdo con su investigación realizada en el país de Colombia, se obtuvo como objetivo: “Analizar la situación de la gestión de seguridad de información en pequeñas y medianas empresas de la ciudad de Ocaña y proponer un modelo de implantación de un sistema de gestión de seguridad de información bajo la norma ISO 27001”. Para lograr este objetivo, se realizó una investigación de forma descriptiva la cual se desarrolló mediante una encuesta para recopilar información sobre las prácticas actuales de seguridad de información en las empresas. Para analizar los datos y proponer este modelo de implantación de un sistema de gestión de seguridad de información, se formó un equipo de trabajo multidisciplinario. Los resultados arrojaron que la mayoría de las empresas a las cuales se les realizó una encuesta no tienen un sistema formal de gestión de seguridad de la información, por lo que se necesitan medidas preventivas urgentes para proteger la información confidencial. Se propuso un modelo para la implementación de un sistema de gestión de seguridad de información según la norma ISO 27001 que las empresas pueden utilizar para mejorar la protección de sus datos. Se propuso un modelo para la implementación de un sistema de gestión de seguridad de información según la norma ISO 27001 que las empresas pueden utilizar para mejorar la protección de sus datos.

Carreño(2024) en su investigación realizada en Bogotá. Donde su objetivo principal es “Establecer las garantías de los tres pilares de la información: confidencialidad, integridad y disponibilidad”. El método que emplearon fue a través del levantamiento de información organizacional y de los activos tecnológicos que garanticen la prestación de sus servicios, mediante un instrumento como el cuestionario y su técnica la encuesta y reunir toda la información posible. Se crearon políticas de seguridad para establecer los estándares generales de la empresa. Como resultado, se demostró que era necesario construir un área de seguridad de la información que cumpliera con las políticas de seguridad establecidas en la norma ISO 27001. Se concluye que

toda la información manejada en esta investigación, se le hace entrega a la compañía, haciendo llegar la matriz de riesgos en donde se expone con lo que se cuenta actualmente, quedando a disposición de la alta gerencia para que determine sus prioridades en la implementación.

2.2 Bases teóricas

2.2.1. Conceptualización de la variable independiente: ISO 27001

La norma principal de la familia SGSI es esta. Describe cómo establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI. Con esta norma se logra certificar las organizaciones que deseen certificar sus Sistemas de Gestión de Seguridad de la Información (Pequeño, 2015). Según Guevara et al. (2022), en su publicación el ISO 27001 dicha norma nos permite gestionar de una forma óptima y precisa una política de seguridad de información, otorgando características lógicas para mejorar la calidad de su servicio, así también como la imagen institucional, atentos a las fuentes de información que permanezcan dentro de la organización, protegiéndola de ataques cibernéticos con la gestión de riesgos, de tal manera, se tendría que aplicar políticas de control de acceso. En la redacción de Trejo (2020), se basa en la gestión de seguridad de manera continua sustentada con la identificación de los riesgos ya que toma un proceso encaminado para constituir, instrumentar, desempeñar, seguir, inspeccionar, tener y poder de esta forma mejorar el sistema de gestión para proteger la información de la empresa. En otras normas se emplean los conceptos de “línea base de seguridad”, que como ISO 2701 se le denomina inicio de la seguridad de la información; que vienen a ser una de las principales guías; para la aplicación en la mayoría de las organizaciones, en base de su implementación para el control esencial como práctica en común para la seguridad de la información (Giménez, 2023). Por otro lado, Martin (2021), manifiesta que, al reforzar sus bases de la seguridad de la

información, los riesgos de fraude disminuyen; así como también; la pérdida de la información, incluso la filtración de esta. En ese sentido, la ISO 27001 es un estándar internacional que establece las especificaciones para un sistema de gestión de la seguridad de la información (SGSI). La norma ha sido actualizada varias veces para mejorar su claridad, flexibilidad y orientación al riesgo. Por ello, la ISO 27001 es una norma ampliamente reconocida y utilizada por organizaciones de todos los tamaños y sectores para gestionar los riesgos de seguridad de la información. Por ello, en la gestión de seguridad las organizaciones deben tener unas políticas que reflejen el control de todos los posibles riesgos que se puedan presentar, y así, para lograr tener el mejor estándar en el rubro que se desempeñen.

La teoría de sistemas de Bertalanffy

Según Vázquez (2023), actualmente el impacto que ha tenido la teoría de sistemas, en sonados casos del mundo, conlleva al hecho de que permite entender el funcionamiento del mundo, desde el sistema más pequeño hasta el más complejo, e incluso en redes sistémicas complejas, en los casos que los sistemas demuestran que el todo es mayor que la suma de sus partes. Tratando de identificar sus propiedades características de su entorno y, a su vez, trasladando a la realidad en la que vivimos. Del mismo modo según Griselda (2002), se enfoca en las propuestas sistemáticas de varios autores porque ofrecen una interpretación política de la teoría de los sistemas. Donde los autores que emitieron sus primeras opiniones están claramente enfocados en la lógica de la ciencia y la sociología política, lo que los lleva a enfocarse en el sistema de toma de decisiones. Por otro lado, los segundos autores muestran cómo la teoría de sistemas ayuda al investigador a articular la política, la economía y la cultura, las cuales se definen como ejes explicativos en cualquiera de esos ámbitos. En ese sentido, Farrand (2005), manifiesta en su artículo que, muchos proyectos de investigación se alinean con él un marco teórico para empezar un estudio, sin embargo, con mucha

pena decimos que, este no siempre es directamente relevante. Es importante destacar que ofrece múltiples puntos de vista teóricos que requieren una explicación mediante la utilización de un modelo que conecta la teoría con el estudio práctico. Asimismo, en el ámbito actual y pensando a futuro como persona o compañía debemos analizar y escoger el mejor sistema de seguridad para la información, en ese sentido, conseguir los mejores aliados y de esta forma seguir desarrollándose de manera comercial y financieramente.

La teoría de contingencias

Según Cristian (2020), en su publicación propone la evaluación de los más resaltantes aportes teóricos que han desarrollado en la administración, tanto le teoría de las contingencias como la teoría de la ecología poblacional, tomando el tema a comparar como es la estructura organizacional y su variable del diseño. Ya que se desea, identificar algunos puntos de encuentro y discrepancias entre ambas perspectivas. En este artículo se presenta una síntesis que reúne una serie de trabajos escritos por diferentes autores y su comparación se centra en la hipótesis de que ambas teorías son más complementarias que excluyentes. De esta manera, en este estudio se habla de la revisión de la literatura de la teoría de la contingencia en administración gerencial (Porporato & Waweru, 2011). Desde la década de 1980, nos permite analizar y enfocar la investigación y el tipo de estudio que dio forma al trabajo. Sin embargo, en los últimos cincuenta años, la teoría de la contingencia ha sido un tema importante en la investigación del desarrollo de las estructuras organizacionales (Jorge, 2013). Sus aportes se enfocan en diversas áreas, siendo una de ellas la lista de factores de continuidad y la identificación de la conexión entre ellos y los componentes estructurales. De esta manera se deduce que los planes de contingencia, son realmente de suma importancia, en toda forma de riesgos de seguridad que necesiten en las compañías, ya que, de esta manera tendrían la confiabilidad que todo cliente necesita.

La teoría Z del liderazgo

Según Mónica G. (2015), se presenta un modelo de liderazgo utilizando teorías organizacionales, en base a una revisión de la literatura de 35 artículos, y adicional a ello se consideran 20 libros con el software Atlas TI. Por este motivo se pudo identificar los componentes involucrados en el proceso de liderazgo, como el entorno, la situación específica, el líder, la organización, la entrega, los resultados, el cliente y la comunidad. Los cuales fueron una amplia fuente de datos para el desarrollo del modelo en el que todos los elementos interactúan. El ejercicio de liderazgo implica una variedad de aspectos para garantizar el liderazgo como un todo, y no es exclusivo del líder. Del mismo modo, existen diferentes tipos de líderes en las organizaciones, como resultado de las normas y prácticas culturales de la cultura organizacional donde se encuentra el líder (Alejandro C. 2006). Los líderes son aceptados si sus características coinciden con las teorías de los seguidores, manifestadas en la cultura y las prácticas culturales de la organización. Su objetivo consiste en examinar las diferencias individuales en las teorías del liderazgo implicadas en los contextos de índole civil o militar. De acuerdo a sus resultados obtenidos en una comparación de grupo de personas, los líderes se manifiestan de acuerdo a sus contextos individuales. Según Villa et al. (2018), este ensayo describe brevemente cómo ha cambiado el pensamiento administrativo para demostrar que las estrategias de cambio se enfocan en aspectos humanos en lugar de variables técnicas. Los psicosociales de las organizaciones a veces buscan que las personas cambien sus actitudes y comportamientos para mejorar la productividad y la eficacia general de la organización. Este artículo establece una relación entre el liderazgo como situacional en función del grado de estructuración de los problemas. De tal forma que, podemos decir que toda empresa líder, se basa en el trabajo y sacrificio de su gente colaboradora, que la formación se sus equipos tienen que ver

mucho con el liderazgo de cada grupo humano, al ser equilibrado sus resultados van a ser satisfactorios.

Definición de ISO 27001

La ISO 27001 es una norma internacional de Seguridad de la Información que ayuda a poder mantener de forma segura la confidencialidad, integridad y disponibilidad de toda la información de una organización, especialmente de empresas, también de los sistemas y de sus aplicaciones. Fue desarrollada por la Organización Internacional de Normalización o IOS por sus siglas en inglés (International Organization for Standardization) y por la Comisión Electrotécnica Internacional o IEC (International Electrotechnical Commission). La norma define de manera genérica, independientemente de los factores ambientales de organización internos y también externos, así como activos de los procesos de la organización (UNIR,2019).

Características de la norma ISO 27001:

Según Ostec (2015), muestra las siguientes definiciones y características en el ISO 27001: (i) el análisis de riesgo, esta norma exige que se realice periódicamente un análisis de riesgo a todas las empresas que cuenten con un sistema informático y de acuerdo con ello realizar cambios significativos si lo requieren. Después de realizar este análisis, es importante asegurarse de que se lleve a cabo de manera adecuada, estableciendo los criterios de aceptación de riesgos y estableciendo la forma de ser medidos. Asimismo, se debe considerar, las consecuencias que estos riesgos identificados, que puedan ocurrir y sus niveles; (ii) el compromiso de la alta dirección, en esta norma es imperativo que, la alta administración está muy comprometida con el SGSI, es allí, donde la empresa presenta la mayor parte de la responsabilidad por la seguridad de la información. Los directores son encargados de asegurarse de forma responsable de que los recursos para la implementación del sistema estén disponibles y asignados correctamente, así como de indicar a

los colaboradores para garantizar que el sistema sea verdaderamente eficiente; (iii) la definición de objetivos y estrategias, mediante la planificación, es necesario que la organización cuente con los objetivos de seguridad claros y las estrategias establecidas para alcanzar esos objetivos. Los objetivos no deben ser genéricos, si no, deben ser mensurables contando con los requisitos de seguridad; iv) las empresas deben garantizar que todos los recursos necesarios para la instalación y el mantenimiento de sistemas accesibles. Además, se necesita establecer competencias necesarias para que las personas responsables garanticen su experiencia, incluyendo sus documentos comprobatorios.

Ventajas de la norma ISO 27001:

Estas son las ventajas de implementar la norma ISO 27001; (i) el equilibrio y coordinación de los procesos de seguridad;(ii) el cual, reducir los riesgos y aumenta el nivel en gestión de la seguridad gracias a sus metodologías; (iii) le permite un plan de acción para evitar cualquier riesgo de amenaza; (iv) se prioriza la ejecución de los requerimientos legales; (v) al promover la eficiencia reduce los costos; (vi) se construye ambientes de confianza entre las partes implicadas en la organización (Tecnología, 2019).

Dimensiones de la norma ISO 27001:

Dimensión 1: Planificar:

Según Alba (2021), nos comenta que, esta dimensión es parte de la estructura del ciclo de Deming, la cual, es la fase inicial del SGSI donde se verifican los riesgos que pueden presentarse en la seguridad de la información. En donde se realiza un análisis de los riesgos potenciales para identificarlos y luego planificar una respuesta y control de los mismos para reducirlos. Asimismo, esta etapa que pertenece a la gestión de calidad PDCA, la cual es referente a Planificar, Hacer, Verificar y Actuar por sus siglas en inglés se le conoce como PDCA (Plan, Do, Check, Act) o

también conocida como ciclo de Deming (Tecnología, 2019), es donde se desarrolla la etapa inicial del proceso de diseño de SGSI en la que se identifican los riesgos relacionados con la seguridad de la información. Los métodos cuantitativos y cualitativos utilizados en este estudio complementan los mecanismos necesarios para mitigar estos riesgos.

Indicadores:

Conocer el estado actual de la situación que se quiere mejorar o cambiar.

Establecer metas y objetivos claros y medibles.

Monitorear y evaluar el progreso y los resultados de las acciones.

Dimensión 2: Hacer:

Alba (2021) habla que, esta dimensión pertenece a la estructura del ciclo de Deming, en la que se encarga de implantar y trabajar con el propio SGSI que con anticipación se desarrolló y ejecutó. Asimismo, (Tecnología, 2019) dice que, la dimensión "do" que forma parte de la gestión de la calidad PDCA, es en donde se implementa y opera el sistema de gestión de seguridad de la información definido y desarrollado.

Indicadores:

Porcentaje de cumplimiento de la empresa.

Tiempo de ciclo de SGSI.

Tasa de defectos del sistema de gestión de seguridad.

Dimensión 3: Verificar:

Alba (2021) nos cuenta que, la dimensión de la cual se está hablando, pertenece al ciclo de Deming, en esta etapa se revisa y evalúa el SGSI implementado resulta eficaz, de lo contrario se analiza las causas que pueden estar sucediendo y para ello se realiza una serie de mejoras. Asimismo, esta dimensión se encarga de revisar y evaluar en cuanto a la eficacia y la eficiencia con la que cuenta

(Tecnología, 2019). En todo caso, si el desempeño no es el esperado se analiza las causas y se determina las mejoras.

Indicadores:

Asegurar la calidad y la confiabilidad del modelo o el producto.

Detectar y corregir posibles errores, defectos o desviaciones.

Evaluar el grado de satisfacción de los clientes o usuarios.

Dimensión 4: Actuar:

Alba (2021) nos comunica que, esta dimensión que pertenece al ciclo de Deming, es aquí en donde su principal finalidad o función es la de establecer una mejora y actualización continua en el SGSI. De esta manera, (Tecnología, 2019) comenta que, en esta dimensión se encarga de estar al pendiente de la mejora continua del sistema de gestión de la seguridad de la información.

Indicadores:

Identificar las oportunidades y las necesidades.

Medir el impacto y el valor agregado de las acciones.

Ajustar y optimizar los procesos y los recursos.

2.2.2. Conceptualización de la variable dependiente: Seguridad de la Información

Diferentes autores señalan que es una ciencia en evolución continúa teniendo como fin cumplir con los objetivos de la organización y también implementa sistemas considerando los riesgos relativos a las TICS. Donde la seguridad de información “es la protección de la información y los sistemas de información contra amenazas que puedan poner en riesgo su confidencialidad, integridad o disponibilidad" (Briceño, 2021).

Teorías de la seguridad de la información:

Teoría de la información: En el caso de Shannon y Weaver (1949), manifiesta que la teoría es también llamada como la teoría matemática de la comunicación, es un enfoque que analiza cómo procesar y medir datos, donde el proceso de comunicación sugerido permitirá que el mensaje fluya a través de un canal específico entre un emisor y un receptor. Esto quiere decir que con respecto a nuestra variable de seguridad de la información esta teoría está relacionada ya que, al enviar o recibir fuentes de información, a través de un transmisor como una fibra óptica donde se emite una señal que viaja por un canal y está a lo largo de su viaje puede ser interferida por algún ruido o invasor si no se tienen los medios de seguridad correspondientes.

Teoría de sistemas: En esta teoría Von Bertalanffy (1976) sostiene que un sistema es la suma de todos los factores y puede estudiarse por partes, por otro lado, Norbert Wiener (1964), quien desarrolló la cibernética, la cual es una rama de la TGS que se centra en el control y la comunicación entre los sistemas, también luego de su análisis comparativo concluyo que todo ser, ya sea biológico, artificial o mecánico, puede definirse por la naturaleza de los intercambios de información que se sostenga con un ambiente, por consiguiente se refirió a que todos son entes informacionales. Entonces podemos decir que esta teoría también está relacionada estrechamente con la variable de seguridad de información, porque realizar intercambios de información de un sistema a otro, donde se presenta riesgo de vulnerabilidad en el transcurso de su envío.

Definición de Seguridad de la Información:

La Seguridad se refiere a tomar medidas adecuadas para reducir a un nivel aceptable los riesgos que plantean las amenazas y vulnerabilidades en el uso de la tecnología de la información. La seguridad de la información se refiere a la confidencialidad, integridad e integridad de la

información y la tecnología de la información basada en diversas medidas estandarizadas de acuerdo con un régimen o una norma (Fuentes Serrate, 2020).

Dimensiones sobre los pilares de la seguridad de la información:

Confidencialidad: Valencia (2021) nos define que, tiene que ver con el tema de los accesos y el uso de la información ya que solo el acceso es para la persona autorizada y tiene la necesidad de conocerla. La norma ISO 2700 define la confidencialidad como cuando la información no está disponible o revelada a personas, entidades o procesos no autorizados.

Disponibilidad: Valencia (2021) nos comenta que, los usuarios cuentan con autorización sólo cuando lo requieran para verificar la información o en todo caso verificar los activos tecnológicos. Es aquí en donde Cobit define que la información está disponible en el momento que se solicite para los procesos de la organización en cualquier momento.

Integridad: Valencia (2021) nos informa que, la integridad es la capacidad de proteger la precisión y la integridad de la información y los activos tecnológicos de la alteración o eliminación no autorizada. Cobit define la integridad como la precisión y llegada completa de la información, así como su veracidad. con respecto a los activos de valor de la organización y sus expectativas.

Evolución de la seguridad de la información

Diferentes aspectos a considerar en la evolución de la teoría de la seguridad de la información, que a continuación mencionaremos a los más resaltantes por su importancia: En 1990, La OTAN combina todas las ideas de seguridad de transmisión (TRANSEC), seguridad de redes (NETSEC) y seguridad de ordenadores (COMPUSEC) en un concepto importante para ellos llamado seguridad de información (INFOSEC), la cual tiene el principal objetivo de proteger la información en tres aspectos: confidencialidad, integridad y disponibilidad (Agustín, 2005).

Karyda, Kiountouzis y Kokolakis en 2004 analizaron e interpretaron las políticas de seguridad de los sistemas de información desde un punto de vista contextual. Cardenas et al. (2013), mientras tanto, en el 2005 fue publicada la primera versión de las normas ISO/IEC 27000: Los requisitos y las pautas para la gestión de la seguridad de la información se establecen en esta familia de normas (Duque, 2021). Asimismo, en el 2022 se publica la última versión de un sistema de seguridad de información ISO/IEC 27001: Este estándar global establece un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de seguridad de la información (SGSI). En resumen, diferentes autores interpretan la seguridad de la información, cada uno a su estilo y perspectiva. La norma ISO/IEC 27001 ha dado un auge con el paso del tiempo y su última versión publicada el 2022.

Características de la seguridad de la información:

Las características de la seguridad de la información son necesarias para que las empresas protejan sus sistemas de información.

Dimensiones:

- Confidencialidad:

La confidencialidad es toda información accesible solo para personal autorizado. Esta información no debe llegar a personas o entidades que no estén autorizados o que no tengan ningún tipo de relación con la empresa.

- Disponibilidad:

La disponibilidad nos indica que podemos tener acceso a la información cuando se requiera, teniendo en cuenta la privacidad. Así evitar las conocidas “caídas” del sistema las cuales permiten accesos ilegítimos a otros usuarios o servidores, lo que se debería de lograr es que impidan el acceso a servicios como un correo u otro servidor privado.

- Integridad:

La integridad es la información correcta sin modificaciones no autorizadas ni errores. Se protege frente a vulnerabilidades externas o algún posible error humano, dentro de ello podemos incluir el mal uso de los trabajadores o usuarios directos.

Indicadores:

- Nivel de cumplimiento de confidencialidad, se debe de verificar el estado actual de confidencialidad de la empresa y comparar con los resultados obtenidos de acuerdo con el ISO 27001.
- Nivel de cumplimiento de disponibilidad, se debe de verificar el estado actual de disponibilidad de la empresa y comparar con los resultados obtenidos de acuerdo con el ISO 27001.
- Nivel de cumplimiento de integridad, se debe de verificar el estado actual de integridad de la empresa y comparar con los resultados obtenidos de acuerdo con el ISO 27001.

2.3 Formulación de hipótesis

2.3.1 Hipótesis general

Hi: La implementación de la ISO 27001 mejora la seguridad de la información en una empresa tecnológica, Lima 2024.

2.3.2 Hipótesis específica

HE1: La implementación de la ISO 27001 mejora el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024.

HE2: La implementación de la ISO 27001 mejora el nivel de disponibilidad de la información en una empresa tecnológica, Lima 2024.

HE3: La implementación de la ISO 27001 mejora el nivel de integridad de la información en una empresa tecnológica, Lima 2024.

CAPÍTULO III: METODOLOGÍA

3.1 Método de la investigación

En el siguiente proyecto, se utilizó tres tipos de metodologías: i) analíticos, ii) hipotéticos y iii) deductivos. Asimismo, se formularon las hipótesis de investigación respectivas para comprender y obtener las conclusiones sobre las variables en estudio.

El método analítico es un método científico que consiste en dividir un fenómeno complejo en sus partes más simples para su estudio. (Rodriguez Calero, 2022) afirma que, este enfoque se emplea en ciencias naturales y sociales para obtener una mejor comprensión de la estructura y funcionamiento de los sistemas. Por ejemplo, en el estudio de la economía, el método analítico puede utilizarse para analizar las causas de una crisis económica o las consecuencias de una política en particular.

El método deductivo es un criterio científico, en el cual, se aplica una ley general a un caso específico. Según (López -lópez, 2023), este enfoque se emplea tanto en las ciencias naturales como en las sociales para crear hipótesis o predicciones. Por ejemplo, en el campo de la física, se puede utilizar el método deductivo para predecir el comportamiento de un objeto en función de sus propiedades.

El método hipotético-deductivo es un enfoque científico que comienza con la formulación de una hipótesis, la extracción de predicciones de ella y luego la prueba. El científico y filósofo Karl Popper propuso este enfoque en el siglo XX.

(Allan, 2008) sostiene que, el método hipotético-deductivo es el único que puede asegurar el progreso del conocimiento científico. Este enfoque se basa en la idea de que la ciencia solo

puede refutar una hipótesis en lugar de probar su veracidad. Como resultado, la ciencia avanza a través de la eliminación de hipótesis erróneas.

3.2 Enfoque de la investigación

En el proyecto, se empleó, un planteamiento cuantitativo para poder evaluar y aplicar los controles de seguridad según la norma ISO 27001, para si poder identificar y medir las variables que nos permitan cuantificar el estado de seguridad de la información en una institución, de la misma manera podemos decir que el enfoque cuantitativo es un método de investigación que prioriza la objetividad, la medición y la generalización al recopilar y analizar datos numéricos.

Ael (2015) en su estudio manifiesta que, el enfoque cuantitativo es "un método de investigación que utiliza la recolección de datos cuantitativos para probar hipótesis o responder preguntas de investigación". Que es utilizado en las ciencias sociales, como la psicología, la sociología, la economía y la política; algo similar, para (Creswell, 2022)), el enfoque cuantitativo, se basa en la recopilación de datos numéricos que se pueden analizar estadísticamente. Finalmente, Polit y Beck (202) indican que, en la parte del análisis cuantitativo, es un enfoque de investigación que maneja datos numéricos para describir, explicar o predecir un fenómeno. Este enfoque es útil para estudiar fenómenos complejos que se pueden dividir en partes más simples.

3.3 Tipo de investigación

En este estudio se utilizó el tipo de investigación aplicada, en la cual se emplean los conocimientos adquiridos en la práctica, para los beneficios de quienes participan en sus procesos, por ello, se dice que la instigación aplicada se enfoca en solucionar problemas prácticos de la vida real, en conclusión, esta investigación utiliza el método científico para crear conocimiento aplicable a soluciones de problemas de nuestra sociedad en el ámbito productivo (Murillo, 2008). La

investigación aplicada, también conocida como investigación práctica o empírica, se caracteriza por la implementación y sistematización de la investigación (Vargas, 2009).

3.4 Diseño de la investigación

En este proyecto se utilizó el diseño experimental de tipo pre-experimental, un método de investigación que se realiza con la manipulación deliberada de sus variables. Porque tiene un grupo experimental, donde se va a fraccionar para preprueba y la postprueba.

Estos se clasifican en dos, la primera es de forma transversal, la cual se encarga de recolectar datos en un momento, siendo exploratorios, descriptivos o correlacionales; la segunda es longitudinal esta se encarga de analizar el tiempo con el fin de relacionar variables conforme transcurre relacionándolo con las consecuencias y causas que puedan tener (Mata, 2019).

3.5 Población, muestra y muestreo

Población:

Según Condori (2020), indica que es el conjunto de elementos, en el cual se encuentran de manera accesible o también se puede decir que es la unidad de análisis a la que pertenece un ámbito especial del cual se desarrollará un estudio. Asimismo, la población es el universo que estudia cualquier tipo de investigación, sobre las conclusiones deseadas de los resultados, organizadas en función de rasgos o niveles que le permitan diferenciar a los sujetos unos de otros (Fuentes, 2020). Por lo tanto, las poblaciones son un grupo o conjunto de características comunes que tiene un objeto de estudio. A continuación, Organización Internacional de Normalizacion (ISO, 2013), en donde, se consideran 114 controles o eventos de riesgo, de ellos, solo se seleccionan 20 controles del Anexo A de los objetivos de control y controles de referencia de la ISO 27001 (kosutic, 2023).

Muestra:

En referencia al concepto de muestra se entiende que es la parte representativa de la población, que cuenta con las mismas características generales de la población Condori (2020). Según Deivi (2020), el investigador, selecciona una porción o subconjunto de la población como unidades o elementos para mejorar el estudio para obtener información representativa y confiable. Con respecto a las narrativas, Álvarez (2003) nos comenta que, la muestra es la que, valida, la representatividad de todo un universo y se manifiesta como un factor crucial para argumentar los resultados. Lo que podemos hacer referencia, es de que la muestra obtenida, debe contar con los parámetros del estudio realizado, y así, validar el estudio el cual va ser seleccionado. Asimismo, al efectuar el tamaño de la muestra es 20 eventos de riesgos con tipo de muestreo deliberado, las cuales se obtuvieron de acuerdo a la evaluación con los especialistas de ciberseguridad del área de TIC de la organización objeto de estudio, ya que, con las carencias o necesidades de la empresa se sostuvo mantener el análisis previo mediante las bases de ISO 27001, para ser observados en 15 días.

Muestreo:

Población es un grupo específico con características comunes o en todo caso se encuentran vinculados por uno o más factores como edad, etnia, región geográfica (Hernández & Mendoza, 2018). Por otro lado, con respecto al aporte, para este estudio se incluyen 20 controles de la norma ISO 27001, junto con guías de observación antes del proceso, durante el proceso y después del proceso en la mejora de la seguridad de la información. Estos 20 controles se tuvieron que emplear categorías para cada dimensión. En el caso de la dimensión de confidencialidad se contó con el control (A9), que se encarga de los accesos y sus permisos , en la parte de redes, registros y gestión

de accesos de los usuarios, por otro lado, la dimensión disponibilidad se relaciona con el control (A13) que ve el tema de seguridad en las comunicaciones y de gestión de políticas y procedimientos para el manejo de información, así también la dimensión integridad se identificaba con el control (A11) que nos muestra, la seguridad física y del entorno, considerando las amenazas externas, seguridad del perímetro manteniendo el áreas seguras .

El muestreo se basa solo en la selección de la población que se entrevistan en las situaciones que se van a observar y también en los lugares que sean posible obtener la participación de las personas y las diversas situaciones que se presenten (Uwe, 2015). En el caso de Fidias (1997) comenta que, el muestreo es un proceso en el que se sabe la posibilidad que cuenta cada elemento para integrar la muestra. En resumen, al tener 20 controles de seguridad como una muestra de 114 controles, estos se obtuvieron en el siguiente orden:

Sección: A9 Control de acceso

Control: 9.1.2 Acceso a las redes y a los servicios de red

1. Control de acceso con usuario y clave único, en base a roles para accesos diferenciados.

2. Procedimientos de autorización para el acceso a la red.

3. Control de los dispositivos por cual se accede a la red.

Control: 9.2.1 Registro de usuarios y cancelación del registro

4. Monitoreo de las actividades inusuales o intentos de acceso no autorizados de los usuarios.

5.Baja a las cuentas de usuario cuando el trabajador abandona la organización.

Control: 9.2.2 Gestión de acceso a los usuarios

6. Accesos que cumplen con la longitud > 8 a caracteres, incluyendo caracteres especiales, mayúsculas, minúsculas y números.

7. Accesos otorgados a los usuarios.

8. Roles de acceso a los usuarios para los permisos que sean necesarios.

Sección: A13 Seguridad en las comunicaciones

Control: 13.1.2 Seguridad de los servicios de red

9. Filtrado de paquetes para control del tráfico de red y prevenir ataques maliciosos.

10. Firewall certificado para la seguridad de la red.

Control: 13.2.1 Políticas y procedimientos de intercambio de información

11. Filtro para la transmisión de la información.

12. Mecanismo de encriptación para el intercambio de información.

13. Procedimientos para el respaldo de los datos.

Control: 13.2.2 Acuerdos de intercambio de información

14. Formatos certificados para el intercambio de información con el caso de boleta electrónica.

Sección: A13 Seguridad en las comunicaciones

Control: 13.1.2 Seguridad de los servicios de red

15. Reglas de filtrado de paquetes para control del tráfico de red y prevenir ataques maliciosos.

16. Firewall certificado para la seguridad de la red.

Control: 13.2.1 Políticas y procedimientos de intercambio de información

17. Filtro para la transmisión de la información.

18. Mecanismo de encriptación para el intercambio de información.

19. Procedimientos para el respaldo de los datos.

Control: 13.2.2 Acuerdos de intercambio de información

20. Formatos certificados para el intercambio de información con el caso de boleta electrónica.

3.6 Variables y operacionalización

Para el siguiente proyecto, se tomó en cuenta, las principales variables ISO 27001 y la Seguridad de la Información, como parte del estudio en una empresa de tecnología.

Variable independiente: ISO 27001

Definición conceptual: Estándares internacionales para establecer, implementar, mantener además de mejorar continuamente los sistemas de gestión de seguridad de la información utilizando procesos de gestión de riesgos para poder así proteger la confidencialidad, integridad y disponibilidad de la información en los diferentes controles que maneja, permitiendo a las empresas mantener protegida su información (Duque, 2021).

Definición operacional: Se trata los diferentes conceptos fundamentales de hardware y software, sobre todo en la interconexión de los sistemas, verificando todo tipo de controles de acceso, gestión de la seguridad y áreas seguras (Forouzan, 2012). En este caso se aborda cómo los ajustes en la configuración de redes y datos pueden influir en la protección y el desempeño general de la organización.

Variable dependiente: Seguridad de la Información

Definición Conceptual: La seguridad informática, también conocida como seguridad de redes o seguridad de tecnologías de la información, es la protección de los sistemas informáticos contra el robo o daño del hardware, software o información que contienen, y la interrupción o desvío de los servicios que prestan (Estrada, 2017).

Definición operacional: La seguridad de la información es la protección de la información de la confidencialidad, la integridad y la disponibilidad. cuyos indicadores miden las características de cada uno de estos tres pilares:

Para el caso de control de accesos de la norma ISO 27001, están abocados a controlar y monitorizar los accesos a la información de acuerdo a las políticas definidas por la empresa.

En la parte de seguridad de las comunicaciones de la norma ISO 27001, su orientación es básicamente en asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

En la sección de seguridad física y del entorno de la norma ISO 27001, se centra en la necesidad de identificar y crear medidas de control físicas para mantener seguros los activos de la información para evitar incidentes que afecten a la integridad de la información o interferencias no deseadas.

Operacionalización de variables:

Las matrices de resolución de variables, es la forma como se va poder definir de forma clara, la manera como se observa y se mide cada característica del estudio, dentro de ello se encuentran: objetivos generales, objetivos específicos, variables, dimensiones e indicadores. En esta investigación podemos encontrarlo en el anexo N°1.

3.7 Técnicas e instrumentos de recolección de datos

3.7.1 Técnica

Conjunto de procedimientos que nos permitirán establecer la relación que existe entre un objeto o sujeto de la investigación Hernández et al. (2006)- Por otro lado, el término "técnica" nos explica cómo los investigadores realizan las operaciones para obtener resultados que se ajusten al objeto

de la investigación. Su importancia radica en que son la garantía de la cientificidad Gómez (2020). por lo tanto, en este estudio se optó por utilizar como técnica la observación, en la cual veremos el comportamiento de los controles en base a un pre y post estudio, de acuerdo a los eventos a realizar.

3.7.2 Instrumentos

Es un mecanismo que usa el investigador para recolectar y registrar la información Falcón & Herrera (2005). Por otro lado, Miñan (2023), define que, son las herramientas o dispositivos empleados para recopilar datos de manera sistemática. Por lo tanto, en este estudio se optó por utilizar una ficha de observación como instrumento.

Según Medina Romero et al. (2023), la ficha de observación es un instrumento que se utiliza para poder organizar información de resultados de una investigación, hecho o algún acontecimiento personal, para esta ficha el investigador debe de trasladarse al lugar de los eventos.

En el proyecto se coordinó con la empresa para realizar una simulación de prueba para la validación del instrumento, para ello se decidió tomar como referencia 10 días antes de lo programado para la ejecución de la ficha de observación; es así que, con este periodo de simulación logramos validar el instrumento tal como queremos mostrar a la empresa.

3.7.3 Validación

Para la validación de los instrumentos, se utiliza el juicio de cuatro expertos para poder incrementar el nivel de confiabilidad, según diversos autores la validez de contenido es un componente importante en la evaluación de estas, así también se debe de tener en cuenta la validez de las inferencias extraídas de los resultados de las pruebas (Ding & Hershberger, 2013).

En ese sentido, se hizo participe a expertos para la validación.

Tabla 1

Relación de expertos validadores del instrumento

Item	Apellidos y nombres	Grado	Puntuación de V de Aiken
1	Walter Chávez. Alvarado	Magíster	1.00
2	Arones Pérez, Paolo Paulino	Magíster	1.00
3	Menacho Navarrete Karen	Magister	1.00
4	Cáceres Trigoso, Jorge Ernesto	Magister	1.00

Resultados: En nuestra investigación al realizar nuestra validación del instrumento podemos comentar, que, en la aplicación de V de Aiken(detallado en el Anexo N°4), donde participaron (n= 4) validadores, también se realizó (S=sumatoria total de la puntuación de expertos), obteniendo como resultado la unidad dentro de una valoración dicotómica (Si, No) lo cual, teniendo en cuenta que (Si= cumple y No= no cumple), por tanto, en el resultado final de V de Aiken se obtuvo una validez total del 100%.

3.7.4 Confiabilidad del instrumento

Mediante un instrumento que produce resultados consistentes y coherentes (Hidalgo, 2005). En tal sentido, la confiabilidad depende de procesos de observación para poder detallar minuciosamente lo que está ocurriendo en un contexto determinado, teniendo en cuenta ello, la confiabilidad trabaja con el pre test y post test los cuales miden la consistencia de los resultados, administrando la misma prueba a la misma muestra en diferentes momentos. Esto nos garantiza que los resultados de una prueba puedan reproducirse en las mismas condiciones a lo largo del tiempo. Una correlación de al menos 0,70 o más normalmente indica una buena confiabilidad (Ied Lote, 2024).

Se revisó el instrumento con los registros apropiados para llevar a cabo la correlación de Pearson, en base a ello, se crearon tablas de verificación previa para mostrar la confiabilidad de nuestro instrumento; los resultados entre los ensayos previos y posteriores se realizaron del 13/11/2023 al 24/12/2023 se muestran en el Anexo 3.

Tabla 2

Correlaciones de Pearson Pre Test y Post Test

Correlaciones			
		Pre-Test	**Post Test**
Pre-Test	**Correlación de Pearson**	1	0.791
	Sig. (bilateral)		0.1
	N	5	5
Post Test	**Correlación de Pearson**	0.791	1
	Sig. (bilateral)	0.1	
	N	5	5

En la tabla 2, se presenta que la correlación de Pearson es de 0,791 lo cual nos indica que tiene una correlación significativa entre los valores del Pre-test y Post-Test alta. En ese sentido, se confirma que el instrumento es confiable, ya que supera el 0.70. Teniendo una correlación positiva considerable, indicando que cuando las incidencias aumentan en el test, también tiende a elevar las incidencias en el retest.

3.8 Plan de procesamiento y análisis de datos

Para la siguiente investigación se empleó un planteamiento cuantitativo, en cuanto, al diseño no experimental como parte del tratamiento de datos. Se utilizó la ficha de observación basada en la seguridad de información y la “ISO 27001”. Para el procesamiento de datos se utilizó el aplicativo

llamado SPSS, el cual es popular entre los usuarios de Windows por la captura y análisis de datos para crear tablas y gráficos complejos. Asimismo, permite importar o ingresar manualmente datos de hojas de cálculo, archivos de texto u otros tipos de archivos, esto se diferencia de la hoja de cálculo más común en que el análisis se realiza con comandos en menús desplegables en lugar de en la hoja de cálculo.

3.9 Aspectos éticos

En este estudio, se garantiza la confidencialidad de la información proporcionada por la empresa por razones éticas y profesionales. Se siguen los procedimientos adecuados para asegurar un proceso transparente. Asimismo, se asegura la imparcialidad y la integridad de la información sin realizar ninguna manipulación. La ficha de observación utilizada será exclusiva para la empresa objeto de estudio, manteniendo la confidencialidad de los datos recopilados. Se aplicará la técnica de observación y se seguirá el formato APA 7 para la redacción, cumpliendo con los estándares requeridos, como se detalla en el anexo 5.

CAPÍTULO IV: RESULTADOS

4.1 Resultados

La presente investigación de diseño experimental con nivel pre experimental, examinó los riesgos de seguridad de la información y los controles de la ISO 27001. Los datos se recopilaron en las fichas de observación, con el apoyo de los encargados de la empresa en la cual se realiza el estudio.

4.1.1. Análisis descriptivo de resultados

En este apartado, se empleó como gestor del análisis estadístico, teniendo en cuenta, los datos de los 3 indicadores que se presentan en el objetivo principal, los cuales resultaron al emplear el programa: SPSS v.25. Tal como podemos apreciar en la tabla 3.

Tabla 3

Procesamiento datos

Estadísticos							
		PROM_PRECON	PROM_POSTCON	PROM PREDIS	PROM_POSTDIS	PROM_PREINTE	PROM_POSTINTE
N	Válido	15	15	15	15	15	15
	Perdidos	0	0	0	0	0	0
Media		**0,55**	**0,15**	**0,71**	**0,44**	**0,74**	**0,44**
Moda		0,50	0,13	0,67	,17[a]	0,67	,17[a]
Desv. Desviación		0,15	0,15	0,25	0,27	0,24	0,27
Varianza		0,02	0,02	0,06	0,07	0,06	0,07
Suma		8,25	2,38	10,67	6,67	11,17	6,67

En la tabla 4 se demostró que la valoración de los hechos que influye en la confidencialidad entre la media como dato estadístico del pre-test y la media estadística del post-test existe una diferencia del 40 %. Considerando que la valoración de los hechos para el

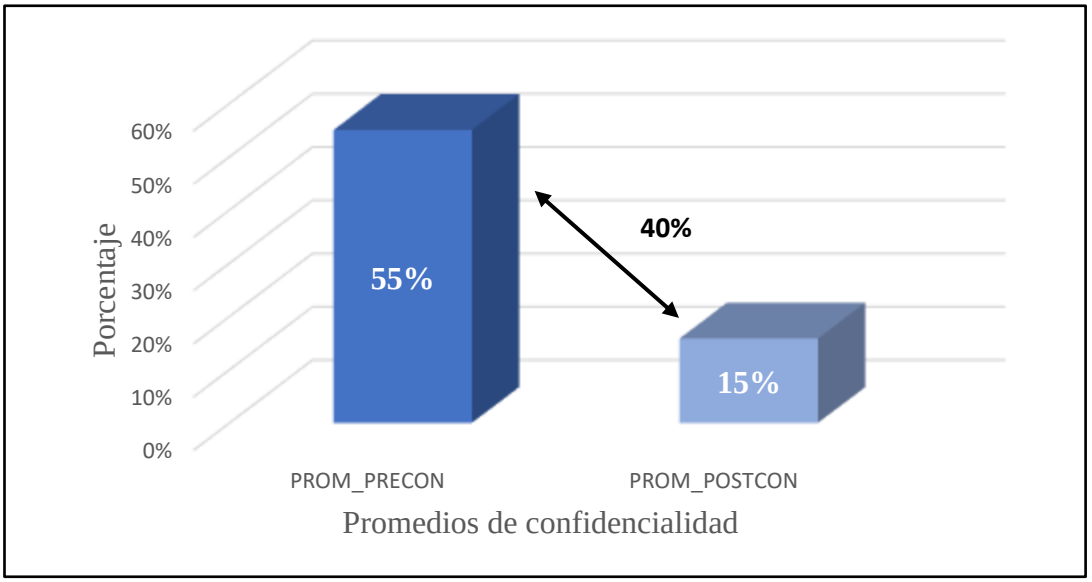
pre-test es del 55%, mientras que la valoración de los hechos para el post-test es del 15%. estos datos los apreciamos en el porcentaje acumulado de cada prueba.

Tabla 4

Comprobación de incidente que afectan la confidencialidad

		PROM_PRECON	PROM_POSTCON
N	Válido	15	15
Media		**0,55**	**0,15**
Desv. Desviación		0,15	0,15
Mínimo		0,38	0,00
Máximo		0,75	0,50
Suma		8,25	2,38

Figura 1 **Tasa de incidentes que afectan la confidencialidad**



En el caso de la tabla 5 se demostró la valoración de los hechos que influyen en la disponibilidad entre la media como dato estadístico del pretest y la media estadística del post-test

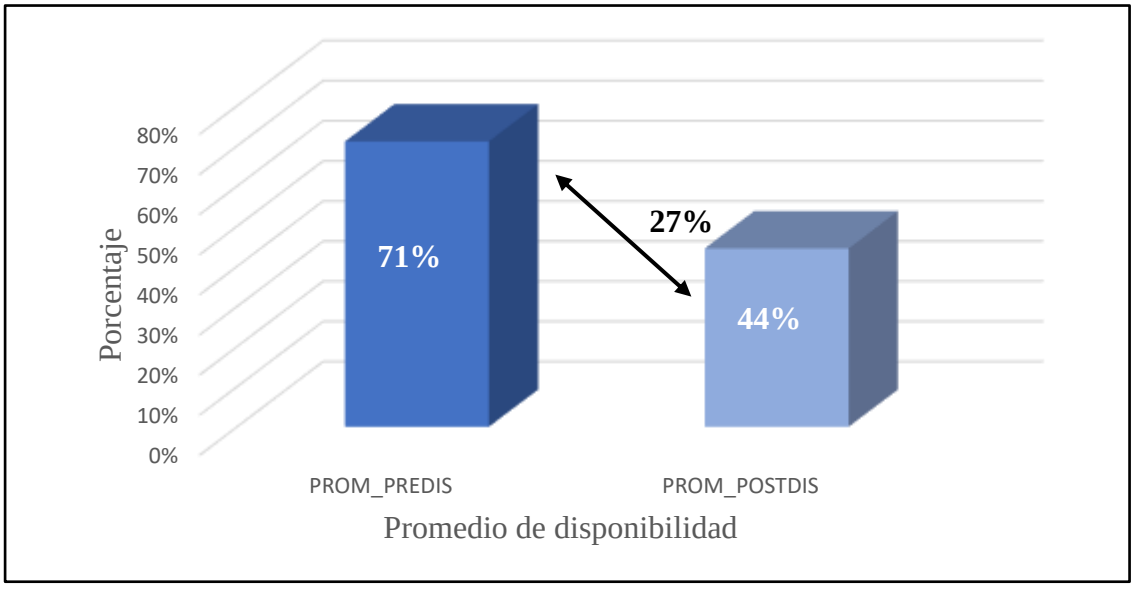
existe una diferencia del 27 %. Considerando que la valoración de los hechos para el pre-test es del 71%, mientras que la valoración de los hechos para el post-test es del 44%. estos datos los apreciamos en el porcentaje acumulado de cada prueba.

Tabla 5

Comprobación de incidente que afectan la disponibilidad

		PROM PREDIS	PROM_POSTDIS
N	Válido	15	15
Media		**0,71**	**0,44**
Desv. Desviación		0,25	0,27
Mínimo		0,00	0,17
Máximo		1,00	1,00
Suma		10,67	6,67

Figura 2 Tasa de incidentes que afectan la disponibilidad



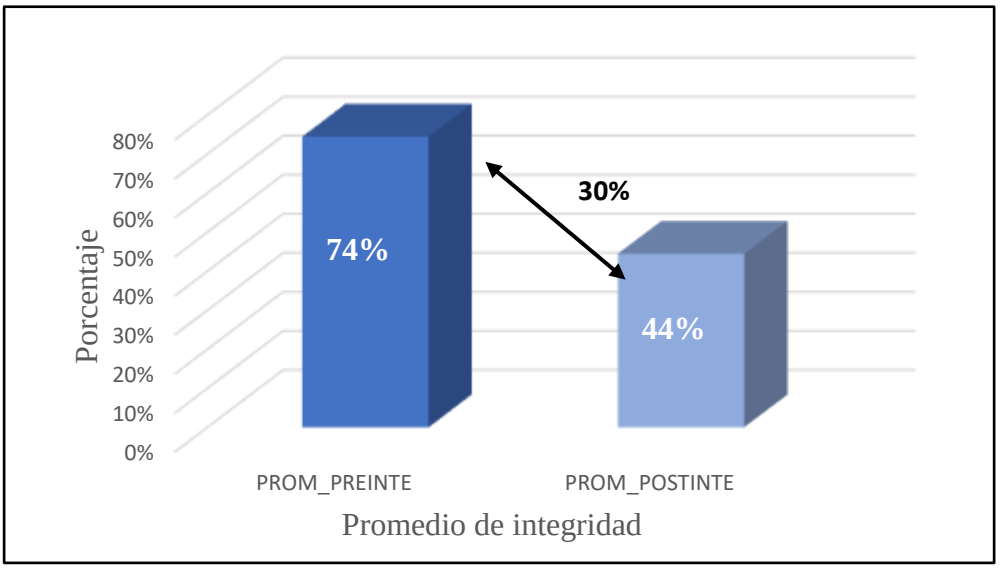
Para la tabla 6 se demostró que la valoración de los hechos que influyen en la disponibilidad entre la media como dato estadístico del pretest y la media estadística del post-test existe una diferencia del 30 %. Por lo tanto, Considerando que la valoración de los hechos para el pre-test es del 74%, mientras que la valoración de los hechos para el post-test es del 44%. estos datos los apreciamos en el porcentaje acumulado de cada prueba.

Tabla 6

Comprobación de incidente que afectan la integridad

		PROM_PREINTE	PROM_POSTINTE
N	Válido	15	15
Media		**0,74**	**0,44**
Desv. Desviación		0,24	0,27
Mínimo		0,00	0,17
Máximo		1,00	1,00
Suma		11,17	6,67

Figura 3 Tasa de incidentes que afectan la integridad



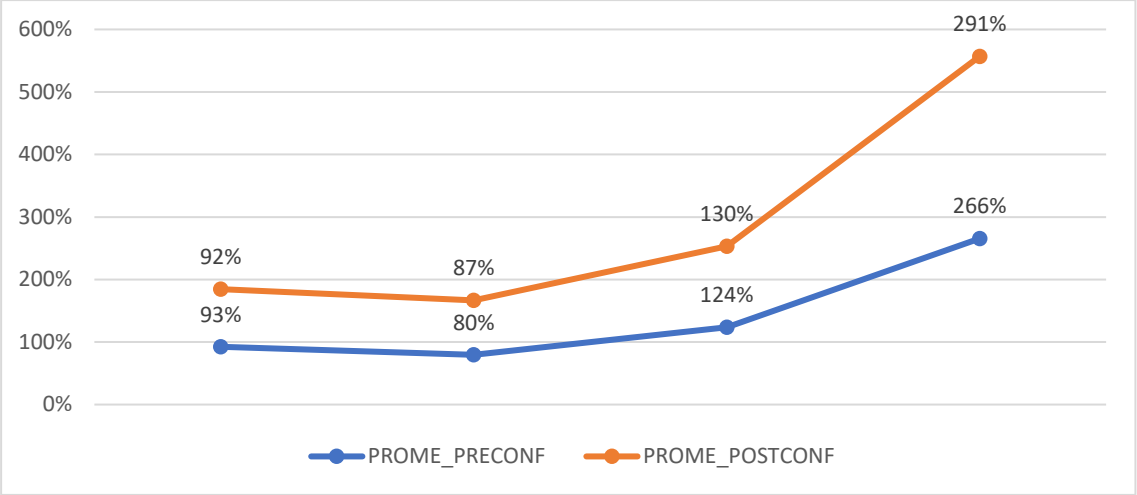
4.1.2. Prueba de Hipótesis

Según Arteaga (2020) en el caso de la prueba de hipótesis el proceso se basa en la evidencia encontrada en una muestra y el empleo de la teoría de la probabilidad para definir si es una hipótesis verdadera. En nuestro caso, consiste en la toma de decisiones en base a una evaluación de afirmaciones o suposiciones sobre una muestra de datos, en una población determinada, y poder determinar si existe suficiente evidencia en los datos de la muestra para rechazar o no dicha hipótesis.

Hipótesis 1 (HE1): La implementación de la ISO 27001 mejora el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024.

Según Peña (2017) se indica que es un proceso fundamental en la estadística que permite evaluar afirmaciones sobre parámetros poblacionales basándose en datos de una muestra; en este caso se realizara la prueba de hipótesis para comparar 20 controles de la muestra; de los que tomaremos 6 que corresponden a Confiabilidad de la información. Siendo estos monitoreados en 15 días.

Figura 4 Análisis de consistencia de datos Hipótesis 1



La figura 4 se muestra como la recolección de los datos y la validación de los hechos de la muestra en el rango de tiempo estimado varían en porcentajes acumulados de las pruebas hechas entre la comparación del pre y post-test de la confidencialidad, Es decir, una línea curva indica que los datos son consistentes y confiables.

Tabla 7

Consistencia de Pre y Post confidencialidad

Estadísticas de confidencialidad			
	Media	Desviación	N
PROME_PRECONF	0.55	0.15	15
PROME_POSTCONF	0.16	0.15	15

Alfa de Cronbach de Pre y Post	0,71	0,78	2

Como se refleja en la tabla 7 la confiabilidad tiene una consistencia interna de 77% encontrándose en un nivel bueno, de acuerdo con el cuadro de rangos Alfa de Cronbach, donde nos indica que el valor $0.7 \leq \alpha < 0.8$, es aceptable, sabiendo que este es un valor de referencia desde el nivel 0.7 y superiores, los ítems son suficientemente consistentes para indicar que la medida es confiable.

B. Prueba de Normalidad

Se decidió utilizar la evaluación de "Shapiro-Wilk", ya que, se obtuvo valores por debajo a 30 ítems, en comparación con la prueba de Kolmogórov-Smirnov que requiere valores superiores a 50 ítems por ello, se va a resolver si los valores obtenidos son paramétricos o no según su valor de significancia.

En la tabla 8 podemos validar que la confidencialidad, la disponibilidad y la integridad tanto en su pre-test y post-test, muestran resultados no paramétricos, conforme, al criterio estadístico empleado, como es, “Shapiro-Wilk”. La cual muestra los valores de Significancia. menores a 0,05.

Tabla 8

Consolidado de normalidad confidencialidad

Pruebas de normalidad			
		Shapiro-Wilk	
	Estadístico	Gl	Sig.
PROM_PRECON	0,84	15	0,015

PROM_POSTCON	0,87	15	0,035

En esta tabla 8 podemos ver que el valor de confidencialidad tanto en pre con 0.015 y post con 0.035 tienen un valor menor de significancia, en este caso menor al valor de 0.05, por consiguiente, es No Paramétrica

C. Contraste o prueba de hipótesis

En el análisis de contraste de la hipótesis, se observa que HE0: "La implementación de la ISO 27001 no mejora el nivel de confidencialidad en la seguridad de la información en una empresa tecnológica, Lima 2024". Del mismo modo, La HE1: "La implementación de la ISO 27001 mejora el nivel de confidencialidad en la seguridad de la información en una empresa tecnológica, Lima 2024". De tal modo, con la prueba de Wilcoxon se logró obtener un valor de "Sig." que no supera 0.05, en la validación de los hechos que influye en la confidencialidad, por lo tanto, en la ISO 27001 de acuerdo a sus controles, aumentan la confidencialidad de la información de la empresa tecnológica, Lima 2024, anulando la hipótesis.

Tabla 9

Prueba de rangos de Wilcoxon de confidencialidad

Rangos				
		N	Rango promedio	Suma de rangos
PROME POSTCONF - PROME_PRECONF	Rangos negativos	14[a]	8,32	116,50
	Rangos positivos	1[b]	3,50	3,50
	Empates	0[c]		

Total	15

a. PROME POSTCONF < PROME_PRECONF
b. PROME POSTCONF > PROME_PRECONF
c. PROME POSTCONF = PROME_PRECONF

En la tabla 9 encontramos dos rangos promedios negativos al tener valores de 8.32 y 3.50 con una categoría negativa de 14a escogiendo la opción “a". PROME POSTCONF < PROME_PRECONF” de acuerdo a los rangos promedios encontrados.

Tabla 10

Estadísticas de incidentes que impacta la confidencialidad

Estadísticos de prueba	
	PROME POSTCONF - PROME_PRECONF
Z	-3,246[b]
Sig. asintótica(bilateral)	0,001

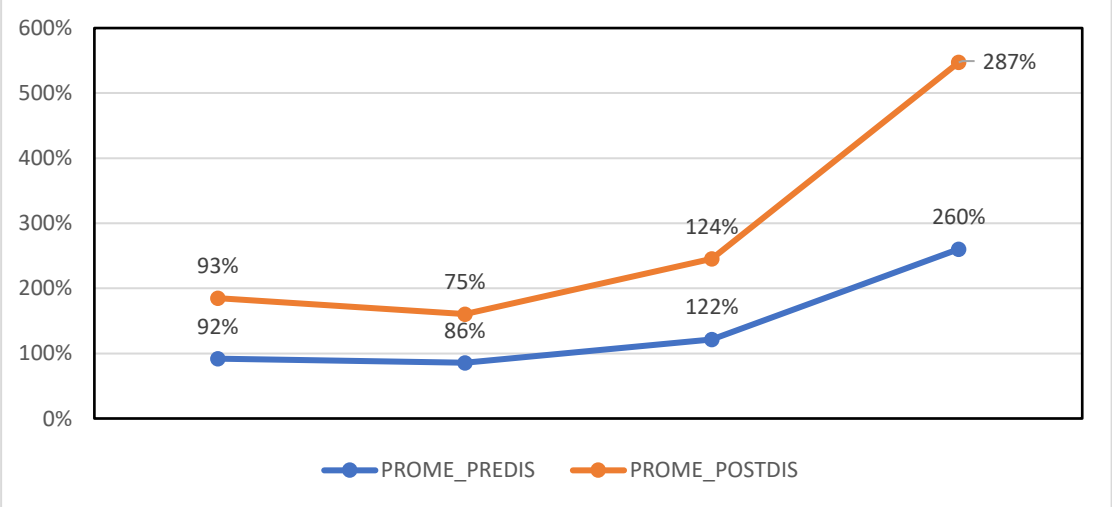
a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

En tabla 10 refleja una significancia bilateral de 0.001 cuyo valor es menos a 0.05, para la valoración de los hechos que influyen en la confidencialidad, de esta manera, se aprobaron los controles de la ISO 27001, los cuales, aumentan la confidencialidad de la información, en una empresa tecnológica 2024, donde se rechaza la hipótesis nula y se acepta la hipótesis 1 (HE1).

Hipótesis 2 (HE2): La implementación de la ISO 27001 mejora el nivel de disponibilidad de la información en una empresa tecnológica, Lima 2024.

Peña (2017) indica que es un proceso fundamental en la estadística que permite evaluar afirmaciones sobre parámetros poblacionales basándose en datos de una muestra; en este caso se realizara la prueba de hipótesis para comparar de los 114 controles los 20 de muestra; de los que tomaremos 6 que corresponden a Disponibilidad de la información. Siendo estos monitoreados en 15 días.

Figura 5 Análisis de consistencia de datos Hipótesis 2



La figura 5 se muestra como la recolección de los datos y la validación de los hechos de la muestra en el rango de tiempo estimado varían en porcentajes acumulados de las pruebas echas

entre la comparación del pre y post-test de la confidencialidad, Es decir, una línea curva indica que los datos son consistentes y confiables.

Tabla 11

Consistencia de Pre y Post disponibilidad

Estadísticas de disponibilidad			
	Media	Desviación	N
PROME_PREDIS	0,71	0,25	15
PROME_POSTDIS	0,44	0,27	15
Alfa de Cronbach de Pre y Post	0,73	0,73	2

Como se refleja en la tabla 11 la disponibilidad tiene una consistencia interna de 73% encontrándose en un nivel bueno, de acuerdo con el cuadro de rangos Alfa de Cronbach, donde nos indica que el valor $0.7 \leq \alpha < 0.8$, es aceptable, sabiendo que este es un valor de referencia desde el nivel 0.7 y superiores, los ítems son suficientemente consistentes para indicar que la medida es confiable.

B. Prueba de normalidad

Se decidió utilizar la evaluación de "Shapiro-Wilk", ya que, se obtuvo valores por debajo a 30 ítems, en comparación con la prueba de Kolmogórov-Smirnov que requiere valores superiores a 50 ítems por ello, se va a resolver si los valores obtenidos son paramétricos o no según su valor de significancia.

En la tabla 11 podemos validar que la confidencialidad, la disponibilidad y la integridad tanto en su pre-test y post-test, muestran resultados no paramétricos, conforme, al criterio estadístico empleado, como es, “Shapiro-Wilk”. La cual muestra los valores de Significancia. menores a 0,05.

Tabla 12

Consolidado de normalidad de disponibilidad

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	Gl	Sig.
PROM PREDIS	0,848	15	0,016
PROM_POSTDIS	0,846	15	0,015

En esta tabla 12 podemos ver que el valor de confidencialidad tanto en pre con 0.016 y post con 0.015 tienen un valor menor de significancia, en este caso menor al valor de 0.05. por consiguiente, corresponde una prueba No Paramétrica.

C. Contraste o prueba de hipótesis

Tabla 13

Prueba de rangos de Wilcoxon de disponibilidad

Rangos				
		N	Rango promedio	Suma de rangos
PROME_POSTDIS - PROME_PREDIS	Rangos negativos	12[a]	7,29	87,50
	Rangos positivos	1[b]	3,50	3,50
	Empates	2[c]		
	Total	15		

a. PROME_POSTDIS < PROME_PREDIS
b. PROME_POSTDIS > PROME_PREDIS
c. PROME_POSTDIS = PROME_PREDIS

En la tabla 13 encontramos dos rangos promedios negativos al tener valores de 7.29 y 3.50 con una categoría negativa de 12a escogiendo la opción “a". PROME_POSTDIS < PROME PREDIOS” de acuerdo a los rangos promedios encontrados.

Tabla 14

Estadísticas de incidentes que impacta la disponibilidad

Estadísticos de prueba	
	PROME_POSTDIS - PROME_PREDIS
Z	-2,973[b]
Sig. asintótica(bilateral)	0,003

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

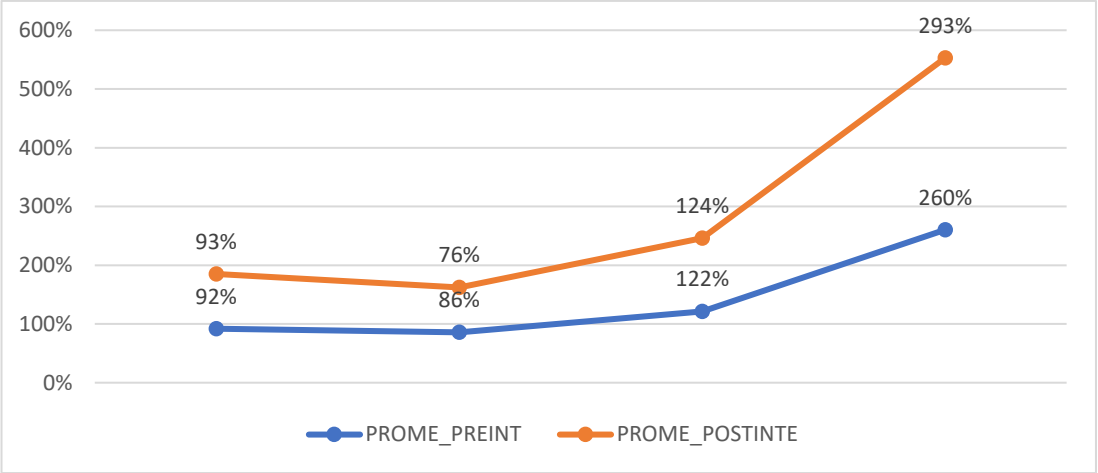
La tabla 14 muestra una significancia bilateral de 0.001 cuyo valor es menos a 0.05, para la valoración de los hechos que influyen en la disponibilidad, de tal manera, se aprueban los controles de la ISO 27001, los cuales, aumentan la disponibilidad de la información, en una empresa tecnológica 2024, donde se rechaza la hipótesis nula y se acepta la hipótesis 2.

Hipótesis 3 (HE3): La implementación de la ISO 27001 mejora el nivel de integridad de la información en una empresa tecnológica, Lima 2024.

Peña (2017) indica que es un proceso fundamental en la estadística que permite evaluar afirmaciones sobre parámetros poblacionales basándose en datos de una muestra; en este caso se realizara la prueba de hipótesis para comparar de los 114 controles los 20 de muestra; de los que

tomaremos 6 que corresponden a Integridad de la información. Siendo estos monitoreados en 15 días.

Figura 6 Análisis de consistencia de datos Hipótesis 3



La figura 6 se muestra como la recolección de los datos y la validación de los hechos de la muestra en el rango de tiempo estimado varían en porcentajes acumulados de las pruebas echas entre la comparación del pre y post-test de la confidencialidad, Es decir, una línea curva indica que los datos son consistentes y confiables.

Tabla 15

Consistencia de Pre y Post integridad

Estadísticas de integridad			
	Media	Desviación	N
PROME_PREINT	0,71	0,25	15
PROME_POSTINTE	0,38	0,26	15
Alfa de Cronbach de Pre y Post	0,70	0,71	2

Como se refleja en la tabla 15 la integridad tiene una consistencia interna de 70% encontrándose en un nivel bueno. Como se refleja en la tabla 6 la confiabilidad tiene una consistencia interna de 77% encontrándose en un nivel bueno, de acuerdo con el cuadro de rangos Alfa de Cronbach, donde nos indica que el valor $0.7 \leq \alpha < 0.8$, es aceptable, sabiendo que este es un valor de referencia desde el nivel 0.7 y superiores, los ítems son suficientemente consistentes para indicar que la medida es confiable. Por consiguiente, corresponde una prueba No Paramétrica.

B. Prueba de normalidad

Se decidió utilizar la evaluación de "Shapiro-Wilk", ya que, se obtuvo valores por debajo a 30 ítems, en comparación con la prueba de Kolmogórov-Smirnov que requiere valores superiores a 50 ítems por ello, se va a resolver si los valores obtenidos son paramétricos o no según su valor de significancia.

En la tabla 15 podemos validar que la confidencialidad, la disponibilidad y la integridad tanto en su pre-test y post-test, muestran resultados no paramétricos, conforme, al criterio estadístico empleado, como es, “Shapiro-Wilk”. La cual muestra los valores de Significancia. menores a 0,05.

Tabla 16

Consolidado de normalidad de integridad

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	Gl	Sig.
PROM_PREINTE	0,74	15	0,001
PROM_POSTINTE	0,85	15	0,015

En esta tabla 16 podemos ver que el valor de confidencialidad tanto en pre con 0.001 y post con 0.015 tienen un valor menor de significancia, en este caso menor al valor de 0.05.

C. Contraste o prueba de hipótesis

Hipótesis 3

Tabla 17

Prueba de rangos de Wilcoxon de integridad

Rangos				
		N	Rango promedio	Suma de rangos
PROME_POSTINTE - PROME_PREINT	Rangos negativos	12[a]	7,42	89,00
	Rangos positivos	1[b]	2,00	2,00
	Empates	2[c]		
	Total	15		

a. PROME_POSTINTE < PROME_PREINT
b. PROME_POSTINTE > PROME_PREINT
c. PROME_POSTINTE = PROME_PREINT

En la tabla 17 encontramos dos rangos promedios negativos al tener valores de 7.42 y 2.00 con una categoría negativa de 12a escogiendo la opción “a". PROME_POSTINTE < PROME_PREINT” de acuerdo a los rangos promedios encontrados.

Tabla 18

Estadísticas de incidentes que impacta la integridad

Estadísticos de prueba	
	PROME_POSTINTE - PROME_PREINT
Z	-3,081[b]
Sig. asintótica(bilateral)	0,002

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

En la tabla 18 refleja una significancia bilateral de 0.001 cuyo valor es menos a 0.05, para la valoración de los hechos que influyen en la integridad, de tal manera, se aprueban los controles de la ISO 27001, los cuales, aumentan la integridad de la información, en una empresa tecnológica 2024, donde se rechaza la hipótesis nula y se acepta la hipótesis 3.

4.2 Discusiones

Respecto a lo demostrado en los fundamentos teóricos y los antecedentes del estudio, se hace referencia a lo evidenciado en los antecedentes del mismo, el cual consistió. en “demostrar la implementación de la ISO 27001 para mejorar la seguridad de la información en una empresa tecnológica, Lima 2024”. En las referencias estadísticas de la variable dependiente, se observó

una reducción del post-test del 40% en la confidencialidad, del 27% en la disponibilidad y del 30% en la integridad durante el análisis de los eventos de riesgo presentados por la empresa tecnológica. Además, podemos referenciar con la estadística inferencial que, se comprueba que la confidencialidad, la disponibilidad y la integridad tanto en su pre-test y post-test, toleran valores no paramétricos tal cual que la prueba estadística de "Shapiro-Wilk". La cual muestra los valores de Significancia menores a 0,05. Por lo tanto, las soluciones obtenidas, coinciden parcialmente con la contribución de Asqui y Torres (2023) quien realizó un proyecto que tuvo la finalidad, de cómo ISO 27001 aumenta la confianza, disponibilidad y la integridad de la información en una organización. En el caso del promedio de la media del pre-test que afectan la confidencialidad existe la diferencia del 40% lo que se refleja en los porcentajes acumulados en un pre-test 55% de no contar con los controles en los perfiles de los usuarios en cuestión, en cambio, en el post-test muestra una disminución de este problema a un 15%. Al realizar el promedio de la media del pre-test de la disponibilidad mostraba un 71% de posibles filtraciones de información, lo cual, cambio en el post-test esto bajo a un 44%. Y cuando verificamos el pre-test de la integridad del sistema de seguridad, presento un 74% de no contar con firewall especifico, por lo tanto, eso cambio al realizar un post-test, en el cual, nos indica un 44%. Es decir que con la mejora de la seguridad de la información con la norma ISO 2701 permite disminuir los eventos de riesgo que se puedan presentar según los controles analizados. Medina (2023) nos habló de la técnica de recolección de datos la cual nos ayuda a tener resultados confiables y de cómo se descubre que la ISO 27001 aumenta la seguridad de la comunicación.

En el estudio que a continuación se trata, se tiene como objetivo específico 1, Determinar en qué medida la implementación de la ISO 27001 mejora el nivel de confidencialidad en la seguridad de la información en una empresa tecnológica, Lima 2024. Se logra identificar el

resultado descriptivo que se presenta en este proyecto, donde señalamos que, en la valoración de los hechos, que influyen en la confidencialidad entre la media como dato estadístico del pretest y la media estadística del post-test existe un resto del 40%. De tal modo, en la validación de los hechos para el pre-test es del 55%, mientras que, para el post-test es del 15%. También, se realizó la prueba de wilcoxon, donde se obtuvo un valor de "Sig.", inferior que 0.05 en la valoración de los hechos que influyen en la confidencialidad al rechazar hipótesis nula, por lo tanto, se aprueban los controles de la ISO 27001 que aumentan la confidencialidad de la información, en una empresa tecnológica 2024. Aplicando los controles evidenciamos que hay una reducción del 40% al índice de incidentes que afectan a la confidencialidad. Por consiguiente, se asemeja con el aporte de (Aleman, 2023) que tuvo como objetivo "establecer en qué medida afecta la implementación de la norma ISO 27001 en el control de la seguridad de la informática en una consultoría particular". Los resultados del análisis descriptivo confirmaron que el pre-test tuvo un valor promedio de 2% mientras que el post-test tuvo un valor promedio de 1%. También hubo un valor de significancia entre los dos valores. es de 0.00($p<0.05$). Se encontró que la evidencia de la implementación de la norma ISO 27001 mejoró la protección de la información de las consultoras privadas. Además, gracias a la implementación de la norma la organización se encuentra protegida acorde con las exigencias del mercado. En concreto al evaluar los eventos de riesgos mediante la norma de la ISO y sus Controles se logra aumentar la seguridad de la información y tener la confianza de nuestros colaboradores y clientes. Y por último teniendo el aporte de (Pequeño, 2015) quien afirma que la norma principal de la familia SGSI, en la cual, se describe cómo establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI. Con esta norma se certificarán las organizaciones que deseen certificar sus Sistemas de Gestión de Seguridad de la Información.

El presente estudio tiene como objetivo específico 2 “Determinar en qué medida la implementación de la ISO 27001 mejora el nivel de disponibilidad en la seguridad de la información en una empresa tecnológica, Lima 2024”. Donde se alcanzó reconocer el resultado descriptivo que viene aconteciendo en este estudio, en donde se demostró que, la valoración de los hechos que influyen en la disponibilidad entre la media como dato estadístico del pretest y la media estadística del post-test existe una diferencia del 27 %. Por lo tanto, la valoración de los hechos para el pre-test es del 71%, mientras que la valoración de los hechos para el post-test es del 44%, estos datos los apreciamos en el porcentaje acumulado de cada prueba. De tal modo que, para la estadística inferencial se determinó que, el promedio de los dos valores de los hechos de disponibilidad es relevante, con un promedio del 71 % en el pretest y un promedio del 44 % en el post-test. Además, se realizó la prueba de wilcoxon en donde se obtuvo un valor de "Sig." inferior que 0.05 en la valoración de los hechos que afectan la disponibilidad, en donde se rechaza la hipótesis nula y se admite que los controles de la ISO 27001 optimizan la disponibilidad de la data en una empresa tecnológica 2024 rechazando la hipótesis nula. Por lo tanto, se asemeja con el aporte de (Medina, 2023) que tuvo como objetivo: “Encontrar de qué forma el ISO 27001 afecta en la gestión de la seguridad de la información en el área de TI en una industria”. La técnica de recolección de datos utilizada fue la encuesta y su instrumento fue el cuestionario. Se descubrió que la ISO 27001 aumentó la seguridad de la comunicación, la criptografía y el manejo de activos en un 30 % y la eficacia de las gestiones operativas de los sistemas en un 27 %., de tal forma se reflejó por medio de una $p<0.05$. Se descubrió que la métrica ISO 27001 tiene un impacto significativo en la seguridad de la información en el sector de TI. Demostrando cambios significativos en la gestión de procesos de la organización. En el aporte de Carreño (2024), quien

basa su investigación en Establecer las garantías de los tres pilares: confidencialidad, integridad y disponibilidad la cual con el instrumento se demuestra que es necesario construir el área de seguridad de la información con políticas de seguridad para los estándares de la empresa.

En este estudio tiene como objetivo específico 3 “Determinar en qué medida la implementación de la ISO 27001 mejora el nivel de integridad en la seguridad de la información en una empresa tecnológica, Lima 2024”. Se ha presentado un hallazgo descriptivo en el estudio, el cual indica que la diferencia en la valoración de los hechos que impactan en la integridad entre la media como dato estadístico del pretest y la media del post-test es del 30%. En el pretest, la tasa de incidentes fue del 74%, mientras que en el post-test fue del 44%. Además, para la estadística inferencial se determinó que, la media de las dos tasas de los hechos de integridad es notable, con un promedio del 74 % en el pre-test y un promedio del 44 % en el post-test. Además, se realizó wilcoxon, donde el valor de "Sig.", estuvo por debajo de 0.05 en la valoración de los hechos que influyen en la integridad, como resultado no se anula la hipótesis , y se considera, que, en el caso, de la integridad de la ISO 27001, mejoran la información en una empresa tecnológica 2024 rechazando la hipótesis nula. De manera similar, se contrasta con la contribución de Moron (2023), cuyo propósito era desarrollar un Sistema de Seguridad de la Información para una empresa privada alineado con los nuevos estándares internacionales de tecnologías de la información. En su investigación, se empleó una ficha técnica como documento de respaldo. Los resultados revelaron que el promedio del análisis inicial fue del 69.90%, mientras que el promedio del análisis posterior fue del 14.00%. A pesar de que el valor más bajo en la fase previa fue del 50% y el más alto del 88%, en la etapa posterior los valores oscilaron entre 0% y 27%. Respecto a la significancia, se obtuvo un nivel de 0.265 en la evaluación inicial y de 0.108 en la evaluación posterior. Determinando si el indicador es compatible con una

distribución normal paramétrica (P > 0.05). Cuando una empresa identifica deficiencias, es crucial realizar una evaluación de riesgos utilizando los controles proporcionados por la norma ISO 27001 para mejorar la seguridad de su información, que es el objetivo fundamental de cualquier norma. Con la implementación de nuevos estándares, las organizaciones pueden alcanzar un alto nivel de seguridad de la información. Según (De la Rosa, 2021), al fortalecer los fundamentos de la seguridad de la información, se reduce el riesgo de fraude, pérdida e incluso filtración de datos. La norma ISO 27001, como estándar internacional, establece las especificaciones para un Sistema de Gestión de la Seguridad de la Información (SGSI). Con su explicación nos hace entender que al poner mayor atención en la seguridad de la información evita los eventos de riesgo.

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES.

5.1. Conclusiones

Primero: Se manifestó que al utilizar la norma ISO 27001 se logra mejorar la seguridad de la información en una empresa tecnológica, en Lima en el año 2024, se evidencia que las tasas de incidentes que afectan a las dimensiones han mejorado en un 40% en la confidencialidad en un 27% en disponibilidad y un 30% en la integridad al tener esta variación demuestra que lo controles nos ayudan a mejorar la seguridad de la información en la organización.

Segundo: Se cumplió con el objetivo específico N° 1 al demostrar que la implementación de la norma ISO 27001 mejora el nivel de confidencialidad en la seguridad de la

información en una empresa tecnológica, en Lima en el año 2024; De tal modo podemos decir, que el control que tratamos en esta dimensión, el cual pertenece a la sección A9 sobre el control de acceso como objetivo control 1, en su control 9.2.2 sobre gestión de acceso a los usuarios, donde se observó que se llegó a instalar los registros tras la evaluación de las pruebas del post y pre obteniendo la diferencia promedio de 55% y 16% lo que nos concluyó con la disminución de los índices que afectan a la confidencialidad con esto podemos decir que se mejoró estos controles analizados.

Tercero Se cumplió con el objetivo específico N° 2 al demostrar cómo la implementación de la norma ISO 27001 mejora el nivel de disponibilidad en la seguridad de la información en una empresa tecnológica, en Lima en el año 2024; De tal modo podemos decir, que el control que tratamos en esta dimensión, el cual pertenece a la sección A13 referente a la seguridad en comunicaciones como objetivo de control, en su control 13.1.2, sobre la seguridad de los servicios de red ,se llegó a instalar el registro evaluado y también en su control 13.2.2, se refiere a los acuerdos de intercambio de información, se instaló el registro, donde se observó que tras la evaluación de las pruebas del post y pre se obtuvo la diferencia promedio de 71% y 44% lo que nos concluyó con la disminución de los índices que afectan a la disponibilidad con esto podemos decir que se mejoró los controles de la sección A13 analizados.

Cuarto Se cumplió con el objetivo específico N° 3 al demostrar cómo la implementación de la norma ISO 27001 mejora el nivel de integridad en la seguridad de la

información en una empresa tecnológica, en Lima en el 2024; De tal modo podemos decir, que el control que tratamos en esta dimensión, el cual pertenece a la sección A11, que nos indica los controles de seguridad física y entorno, en su control 11.1.4, la cual está relacionada con los eventos que son causados por la naturaleza y las diferentes acciones que realiza el hombre, en este caso los trabajadores o personas a cargo, se llegó a instalar los registros evaluados y también en su control 11.1.5, que menciona sobre cómo prevenir el acceso físico no autorizado, se observó que tras la evaluación de las pruebas del post y pre se obtuvo la diferencia promedio de 74% y 44% lo que nos concluyó con la disminución de los índices que afectan a la integridad, con esto podemos decir que se mejoró estos controles de la sección A11 analizados.

5.2. Recomendaciones

Primero Se recomienda al directorio, que realice el cumplimiento de todas las políticas de seguridad de la información indicando al personal la importancia de los activos de la organización, con esta medida poder reducir en un porcentaje casi o igual al 100% los eventos de riesgo que influyen en la seguridad de la información.

Segundo Se recomienda al gerente, coordinar capacitaciones constantes en relación con las amenazas y vulnerabilidades que pueden generar fallas en los equipos de la organización, al no poner en práctica, las reglas o directrices presentes en la norma ISO 27001, y así reducir en un porcentaje igual o mayor al 99% la tasa de eventos de riesgo que dañan la confidencialidad, disponibilidad y la integridad.

Tercero Se recomienda al supervisor de TI, realizar la mejora de las normas y los controles que se rigen en la norma ISO 27001 empleando de esta manera una mejora de forma continua, de esta manera llegar a reducir en un porcentaje igual o mayor al 99% los eventos de riesgo que afectan la seguridad de la información, con el compromiso de llegar al nivel máximo de seguridad.

Cuarto Se recomienda al dueño de la organización, desarrollar al 100% la norma "ISO 27001" a nivel organizacional, apuntando así a la certificación y al reconocimiento internacional.

REFERENCIAS

Ael. (2015,29 de abril). *www.ucol.mx*. https://recursos.ucol.mx/tesis/investigacion.php

Aguilar, J. (13 de 05 de 2020). *https://seguridadinternacional.es/*. Obtenido de https://seguridadinternacional.es/: https://seguridadinternacional.es/resi/html/la-brecha-de-ciberseguridad-en-america-latina-frente-al-contexto-global-de-ciberamenazas/

Alba, M. (23 de 11 de 2021). *https://www.ineaf.es/*. Obtenido de https://www.ineaf.es/: https://www.ineaf.es/tribuna/norma-iso-27001/

Alejandro, C. (22 de 6 de 2006). *https://www.redalyc.org/*. Obtenido de https://www.redalyc.org/: https://www.redalyc.org/pdf/167/16722112.pdf

Aleman Balladares, F. (2023). https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/106824/Aleman_BFY-SD.pdf?sequence=1&isAllowed=y. Obtenido de https://hdl.handle.net/20.500.12692/106824

Allan. (2008). *El método hipotético-deductivo.* Ciencias económicas.

Alvarez. (2003). Como hacer investigacion cualitativa. Paidos Ecuador.

Alvarez Cuzme, J. (2019). Plan Informático Basado En La Norma Iso 27001-2013 Para Mejorar La Seguridad De La Información Y La Infraestructura Tecnológica En La Empresa "Calsado Carlín" De Santo Domingo . Santo Domingo – Ecuador: Universidad Regional Autónoma De Los Andes.

Arévalo José, Bayona, R., & Rico, D. (2015). *Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información.* Red de Revistas Científicas de América Latina, el Caribe, España y Portugal.

Arteaga Medranda, L. (2020). "Pasos para realizar una prueba de hipótesis". Manabi - Ecuador: Docz.

Asqui, J., & Torres, J. (2023). *ISO 27001 para mejorar la seguridad de la información en una institución educativa, Lima.* Facultad de Ingeniería y Negocios - Universidad Norbert Wiener.

Agustin, L. (2005). iso27000.es. Obtenido de iso27000.es: https://www.iso27000.es/sgsi.html

Briceño, E. (2021). *Seguridad de la información.* Costa Rica: 3 Ciencias.

Business School, B. (2018). *"La Teoría General de Sistemas y los Sistemas de Producción".* Barcelona: Masters y Posgrados.

Cardenas, L., Becerra, L., & Martinez, H. (2013). *GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.* México: Anfeca.

Carreño Ospina, H. F. (2024). Modelo de ciberseguridad para la protección de la información crítica en las universidades públicas de Colombia. Bogota - Colombia: Editorial ESDEG.

Claude, E. (1948). A Mathematical Theory of Communication de Claude.

Condori-Ojeda, P. (2020). *Universo, población y muestra. Curso Taller.* Obtenido de https://www.aacademica.org/cporfirio/18.pdf

Creswell. (2022). Enfoques cualitativos, cuantitativos y de métodos mixtos . Publicaciones SAGE.

Cristian, D. A. (2020). *http://www.scielo.org.ar/*. Obtenido de http://www.scielo.org.ar/: http://www.scielo.org.ar/pdf/cadmin/n15/2314-3738-cadmin-15-75.pdf

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. Italia: https://www.emerald.com/.

De la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la informa-ción basado en la Norma ISO/IEC 27001. Revista Universidad y Sociedad.

Deivi, F. (2020). Metodología de la investigación: Conceptos, herramientas y ejercicios prácticos en las ciencias administrativas y contables. Editorial Universidad Pontificia Bolivariana. doi: http://doi.org/10.18566/978-958-764-879-9

Desarrollo, B. I. (2020, 14 de julio). *https://publications.iadb.org/*. Obtenido de https://publications.iadb.org/: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Ding, Hershberger. (2013). Tecnologías de la información - Técnicas. Santiago: Norma Chilena.

Elwood Shannon, C., & Weaver, W. (1949). Linguistics and Communication Theory. New York: The University of Illinois Press.

Estrada, A. C. (2017). *Ciberseguridad. www.darFe.es.*

Falcón, M., & Herrera, R. (2005). Análisis del acto estadístico (Guía didáctica). Universidad Bolivariana de Venezuela.

Farrand, J. (2025, 2 de junio). *https://www.redalyc.org/*. Obtenido de https://www.redalyc.org/: https://www.redalyc.org/pdf/401/40170210.pdf

Fidias, A. (1997). *El proyecto de Investigación-Introducción a la metodología científica.* Venezuela: Episteme.

Fuentes Serrate, R. (2020). Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca. Lambayeque – Perú: Universidad Nacional Pedro Ruiz Gallo.

Fuentes. (2022). Metodología de la investigación: Fundamentos, procesos y aplicaciones. Editorial Académica Universitaria.

Flores, G. (2021). Obtenido de ¿Qué es una ficha de observación y cómo se realiza?: New Message! (la-respuesta.com)

Forouzan, B. (2012). Comunicaciones de datos y redes. McGraw.

Giménez. (2023). *Seguridad en equipos informáticos. IFCT0109.* IC Editorial.

Gomez , G. (2020). Métodos y técnicas de investigación utilizados en los estudios sobre comunicación en España. Madrid: Mediterranea.

Griselda, M. (2002). *https://www.redalyc.org/*. Obtenido de https://www.redalyc.org/: *https://www.redalyc.org/pdf/726/72602208.pdf*

Guevara, E., Delgado, J., & Mendoza, A. (20 de 09 de 2022). *https://revistasinvestigacion.unmsm.edu.pe/*. Obtenido de https://revistasinvestigacion.unmsm.edu.pe/: https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/23362

Hernández, R., & Mendoza, C. (2018). *Metodología de la Investigación - Las rutas cuantitativa, cualitativa y mixta*. McGraw-HILL INTERAMERICANA EDITORES, S.A. de C. V.

Hidalgo, L. (2005). Confiabilidad y Validez en el Contexto de la Investigación y Evaluación Cualitativas.

Jorge, W. (2013, 2 de diciembre). *https://www.redalyc.org/*. Obtenido de https://www.redalyc.org/: https://www.redalyc.org/pdf/5116/511651378004.pdf

Julian, R. (2013). *https://www.nqa.com*. Obtenido de https://www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Kosutic, D. (2017,16 de febrero). *PECB Magazine*. Obtenido de https://pecb.com/en: https://pecb.com/past-webinars/7-key-problems-to-avoid-in-iso-27001-implementation

Pequeño, M. (2015). Gestión de servicios en el sistema informático. Editorial Elearning, S.L..

Martin, D. l. (2021,10 de junio). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lang=es. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lang=es: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/http://scielo.sld.cu/pdf/rus/v13n5/2218-3620-rus-13-05-495.pdf

Mata, s. (2019). *Diseños de investigaciones con enfoque cuantitativo de tipo no experimental*. Obtenido de https://investigaliacr.com/investigacion/disenos-de-investigaciones-con-enfoque-cuantitativo-de-tipo-no-experimental/

Medina Romero, M., Cevero Rómulo , R., Wilder, B., Raquel Monica , L., Christian Paolo, M., & Roxana Yolanda, C. (2023). Metodología de la investigación: Técnicas e instrumentos de investigación. Puno: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.

Medina Pinillos, J. (2023). ISO 27001 para la gestión de seguridad de la información en el área TI de una empresa industrial. Lima: Universidad César Vallejo.

Miñan Mia. (2023). definicionwiki.com. definicionwiki.com: https://definicionwiki.com/

Mónica, G. (2015,1 de junio). *https://www.redalyc.org/*. Obtenido de https://www.redalyc.org/: https://www.redalyc.org/pdf/2654/265440664005.pdf

Moron Peredo, K. R. (2023). "Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C". Pimentel - Chiclayo: Universidad Señor de Sipan.

Murillo, W. (2008). La investigación científica:Una forma de conocer las realidades con evidencia científica.

Narváez Contero, C. V., & Yungán Cazar, J. C. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. Riobamba - Ecuador: Revista Cientifica dominio de las Ciencias.

Normalización, O. I. (2013). Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información. ISO/IEC 27001:2013.

López -López. (2023). Relación entre el enfoque inductivo o deductivo del aprendizaje basado en casos en el rendimiento académico, la autoeficacia y la satisfacción de los estudiantes de trabajo social. Acciones e Investigaciones Sociales.

OEA. (2020). Reporte Ciberseguridad 2020: Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe. https://doi.org/10.18235/0002513

Ostec. (2015, 06 de octubre). *https://ostec.blog/es*. Obtenido de https://ostec.blog/es: https://ostec.blog/es/aprendizaje-descubrimiento/iso-27001/?cn-reloaded=1.

Ouchi, W. (1981). Theory Z: How American Business Can Meet the Japanese Challenge. Addison-wesley.

Peña, D. (2017). Fundamentos de Estadística. Alianza.

Pontijas Calderón, J. (2023). Unión Europea: ciberseguridad y ciberdefensa. Instituto Español de Estudios Estratégicos, 1-14.

Polit, y Beck, C. (2021). Investigación en enfermería: generación y evaluación de evidencia para la práctica de enfermería. Undécima edición.

Porporato, M., & Waweru, N. (2011 de junio). http://www.observatorio-iberoamericano.org/. Obtenido de http://www.observatorio-iberoamericano.org/: http://www.observatorio-iberoamericano.org/ricg/N%C2%BA_17/Marcela_Porporato_y_Nelson_Waweru.pdf

Pueblo, D. d. (2023, 2 de mayo). *https://www.defensoria.gob.pe/*. Obtenido de https://www.defensoria.gob.pe/: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia

Rodriguez Calero. (2022). Factores de riesgo de dificultad en la canalización venosa periférica en atención hospitalaria. Estudio caso-control multicéntrico. Universitat de les Illes Balears.

Saeckel, A. (2023, 18 de enero). https://www.dqsglobal.com/es-es/. Obtenido de https://www.dqsglobal.com/es-es/formacion/blog/iso-27001-anexo-a-responsabilidades-y-funciones-de-los-empleados?utm_source=chatgpt.com.

Sistemas, A. (23 de 01 de 2019). *https://www.americasistemas.com.pe/*. Obtenido de https://www.americasistemas.com.pe/: https://www.americasistemas.com.pe/empresas-de-aece-logran-certificacion-iso-27001/

Tecnología, I. y. (11 de enero de 2019). *https://www.unir.net/*. Obtenido de https://www.unir.net/: https://www.unir.net/ingenieria/revista/iso-27001/

Torres Chango, C. (2020). Plan De Seguridad Informática Basado En La Norma Iso 27001, Para Proteger La Información Y Activos De La Empresa Privada Megaprofer S.A. Ambato – Ecuador: Universidad Técnica De Ambato.

Trejo Medina, D. (2020, 8 de abril). Gobierno de datos, conceptos básicos. México: Universidad Nacional Autónoma de México.

Unir. (2023). *Seguridad informática: ¿en qué consiste este término?* Obtenido de unir: https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/

Uwe, F. (2015). *El diseño de Investigación cualitativa.* Madrid: Ediciones Morata.

Valencia, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia ISO/IEC 2700.* Bogotá D.C.: Editorial Universidad Nacional de Colombia.

Vargas, z. (2009). *La investigación aplicada: una forma de conocer realidades con evidencia científica.* costa rica: educación 33.

Vázquez, E. (2023, 30 de junio). *https://revistas.utp.edu.co/*. Obtenido de https://revistas.utp.edu.co/: https://revistas.utp.edu.co/index.php/miradas/article/view/25276

Viteri Quishpi, G., Romero Fernández, A., & Mendieta Larreategui, C. (2022). Modelo de gestión por procesos y mejora continua. Santa Ana de Coro. Venezuela: Instituto de Investigación y Estudios Avanzados Koinonía (IIEAK).

Villa, M., Suárez, M., & Molina, L. (28 de 9 de 2018). *https://revistas.uamerica.edu.co/*. Obtenido de https://revistas.uamerica.edu.co/: https://revistas.uamerica.edu.co/index.php/rques/article/view/253/220

Von Bertalanffy, L. (1968). *Teoría general de sistemas: Fundamentos, desarrollo, aplicaciones.* Nueva York: Geroge.

Woodward, J. (1965). Industrial Organization: Theory and Practice. Oxford University Press.

ANEXOS

Anexo 1: Matriz de Consistencia

Título de investigación: ISO 27001 para mejorar la seguridad de la información en una empresa tecnológica, Lima 2024.

Formulación del Problema	Objetivos	Hipótesis	Variables	Diseño metodológico
Problema general: ¿En qué medida la implementación de la ISO 27001 aumenta la seguridad de la información en una empresa tecnológica, Lima 2024? **Problemas específicos:** **PE 1**: ¿En qué medida la implementación de la ISO 27001 aumenta el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024? **PE 2:** ¿En qué medida la implementación de la ISO 27001 aumenta el nivel disponibilidad de la información en una empresa tecnológica, Lima 2024? **PE3**: ¿En qué medida la implementación de la ISO 27001 aumenta el nivel integridad de la información en una empresa tecnológica, Lima 2024?	**Objetivo general:** Determinar en qué medida la implementación de la ISO 27001 aumenta la seguridad de la información en una empresa tecnológica, Lima 2024. **Objetivos específicos:** **OE1:** Determinar en qué medida la implementación de la ISO 27001 aumenta el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024. **OE2:** Determinar en qué medida la implementación de la ISO 27001 aumenta el nivel disponibilidad de la información en una empresa tecnológica, Lima 2024. **OE 3:** Determinar en qué medida la implementación de la ISO 27001 aumenta el nivel de integridad de la información en una empresa tecnológica, Lima 2024.	**Hipótesis general:** La implementación de la ISO 27001 mejora la información en una empresa tecnológica, Lima 2024. **Hipótesis específicas:** **HE1:** La implementación de la ISO 27001 mejora el nivel de confidencialidad de la información en una empresa tecnológica, Lima 2024. **HE2:** La implementación de la ISO 27001 mejora el nivel de disponibilidad de la información en una empresa tecnológica, Lima 2024. **HE3**: La implementación de la ISO 27001 mejora el nivel de integridad de la información en una empresa tecnológica, Lima 2024.	**Variable independiente:** ISO 27001. **Dimensiones:** 1. Planificar. 2. Hacer. 3. Verificar. 4. Actuar. **Variable dependiente:** Seguridad de la información. **Dimensiones:** 1. Confidencialidad. 2. Disponibilidad. 3. Integridad.	**Tipo de investigación Aplicada** **Método y diseño de investigación** **Método:** Hipotético-deductivo y analítico. Diseño: Experimental de tipo preexperimental **Enfoque:** cuantitativo **Población:** 20 tipos de eventos o riesgos, de la entidad privada tecnológica ubicada en Lince. **Muestra:** 20 tipo de eventos de riesgos, observados en 15 días

Anexo 2: Matriz de operacionalización de la variable.

Variable 1: ISO 27001

Definición Conceptual	Definición Operacional	Dimensión	Indicadores	Escala De Medición
La norma ISO 27001:2013 ha sido elaborada con el fin de establecer los requisitos para el establecimiento, la implementación, el mantenimiento y la mejora continua de un sistema de gestión de seguridad de la información que permita preservar la confidencialidad, la integridad y la disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos (Duque F. J., Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 27000, 2021)	La variable ISO27001, se medirá por medio de una ficha de cotejo que posee un total de 022 controles a evaluar en la empresa tecnológica, el cual aborda 3 dimensiones; Confidencialidad (8 ítems), Disponibilidad (7 ítems) e Integridad(ítems), en una escala alfa de Cronbach, tipo ordinal.	Planificar	Conocer el estado actual de la situación que se quiere mejorar o cambiar. Establecer metas y objetivos claros y medibles. Monitorear y evaluar el progreso y los resultados de las acciones.	Porcentaje
		Hacer	Porcentaje de cumplimiento Tiempo de ciclo Tasa de defectos Asegurar la calidad y la confiabilidad del modelo o el producto.	
		Verificar	Detectar y corregir posibles errores, defectos o desviaciones. Evaluar el grado de satisfacción de los clientes o usuarios.	
		Actuar	Identificar las oportunidades y las necesidades Medir el impacto y el valor agregado de las acciones Ajustar y optimizar los procesos y los recursos	

Variable 2: Seguridad de la Información

Definición Conceptual	Definición Operacional	Dimensión	Indicadores	Escala De Medición
La seguridad informática, también conocida como ciberseguridad o seguridad de las tecnologías de la información, es la protección de los sistemas informáticos contra el robo o daño al hardware, software o la información sobre los mismos, así como a la interrupción o la redirección de los servicios que proveen (Estrada, 2017)	La variable Seguridad de la información se medirá con una ficha de cotejo con 20 controles a evaluar en la empresa tecnológica, que aborda 3 dimensiones; Confidencialidad (8 ítems), Disponibilidad (6 ítems) e Integridad (6 ítems), en una escala del alfa de Cronbach, tipo ordinal.	Confidencialidad	Nivel de cumplimiento de confidencialidad (NCC) va a ser igual a la sumatoria de los puntajes entre número total de controles NCC= $\frac{\sum \square Puntuación\ de\ confidencialidad}{N°\ de\ \ controles\ de\ confidencialidad}$	Porcentaje
		Disponibilidad	Nivel de cumplimiento de disponibilidad (NCD) va a ser igual a la sumatoria de los puntajes entre número de controles $NCD = \frac{\sum \square\ Puntuación\ de\ disponibilidad}{N°\ de\ \ controles\ de\ disponibilidad}$	
		Integridad	Nivel de cumplimiento de integridad (NCI) va a ser igual a la sumatoria de los puntajes entre número de controles $NCI = \frac{\sum \square\ Puntuación\ de\ integridad}{N°\ de\ \ controles\ de\ integridad}$	

Anexo 3: Tablas de Confiabilidad.

Para saber si nuestro instrumento es confiable y pueda permitir realizar el proceso de validación en un procedimiento pre y post tomamos unos días previos para poder ver los resultados y evaluar la confiabilidad del instrumento en la recolección de datos en los días mostrados

PRE-TEST	REGISTRÓ DE EVENTOS	CONFIDENCIALIDAD			DISPONIBILIDAD			INTEGRIDAD			C	D	I	TOTAL, PRE-TEST
Fecha	Días	R1	R2	R3	R1	R2	R3	R1	R2	R3				
13/11/2023	D1	1	1	0	1	0	1	1	0	1	2	2	2	6
14/11/2023	D2	1	1	1	1	1	1	0	0	1	3	3	1	7
15/11/2023	D3	1	0	1	0	1	1	1	0	1	2	2	2	6
16/11/2023	D4	0	1	1	1	0	1	0	1	0	2	2	1	5
17/12/2023	D5	0	1	1	0	1	1	1	0	1	2	2	2	6

POST TEST	REGISTRÓ DE EVENTOS	CONFIDENCIALIDAD			DISPONIBILIDAD			INTEGRIDAD			C	D	I	TOTAL, POST-TEST
Fecha	Días	R1	R2	R3	R1	R2	R3	R1	R2	R3				
20/11/2023	D1	1	1	1	1	0	1	1	1	1	3	2	3	8
21/11/2023	D2	1	1	1	1	1	1	0	1	1	3	3	2	8
22/11/2023	D3	1	0	1	1	1	1	1	1	1	2	3	3	8
23/11/2023	D4	0	1	1	1	1	1	1	1	0	2	3	2	7
24/12/2023	D5	1	1	1	1	1	1	1	0	1	3	3	2	8

Anexo 4: Validación Aiken

Empleo de la Formula V de Aiken

En cuenta de los datos obtenidos se realizó la validación respectiva del instrumento el cual se validó con una fórmula de validación que fue la V de Aiken:

$$V = \frac{S}{(n(c-1))}$$

Donde:

S: sumatoria total de puntuación de los expertos.

n: número total de expertos validadores.

c: número de escala de valores.

En la validación del instrumento al emplear los datos estadísticos del V de Aiken lo que nos permitió validar los ítems seleccionados en base a la ficha de observación que se empleó para la calificación dicotómica, lo cual permitió la comprobación de los expertos que intervinieron en la validación del instrumento, donde obtuvimos como resultado 1(la unidad) que nos permite describir el nivel de consistencia interna o fiabilidad al obtenerlo con el alfa de Cronbach es considerado excelente.

Calculando la fórmula de V de Aiken en una hoja de cálculo:

$$V = \frac{S}{(n(c-1))}$$

Expertos	Validador 1			Validador 2			Validador 3			Validador 4			$V = \frac{S}{(n(c-1))}$	
Criterio	1.P	2.R	3.C	1.P	2.R	3.C	1.P	2.R	3.C	1.P	2.R	3.C		
Confidencialidad	**Sí**			**Sí**			**Sí**			**Sí**			**S**	**V DE AIKEN**
Item 1	1			1			1			1			4	1.00
Item 2	1			1			1			1			4	1.00
Item 3	1			1			1			1			4	1.00
Item 4	1			1			1			1			4	1.00
Item 5	1			1			1			1			4	1.00
Item 6	1			1			1			1			4	1.00
Item 7	1			1			1			1			4	1.00
Item 8	1			1			1			1			4	1.00
Disponibilidad	**Sí**			**Sí**			**Sí**			**Sí**				
Item 9	1			1			1			1			4	1.00
Item 10	1			1			1			1			4	1.00
Item 11	1			1			1			1			4	1.00
Item 12	1			1			1			1			4	1.00
Item 13	1			1			1			1			4	1.00
Item 14	1			1			1			1			4	1.00
Integridad	**Sí**			**Sí**			**Sí**			**Sí**				
Item 15	1			1			1			1			4	1.00
Item 16	1			1			1			1			4	1.00
Item 17	1			1			1			1			4	1.00
Item 18	1			1			1			1			4	1.00
Item 19	1			1			1			1			4	1.00
Item 20	1			1			1			1			4	1.00

Criterios:

P: pertinencia.

R: relevancia.

C: claridad.

Anexo 5: Instrumento.

Universidad Norbert Wiener	**Escuela Académica Profesional de Ingeniería** **ISO 27001 para mejorar la seguridad de la información en una empresa tecnológica, Lima 2024**	
Pre – test	**Observador:** Cruz Córdova Harold **Fecha: 01**/12/2023 al 15/12/2023 **Lugar:** sede única - Lince	**Área: TI** **RE-001** **N°: LC-001**

Objetivo: Demostrar que los controles de la norma ISO 27001 mejora el nivel de confidencialidad en la seguridad de la información en una empresa tecnológica, Lima 2024.

FICHA DE OBSERVACIÓN

Dimensión: Confidencialidad

Sección: A9 Control de acceso

Dimensión Confidencialidad		
	Objetivo control 1: Requisitos de negocio para el control de acceso	**EVENTO**
	Control: 9.1.2 Acceso a las redes y a los servicios de red	
	1. Existe control de acceso con usuario y clave único, en base a roles para accesos diferenciados.	
	2. Existen procedimientos de autorización para el acceso a la red.	
	3. Se tiene un control de los dispositivos por cual se acceden a la red.	
	Objetivo control 2: Gestión del acceso de usuarios	
	Control: 9.2.1 Registro de usuarios y cancelación del registro	
	4.Se monitorea las actividades inusuales o intentos de acceso no autorizados de los usuarios.	
	5.Se da de baja a las cuentas de usuario cuando el trabajador abandona la organización.	
	Control: 9.2.2 Gestión de acceso a los usuarios	
	6. En la verificación de accesos cumplen con la longitud > 8 a caracteres, incluyendo caracteres especiales, mayúsculas, minúsculas y números.	
	7. Se logra registrar los accesos otorgados a los usuarios.	
	8. Se usan los roles de acceso a los usuarios para los permisos que sean necesarios.	
	Nivel de cumplimiento de confidencialidad (NCC) va ser igual a la sumatoria de los puntajes entre número total de controles. **NCC = (∑ Puntuación de confidencialidad) / (N° de controles de confidencialidad)**	

Objetivo: Demostrar que los controles de la norma ISO 27001 mejora el nivel de disponibilidad en la seguridad de la información en una empresa tecnológica, Lima 2024.

Dimensión Disponibilidad	**Dimensión: Disponibilidad**	
	Sección: A13 Seguridad en las comunicaciones	
	Objetivo control 1: Gestión de la seguridad de red	
	Control: 13.1.2 Seguridad de los servicios de red	
	1. Cuenta con reglas de filtrado de paquetes para control del tráfico de red y prevenir ataques maliciosos.	
	2. Cuentan con algún firewall certificado para la seguridad de la red.	
	Objetivo control 2: Intercambio de información	
	Control: 13.2.1 Políticas y procedimientos de intercambio de información	
	3. Existe algún filtro para la transmisión de la información.	
	4. Existe algún mecanismo de encriptación para el intercambio de información.	
	5. Cuentan con procedimientos para el respaldo de los datos.	
	Control: 13.2.2 Acuerdos de intercambio de información	
	6. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica.	
	Nivel de cumplimiento de disponibilidad (NCD) va ser igual a la sumatoria de los puntajes entre número total de controles. **NCD = (∑ Puntuación de disponibilidad) / (N° de controles de disponibilidad)**	
	Objetivo: Demostrar que los controles de la norma ISO 27001 mejora el nivel de integridad en la seguridad de la información en una empresa tecnológica, Lima 2024.	
Dimensión Integridad	**Dimensión: Integridad**	
	Sección: A11 seguridad física y del entorno	
	Objetivo control 1: Áreas seguras	
	Control: 11.1.1 Perímetro de seguridad física	
	1. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulación no autorizada	
	2. Existe alguna medida que restringe el acceso al centro de datos.	
	Control: 11.1.4 Protección contra amenazas externas y del ambiente	
	3. Existe algún plan de contingencia contra desastres naturales.	
	4. Existe alguna protección física contra ataques maliciosos o accidentes.	
	Control: 11.1.5 El trabajo en las áreas seguras	
	5. Cuentan con protocolos para el acceso de terceros al área de TI	
	6. Existen alguna restricción para el ingreso de equipos tecnológicos al área de TI	
	El Nivel de cumplimiento de integridad (NCI) va ser igual a la sumatoria de los puntajes entre número total de controles. **NCI = (∑ Puntuación de integridad) / (N°de controles de integridad)**	

	Registro de Eventos	Confidencialidad										Disponibilidad								Integridad							
Fecha	Días	R1	R2	R3	R4	R5	R6	R7	R8		Pre_Conf	R9	R10	R11	R12	R13	R14		Pre_Dispo	R15	R16	R17	R18	R19	R20		Pre_Inte
1/12/2023	D1	1	0	1	1	0	1	0	1	**5**	0.6	1	1	1	1	0	0	**4**	0.7	1	1	1	1	0	1	**5**	0.8
2/12/2023	D2	1	1	1	1	1	0	0	0	**5**	0.6	1	1	1	1	0	0	**4**	0.7	1	0	1	1	0	1	**4**	0.7
3/12/2023	D3	1	1	1	1	1	0	0	0	**5**	0.6	1	1	1	1	0	0	**4**	0.7	1	1	1	1	1	1	**6**	1.0
4/12/2023	D4	1	1	1	1	0	0	0	0	**4**	0.5	1	1	1	1	1	1	**6**	1.0	1	0	1	1	0	1	**4**	0.7
5/12/2023	D5	1	1	1	0	1	0	1	0	**5**	0.6	1	1	1	1	1	1	**6**	1.0	1	0	1	1	1	0	**4**	0.7
6/12/2023	D6	0	0	0	0	0	0	0	0	**0**	0.0	0	1	0	1	0	0	**2**	0.3	1	1	0	1	0	1	**4**	0.7
7/12/2023	D7	1	1	0	0	1	1	0	0	**4**	0.5	1	1	1	1	1	1	**6**	1.0	1	1	1	1	1	1	**6**	1.0
8/12/2023	D8	1	1	0	1	1	0	0	1	**5**	0.6	0	1	1	1	1	0	**4**	0.7	0	1	0	1	1	1	**4**	0.7
9/12/2023	D9	1	1	1	0	0	0	1	1	**5**	0.6	1	0	0	1	0	1	**3**	0.5	0	1	1	1	0	1	**4**	0.7
10/12/2023	D10	1	0	1	0	1	0	1	1	**5**	0.6	1	1	1	0	0	1	**4**	0.7	0	0	1	1	1	1	**4**	0.7
11/12/2023	D11	1	0	0	0	1	1	1	1	**5**	0.6	1	1	0	1	0	0	**3**	0.5	0	1	0	1	1	1	**4**	0.7
12/12/2023	D12	0	1	1	1	0	0	0	0	**3**	0.4	1	0	1	1	1	1	**5**	0.8	1	1	1	0	1	0	**4**	0.7
13/12/2023	D13	0	0	1	1	1	1	0	1	**5**	0.6	0	1	1	0	0	1	**3**	0.5	1	1	1	1	1	1	**6**	1.0
14/12/2023	D14	1	0	1	1	1	0	0	1	**5**	0.6	1	1	1	0	1	1	**5**	0.8	1	0	1	1	1	0	**4**	0.7
15/12/2023	D15	1	0	0	1	0	1	1	1	**5**	0.6	1	1	1	0	1	1	**5**	0.8	0	1	0	1	1	1	**4**	0.7
	PROM	0.8	0.5	0.67	0.60	0.60	0.33	0.33	0.53		**0.55**	0.8	0.9	0.8	0.7	0.5	0.6		**0.71**	0.67	0.67	0.73	0.93	0.67	0.80		**0.74**

Universidad Norbert Wiener	**Facultad de Ingeniería y Negocios** **Escuela Académica Profesional de Ingeniería** **ISO 27001 para mejorar la seguridad de la información en una empresa tecnológica, Lima 2024**

POST – test	**Observador:** Cruz Córdoba Harold	**Área: TI**
	Fecha: 02/01/2024 al 16/01/2024	**RE-001**
	Lugar: sede única - Lince	**N°: LC-001**

Dimensión Confidencialidad

Objetivo: Demostrar que los controles de la norma ISO 27001 mejora el nivel de confidencialidad en la seguridad de la información en una empresa tecnológica, Lima 2024.

FICHA DE OBSERVACIÓN	
Dimensión: Confidencialidad	
Sección: A9 Control de acceso	
Objetivo control 1: Requisitos de negocio para el control de acceso	**EVENTO**
Control: 9.1.2 Acceso a las redes y a los servicios de red	
1. Existe control de acceso con usuario y clave único, en base a roles para accesos diferenciados.	
2. Existen procedimientos de autorización para el acceso a la red.	
3. Se tiene un control de los dispositivos por cual se acceden a la red.	
Objetivo control 2: Gestión del acceso de usuarios	
Control: 9.2.1 Registro de usuarios y cancelación del registro	
4.Se monitorea las actividades inusuales o intentos de acceso no autorizados de los usuarios.	
5.Se da de baja a las cuentas de usuario cuando el trabajador abandona la organización.	
Control: 9.2.2 Gestión de acceso a los usuarios	
6. En la verificación de accesos cumplen con la longitud > 8 a caracteres, incluyendo caracteres especiales, mayúsculas, minúsculas y números.	
7. Se logra registrar los accesos otorgados a los usuarios.	
8. Se usan los roles de acceso a los usuarios para los permisos que sean necesarios.	
Nivel de cumplimiento de confidencialidad (NCC) va ser igual a la sumatoria de los puntajes entre número total de controles. **NCC = (∑ Puntuación de confidencialidad) / (N° de controles de confidencialidad)**	

	Objetivo: Demostrar que los controles de la norma ISO 27001 mejora el nivel de disponibilidad en la seguridad de la información en una empresa tecnológica, Lima 2024.	
Dimensión Disponibilidad	**Dimensión: Disponibilidad**	
	Sección: A13 Seguridad en las comunicaciones	
	Objetivo control 1: Gestión de la seguridad de red	
	Control: 13.1.2 Seguridad de los servicios de red	
	1. Cuenta con reglas de filtrado de paquetes para control del tráfico de red y prevenir ataques maliciosos.	
	2. Cuentan con algún firewall certificado para la seguridad de la red.	
	Objetivo control 2: Intercambio de información	
	Control: 13.2.1 Políticas y procedimientos de intercambio de información	
	3. Existe algún filtro para la transmisión de la información.	
	4. Existe algún mecanismo de encriptación para el intercambio de información.	
	5. Cuentan con procedimientos para el respaldo de los datos.	
	Control: 13.2.2 Acuerdos de intercambio de información	
	6. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica.	
	Nivel de cumplimiento de disponibilidad (NCD) va ser igual a la sumatoria de los puntajes entre número total de controles. **NCD = (∑ Puntuación de disponibilidad) / (N° de controles de disponibilidad)**	
	Objetivo: Demostrar que los controles de la norma ISO 27001 mejora el nivel de integridad en la seguridad de la información en una empresa tecnológica, Lima 2024.	

Dimensión Integridad		
	Dimensión: Integridad	
	Sección: A11 seguridad física y del entorno	
	Objetivo control 1: Áreas seguras	
	Control: 11.1.1 Perímetro de seguridad física	
	1. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulación no autorizada	
	2. Existe alguna medida que restringe el acceso al centro de datos.	
	Control: 11.1.4 Protección contra amenazas externas y del ambiente	
	3. Existe algún plan de contingencia contra desastres naturales.	
	4. Existe alguna protección física contra ataques maliciosos o accidentes.	
	Control: 11.1.5 El trabajo en las áreas seguras	
	5. Cuentan con protocolos para el acceso de terceros al área de TI	
	6. Existen alguna restricción para el ingreso de equipos tecnológicos al área de TI	
	El Nivel de cumplimiento de integridad (NCI) va ser igual a la sumatoria de los puntajes entre número total de controles. **NCI = (∑ Puntuación de integridad) / (N° de controles de integridad)**	

	Registro de Eventos	Confidencialidad										Disponibilidad								Integridad								
Fecha	Días	R1	R2	R3	R4	R5	R6	R7	R8		Post_Conf	R9	R10	R11	R12	R13	R14		Post_Dispo	R15	R16	R17	R18	R19	R20		Post_Inte
2/01/2024	D1	0	0	0	0	1	0	0	1	**2**	0.3	1	0	1	1	0	0	**3**	0.5	1	1	1	1	0	0	**4**	0.67
3/01/2024	D2	1	0	0	0	0	0	0	0	**1**	0.1	0	0	1	1	0	0	**2**	0.3	1	1	1	0	0	0	**3**	0.50
4/01/2024	D3	0	0	1	0	0	0	0	0	**1**	0.1	1	0	1	1	0	0	**3**	0.5	1	1	1	1	1	1	**6**	1.00
5/01/2024	D4	0	1	0	0	0	0	0	0	**1**	0.1	1	1	0	1	1	1	**5**	0.8	0	0	1	0	0	0	**1**	0.17
6/01/2024	D5	0	0	0	0	1	0	0	0	**1**	0.1	1	0	1	1	0	1	**4**	0.7	1	0	0	1	0	0	**2**	0.33
7/01/2024	D6	0	0	0	1	0	0	0	0	**1**	0.1	0	1	0	0	1	0	**2**	0.3	1	1	0	0	1	0	**3**	0.50
8/01/2024	D7	0	1	0	0	0	1	0	0	**2**	0.3	0	1	1	0	0	0	**2**	0.3	0	0	1	0	0	0	**1**	0.17
9/01/2024	D8	0	0	0	0	0	0	0	1	**1**	0.1	0	1	0	1	0	0	**2**	0.3	1	1	0	0	1	0	**3**	0.50
10/01/2024	D9	1	0	0	0	0	0	0	1	**2**	0.3	0	1	1	1	0	0	**3**	0.5	1	0	0	0	1	0	**2**	0.33
11/01/2024	D10	0	0	0	0	0	0	1	0	**1**	0.1	0	0	1	0	1	0	**2**	0.3	0	1	1	0	1	1	**4**	0.67
12/01/2024	D11	1	0	0	0	0	0	0	0	**1**	0.1	0	0	1	0	1	0	**2**	0.3	0	1	0	1	0	0	**2**	0.33
13/01/2024	D12	0	0	0	0	0	0	0	0	**0**	0.0	0	1	0	1	1	0	**3**	0.5	0	0	1	0	0	1	**2**	0.33
14/01/2024	D13	0	0	1	0	0	0	1	0	**2**	0.3	1	0	0	0	0	1	**2**	0.3	1	1	0	1	1	0	**4**	0.67
15/01/2024	D14	0	0	0	1	0	0	0	0	**1**	0.1	0	1	0	0	0	1	**2**	0.3	1	0	1	0	0	0	**2**	0.33
16/01/2024	D15	1	0	0	0	0	0	0	0	**1**	0.1	0	1	0	1	1	0	**3**	0.5	0	0	1	0	0	0	**1**	0.17
	PROM	0.3	0.1	0.1333	0.13	0.1	0.067	0.1	0.2		**0.15**	0.33	0.5	1	0.6	0.4	0		**0.44**	0.6	0.5	1	0.33	0	0		**0.44**

Anexo 6: Validez del Instrumento.

N. º DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
Variable 2: Seguridad de la Información							
DIMENSIÓN 1: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1. Existe control de acceso con usuario y clave único, en base a roles para accesos diferenciados.	X		X		X		
2. Existen procedimientos de autorización para el acceso a la red.	X		X		X		
3. Se tiene un control de los dispositivos por cual se acceden a la red.	X		X		X		
4. Se monitorea las actividades inusuales o intentos de acceso no autorizados de los usuarios.	X		X		X		
5. Se le da de baja a las cuentas de usuario cuando el trabajador abandona la organización.	X		X		X		
6. En la verificación de accesos cumplen con la longitud > a 8 incluyendo caracteres especiales, mayúsculas, minúsculas y números	X		X		X		
7. Se logra registrar los accesos otorgados a los usuarios.	X		X		X		
8. Se usan los roles de acceso a los usuarios para los permisos que sean necesarios.	X		X		X		
DIMENSIÓN 2: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9. Cuentan con reglas de filtrado de paquetes para control del tráfico de red para prevenir ataques maliciosos	X		X		X		
10. Cuentan con algún firewall certificado para la seguridad de la red.	X		X		X		
11. Existe algún filtro para la transmisión de la información.	X		X		X		
12. Existe algún mecanismo de encriptación para el intercambio de información.	X		X		X		
13. Cuentan con procedimientos para el respaldo de los datos.	X		X		X		
14. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica.	X		X		X		
DIMENSIÓN 3: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
15. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulación no autorizada.	X		X		X		
16. Existe alguna medida de protección de acceso al centro de datos.	X		X		X		
17. Existe algún plan de contingencia contra desastres naturales.	X		X		X		
18. Existe alguna protección física contra ataques maliciosos o accidentes.	X		X		X		
19. Cuentan con protocolos para el acceso de terceros al área de TI.	X		X		X		
20. Existe alguna restricción para el ingreso de equipos tecnológicos al área de TI.	X		X		X		

1 **Pertinencia:** el ítem corresponde al concepto teórico formulado.

2 **Relevancia:** el ítem es apropiado para representar al componente o dimensión específica del constructo.

3 **Claridad:** se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

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

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:
Aplicable [X]
Aplicable después de corregir [ ]
No aplicable [ ]

Apellidos y nombres del juez validador: Chávez Alvarado, Walter Amador **DNI:** 09731774
Correo electrónico institucional:
Metodólogo [ ]
Temático [X]
Estadístico [ ]

Lima, 13 de enero del 2024

Firma del experto informante

N.º DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
Variable 2: Seguridad de la Información							
DIMENSIÓN 1: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1. Existe control de acceso con usuario y clave único, en base a roles para accesos diferenciados.	X		X		X		
2. Existen procedimientos de autorización para el acceso a la red.	X		X		X		
3. Se tiene un control de los dispositivos por cual se acceden a la red.	X		X		X		
4. Se monitorea las actividades inusuales o intentos de acceso no autorizados de los usuarios.	X		X		X		
5. Se le da de baja a las cuentas de usuario cuando el trabajador abandona la organización.	X		X		X		
6. En la verificación de accesos cumplen con la longitud > a 8 incluyendo caracteres especiales, mayúsculas, minúsculas y números	X		X		X		
7. Se logra registrar los accesos otorgados a los usuarios.	X		X		X		
8. Se usan los roles de acceso a los usuarios para los permisos que sean necesarios.	X		X		X		
DIMENSIÓN 2: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9. Cuentan con reglas de filtrado de paquetes para control del tráfico de red para prevenir ataques maliciosos	X		X		X		
10. Cuentan con algún firewall certificado para la seguridad de la red.	X		X		X		
11. Existe algún filtro para la transmisión de la información.	X		X		X		
12. Existe algún mecanismo de encriptación para el intercambio de información.	X		X		X		
13. Cuentan con procedimientos para el respaldo de los datos.	X		X		X		
14. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica.	X		X		X		
DIMENSIÓN 3: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
15. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulación no autorizada.	X		X		X		
16. Existe alguna medida de protección de acceso al centro de datos.	X		X		X		
17. Existe algún plan de contingencia contra desastres naturales.	X		X		X		
18. Existe alguna protección física contra ataques maliciosos o accidentes.	X		X		X		
19. Cuentan con protocolos para el acceso de terceros al área de TI.	X		X		X		
20. Existe alguna restricción para el ingreso de equipos tecnológicos al área de TI.	X		X		X		

1 **Pertinencia:** el ítem corresponde al concepto teórico formulado.

2 **Relevancia:** el ítem es apropiado para representar al componente o dimensión específica del constructo.

3 **Claridad:** se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

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

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:
Aplicable [X]
Aplicable después de corregir [ ]
No aplicable [ ]

Apellidos y nombres del juez validador: Arones Pérez, Paolo Paulino **DNI:** 75096354
Correo electrónico institucional:
Metodólogo [ ]
Temático [ ]
Estadístico [ ]

Lima, 29 de enero del 2024

Firma del experto informante

N.º DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
Variable 2: Seguridad de la Información							
DIMENSIÓN 1: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1. Existe control de acceso con usuario y clave único, en base a roles para accesos diferenciados.	X		X		X		
2. Existen procedimientos de autorización para el acceso a la red.	X		X		X		
3. Se tiene un control de los dispositivos por cual se acceden a la red.	X		X		X		
4. Se monitorea las actividades inusuales o intentos de acceso no autorizados de los usuarios.	X		X		X		
5. Se le da de baja a las cuentas de usuario cuando el trabajador abandona la organización.	X		X		X		
6. En la verificación de accesos cumplen con la longitud > a 8 incluyendo caracteres especiales, mayúsculas, minúsculas y números	X		X		X		
7. Se logra registrar los accesos otorgados a los usuarios.	X		X		X		
8. Se usan los roles de acceso a los usuarios para los permisos que sean necesarios.	X		X		X		
DIMENSIÓN 2: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9. Cuentan con reglas de filtrado de paquetes para control del tráfico de red para prevenir ataques maliciosos	X		X		X		
10. Cuentan con algún firewall certificado para la seguridad de la red.	X		X		X		
11. Existe algún filtro para la transmisión de la información.	X		X		X		
12. Existe algún mecanismo de encriptación para el intercambio de información.	X		X		X		
13. Cuentan con procedimientos para el respaldo de los datos.	X		X		X		
14. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica.	X		X		X		
DIMENSIÓN 3: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
15. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulación no autorizada.	X		X		X		
16. Existe alguna medida de protección de acceso al centro de datos.	X		X		X		
17. Existe algún plan de contingencia contra desastres naturales.	X		X		X		
18. Existe alguna protección física contra ataques maliciosos o accidentes.	X		X		X		
19. Cuentan con protocolos para el acceso de terceros al área de TI.	X		X		X		
20. Existe alguna restricción para el ingreso de equipos tecnológicos al área de TI.	X		X		X		

1 Pertinencia: el ítem corresponde al concepto teórico formulado.

2 Relevancia: el ítem es apropiado para representar al componente o dimensión específica del constructo.

3 Claridad: se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

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

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:
Aplicable [X]
Aplicable después de corregir [ ]
No aplicable [ ]

Apellidos y nombres del juez validador: Karen Menacho Navarrete **DNI:** 24002602
Correo electrónico institucional:
Metodólogo [ ]
Temático [X]
Estadístico [ ]

Lima, 13 de enero del 2024

Firma del experto informante

N.º DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
Variable 2: Seguridad de la Información							
DIMENSIÓN 1: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1. Existe control de acceso con usuario y clave único, en base a roles para accesos diferenciados.	X		X		X		
2. Existen procedimientos de autorización para el acceso a la red.	X		X		X		
3. Se tiene un control de los dispositivos por cual se acceden a la red.	X		X		X		
4. Se monitorea las actividades inusuales o intentos de acceso no autorizados de los usuarios.	X		X		X		
5. Se le da de baja a las cuentas de usuario cuando el trabajador abandona la organización.	X		X		X		
6. En la verificación de accesos cumplen con la longitud > a 8 incluyendo caracteres especiales, mayúsculas, minúsculas y números	X		X		X		
7. Se logra registrar los accesos otorgados a los usuarios.	X		X		X		
8. Se usan los roles de acceso a los usuarios para los permisos que sean necesarios.	X		X		X		
DIMENSIÓN 2: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9. Cuentan con reglas de filtrado de paquetes para control del tráfico de red para prevenir ataques maliciosos	X		X		X		
10. Cuentan con algún firewall certificado para la seguridad de la red.	X		X		X		
11. Existe algún filtro para la transmisión de la información.	X		X		X		
12. Existe algún mecanismo de encriptación para el intercambio de información.	X		X		X		
13. Cuentan con procedimientos para el respaldo de los datos.	X		X		X		
14. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica.	X		X		X		
DIMENSIÓN 3: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
15. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulación no autorizada.	X		X		X		
16. Existe alguna medida de protección de acceso al centro de datos.	X		X		X		
17. Existe algún plan de contingencia contra desastres naturales.	X		X		X		
18. Existe alguna protección física contra ataques maliciosos o accidentes.	X		X		X		
19. Cuentan con protocolos para el acceso de terceros al área de TI.	X		X		X		
20. Existe alguna restricción para el ingreso de equipos tecnológicos al área de TI.	X		X		X		

[1] **Pertinencia:** el ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** el ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad:** se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

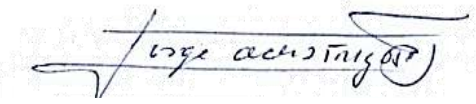
Nota. Suficiencia: se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:
Aplicable [X]
Aplicable después de corregir [ ]
No aplicable [ ]

Apellidos y nombres del juez validador: Cáceres Trigoso, Jorge Ernesto **DNI:** 07305972
Correo electrónico institucional:
Metodólogo [ ]
Temático [X]
Estadístico [ ]

Lima, 13 de enero del 2024



Firma del experto informante

Anexo 7: Informe de Turnitin.

Reporte de similitud

NOMBRE DEL TRABAJO	AUTOR
Tesis_Final._Cruz_Gamarra_V15.docx	Cruz_Gamarra Cruz_Gamarra

RECUENTO DE PALABRAS	RECUENTO DE CARACTERES
24779 Words	129049 Characters
RECUENTO DE PÁGINAS	**TAMAÑO DEL ARCHIVO**
136 Pages	12.0MB
FECHA DE ENTREGA	**FECHA DEL INFORME**
Jul 13, 2025 11:01 PM GMT-5	Jul 13, 2025 11:03 PM GMT-5

16% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 13% Base de datos de Internet
- 4% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 14% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 10 palabras)

Anexo 8: Desarrollo de las políticas del ISO 27001

Lan infotech

POLÍTICA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN DE LAN INFOTECH S.A.C

OBJETIVO

Dar a conocer las políticas y lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa Lan infotech S.A.C, necesarios para implementar los controles que seleccionamos en el Anexo A de la norma ISO 27001, los cuales permiten alcanzar los objetivos definidos para la seguridad de la información de la empresa.

ALCANCE.

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de Lan infotech S.A.C

Es para aplicar en toda la empresa o para toda persona que tenga relación con la misma.

Este documento de políticas de seguridad de la información está basado en los controles de acceso a las redes y servicios de red es fundamental para garantizar la protección de los datos y la prevención de posibles amenazas y ataques cibernéticos. Presentaremos algunos puntos importantes para tener presente:

1. Cumplir con los requisitos especificados en la Norma Técnica Peruana NTP-ISO/IEC 27001 para la ejecución del Sistema de Gestión de Seguridad de la Información. Asimismo, el SGSI podrá operar alineado a otras buenas prácticas y marcos de trabajo vigentes.
2. Establecer los objetivos generales del sistema de gestión de seguridad de la información, como la confidencialidad, integridad y disponibilidad de la información.
3. Establecer controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información. Esto puede incluir la implementación de autenticación de usuarios, gestión de contraseñas y control de acceso basado en roles.
4. Establecer medidas de seguridad física para proteger los activos de información, como el control de acceso a las instalaciones, la protección contra incendios y el resguardo de los equipos.
5. Proteger la información, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en normas de seguridad de la información, procedimientos asociados y en las recomendaciones dadas por el responsable de dicha información.
6. Establecer que todo/a colaborador/a y/o contratista sea responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información que custodia, asimismo, que rinda cuentas cuando sea solicitado.

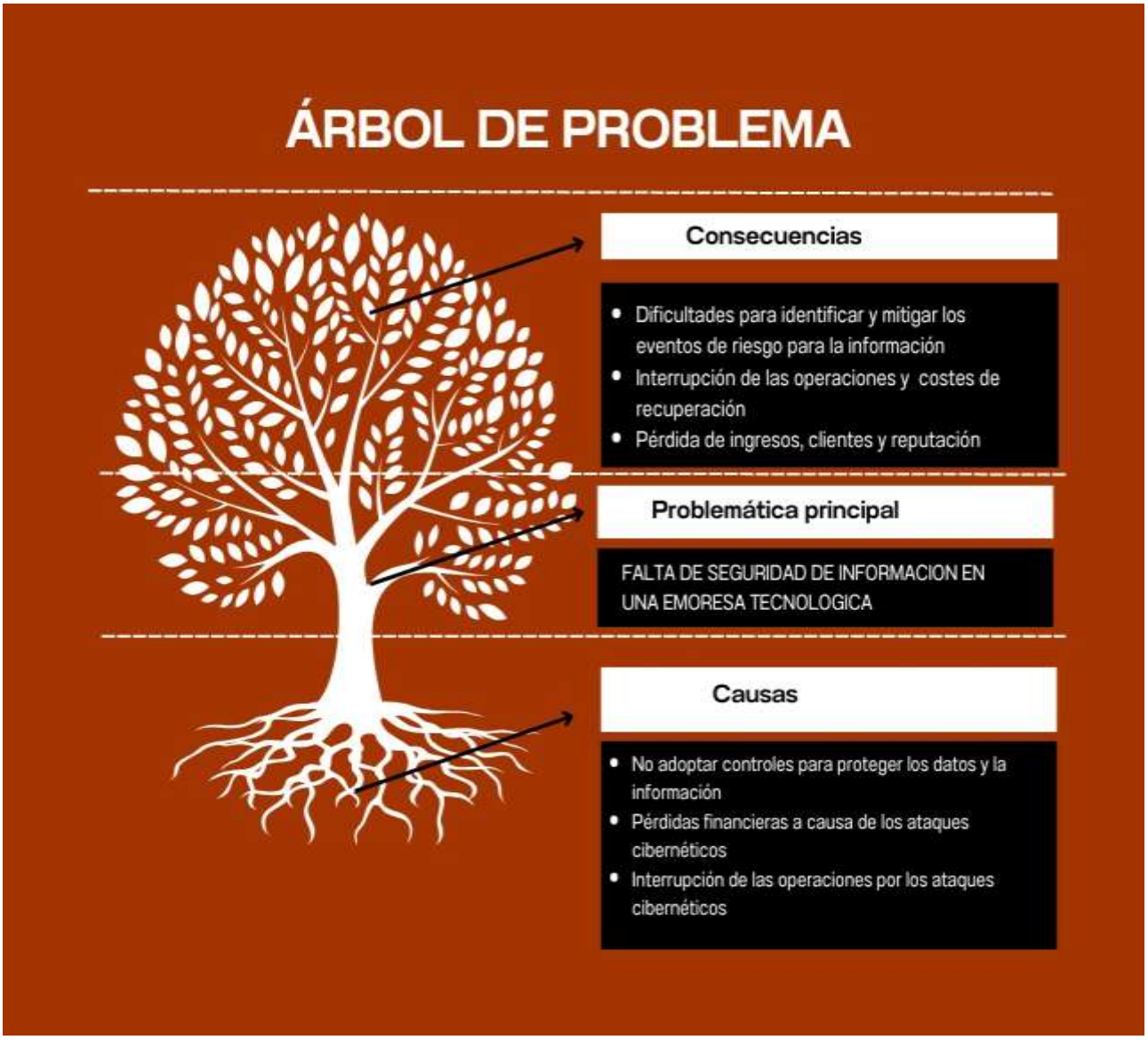
JAIME JESUS DIEZ CANSECO OLCAY
GERENTE GENERAL

Lan infotech

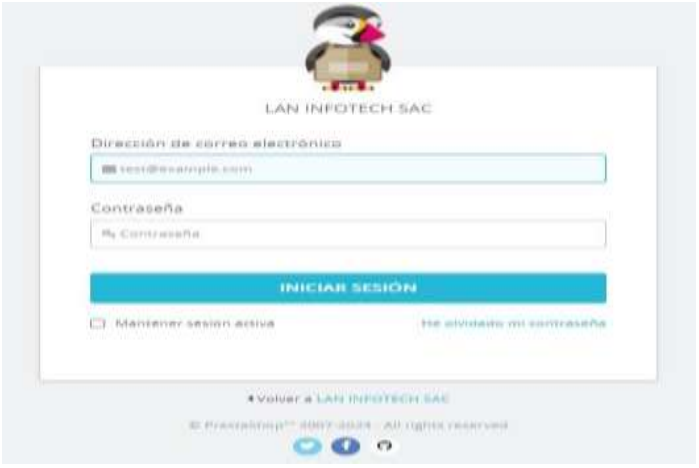
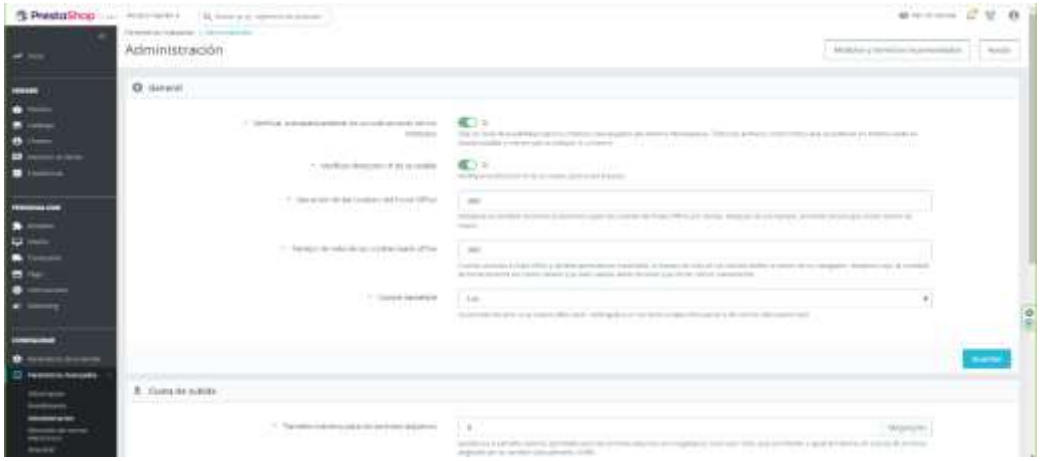
OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. Construir y consignar una cultura de seguridad de información dentro de la empresa
2. Tomar medidas para proteger la confidencialidad, la integridad y la disponibilidad de los datos de la Organización.
3. capacitar sobre buenas prácticas de seguridad, sensibilizar sobre los riesgos de seguridad y promover una cultura de seguridad en toda la organización.

Anexo 9: Árbol del problema



Anexo 10: Controles de seguridad de la información observados

Control: 9.1.2 Acceso a las redes y a los servicios de la red
1. Existe control de acceso con usuario y clave único, en base a roles para acceso diferenciados.
 En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa sí cuenta con la existencia del control de acceso con usuario y clave única.
2. Existen procedimientos de autorización para el acceso a la red.
 En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa ya cuenta con procedimientos de autorización del acceso a la red.

3. Se tiene un control de los dispositivos por cual se acceden a la red.

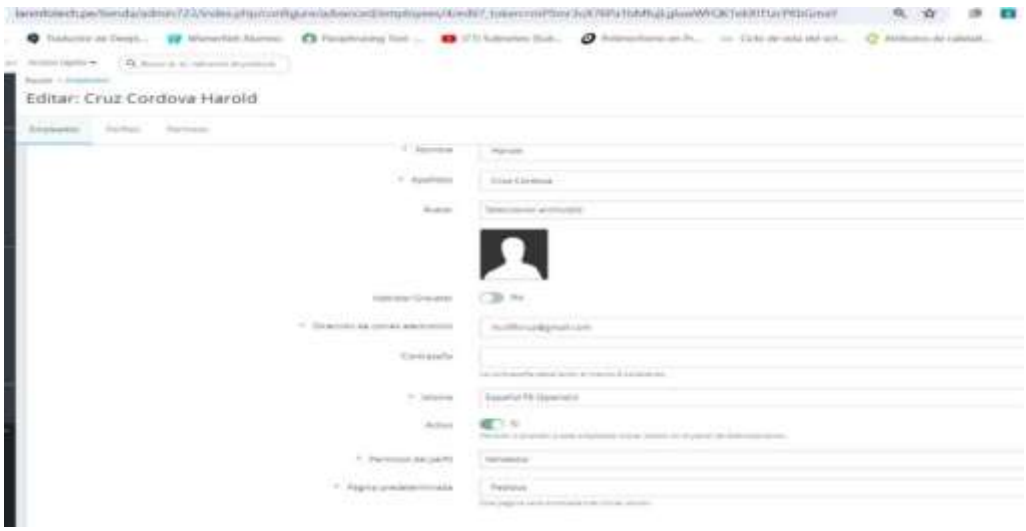
En la imagen que se muestra obtenida de la empresa en investigación, vemos que la empresa ya cuenta con un control de los dispositivos por lo cual se accede a la red.

Control: 9.2.1 Registro de usuarios y cancelación del registro

4. Se monitorea las actividades o intentos de acceso no autorizados de los usuarios.

En la imagen que se muestra obtenida de la empresa en investigación, vemos que la empresa ya cuenta con el monitoreo de las actividades de acceso no autorizado de los usuarios.

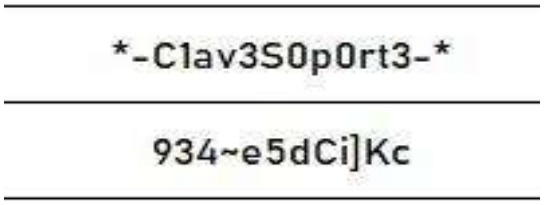
5. Se le da de baja a las cuentas de usuarios cuando el trabajador abandona la organización



En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con formas de monitoreo de accesos no autorizados, así mismo en la misma imagen nos indica que pueden dar de baja a el usuario de un trabajador cuando este se retira de la empresa.

Control: 9.2.2 Gestión de acceso a los usuarios

6. En la verificación de accesos cumplen con la longitud >8 a caracteres, incluyendo caracteres especiales, mayúsculas, minúsculas y números

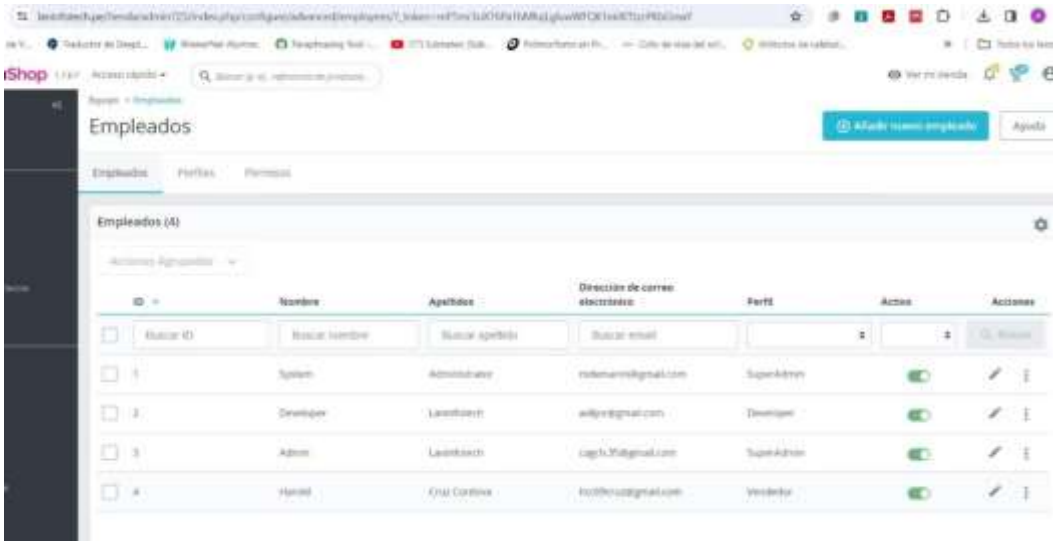


En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa ya cuenta con formas de verificación de acceso que cumplen con la longitud a 8 caracteres, conteniendo caracteres especiales, mayúsculas, minúsculas y números.

7. Se logra otorgar los accesos necesarios a los usuarios

En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con formas de otorgar los accesos a los usuarios, así mismo, en la misma imagen nos indica que pueden verificar los tipos de accesos que pueden contar los usuarios .

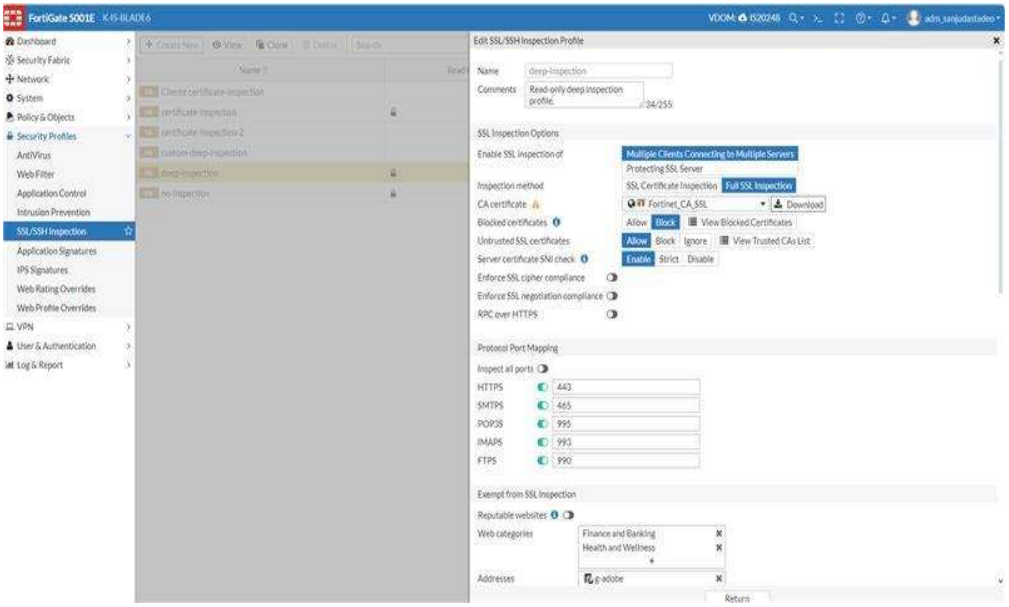
8. Se usan los roles de accesos a los usuarios para los permisos que sean necesarios



En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con la verificación de accesos, también podemos ver que se logra otorgar los accesos necesarios a los usuarios, así también como los roles de accesos a los usuarios y sus permisos.

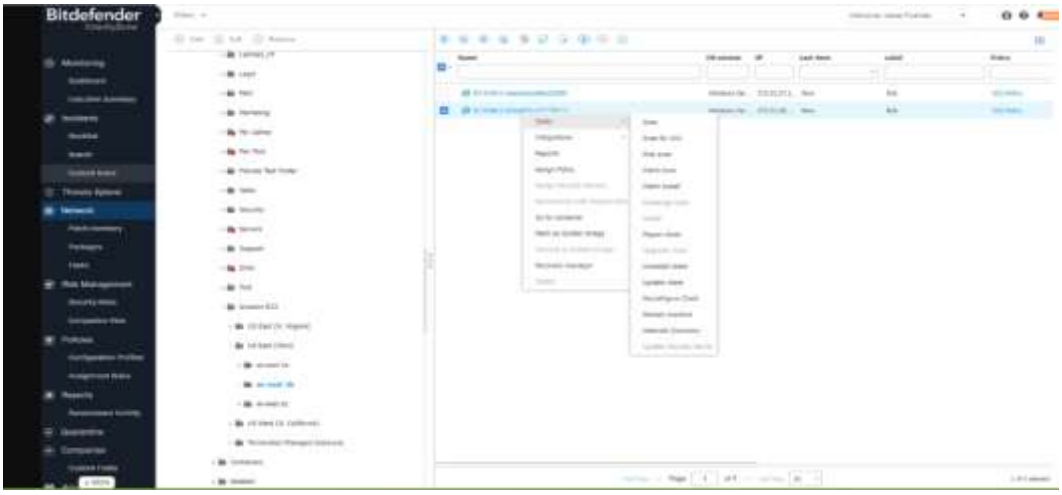
Control: 13.1.2 Seguridad de los servicios de red

9. Cuenta con reglas de filtrado de paquetes para control de tráfico de red y prevenir ataques maliciosos

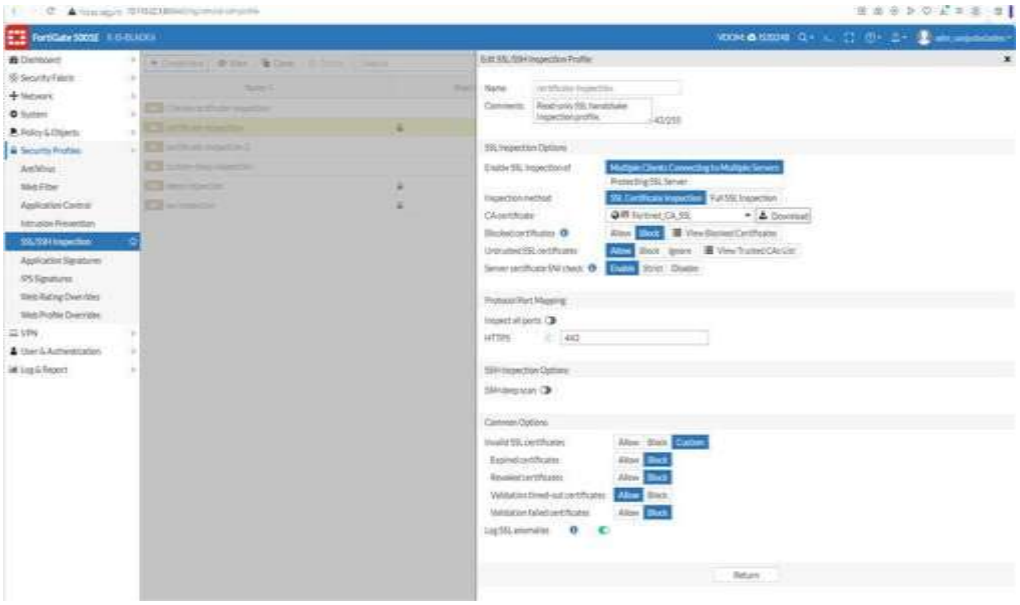
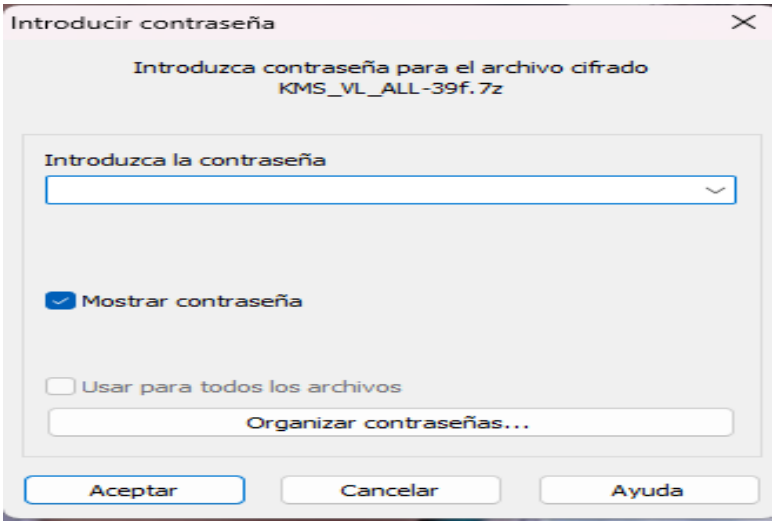


En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa ya cuenta con reglas de filtrado de paquetes para control de red y prevenir ataques maliciosos gracias al fortinet.

10. Cuentan con algún firewall para la seguridad de la red



En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con reglas de filtrado de paquetes para control de tráfico de red y prevenir ataques maliciosos y con un firewall para la seguridad de la red.

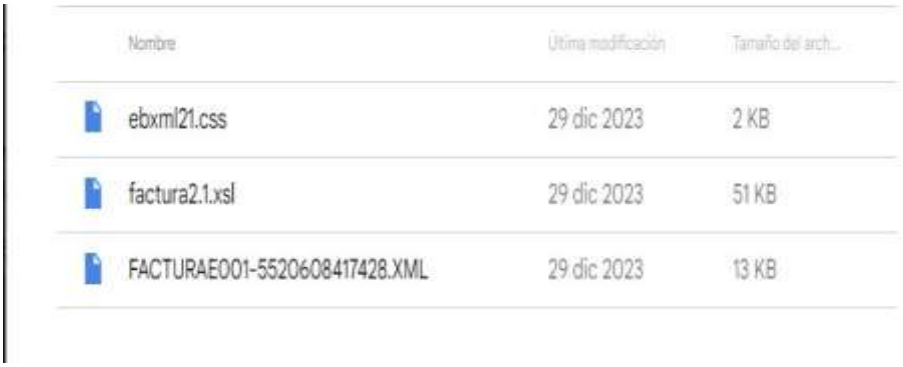
Control: 13.2.1 Políticas y procedimientos
11. Existe algún filtro para la transmisión de la información
 En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa ya cuenta con filtros para la transmisión de la información como es el fortine.
12. Existe algún mecanismo de encriptación para el intercambio de información
   En la imagen que se muestra obtenida de la empresa en investigación, vemos que la empresa ya cuenta con mecanismos de encriptación de la información para el intercambio de la misma.

13. Cuentan con procedimientos para el respaldo de datos

En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con filtro para la transmisión de la información, también vemos que cuentan con mecanismo de encriptación y con procedimientos para el respaldo de datos.

Control: 13.2.2 Acuerdos de intercambio de información

14. Existen formatos certificados para el intercambio de información con el caso de boleta electrónica



En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa sí cuenta con formatos certificados para el intercambio de información con el caso de boleta electrónica.

Control: 11.1.1 Perímetro de seguridad física

15. Se cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulaciones no autorizada

En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con medidas para proteger los equipos y dispositivos físicos contra daños o manipulaciones no autorizadas como son los escritorios y demás artículos de protección correspondientes.

16. Existe alguna medida que restringe el acceso al centro de datos

En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con una medida que restringe el acceso al centro de datos

Control: 11.1.4 protección contra amenazas externas y del ambiente

17. Existe algún plan de contingencia contra desastres naturales

En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa si cuenta con un plan de contingencia contra desastres naturales

18. Existe alguna protección física contra ataques maliciosos o accidentes

En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa sí cuenta con una protección física contra ataques maliciosos o accidentes.

Control 11.1.5 El trabajo en las Áreas seguras

19. Cuentan con protocolos para el acceso de terceros al área de TI

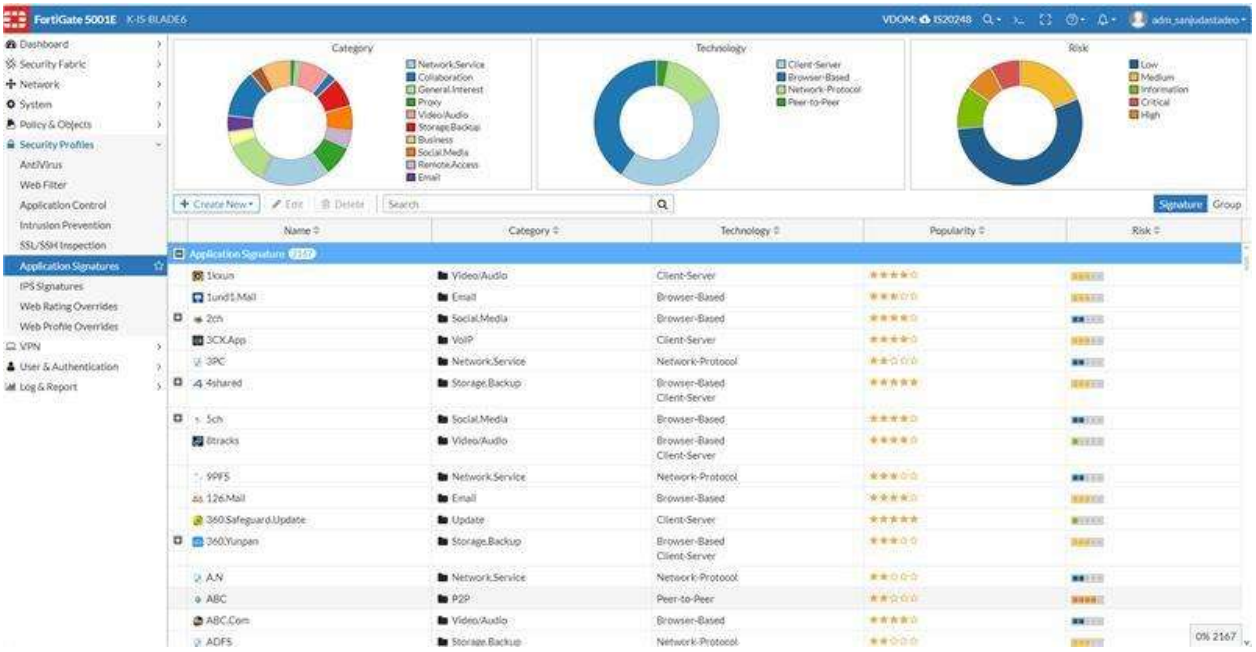
En la imagen que se muestra obtenida de la página de la empresa en investigación, vemos que la empresa sí cuenta con protocolos para el acceso de terceros al área de TI.

20. Existen alguna restricción para el ingreso de equipos tecnológicos al área de TI

.

En la imagen que se muestra obtenida de la empresa en investigación, vemos que la empresa ya cuenta con restricciones para el ingreso de equipos tecnológicos al área de TI.

Figura 7 ***Imagen de filtrado de Información "Fortinet"***



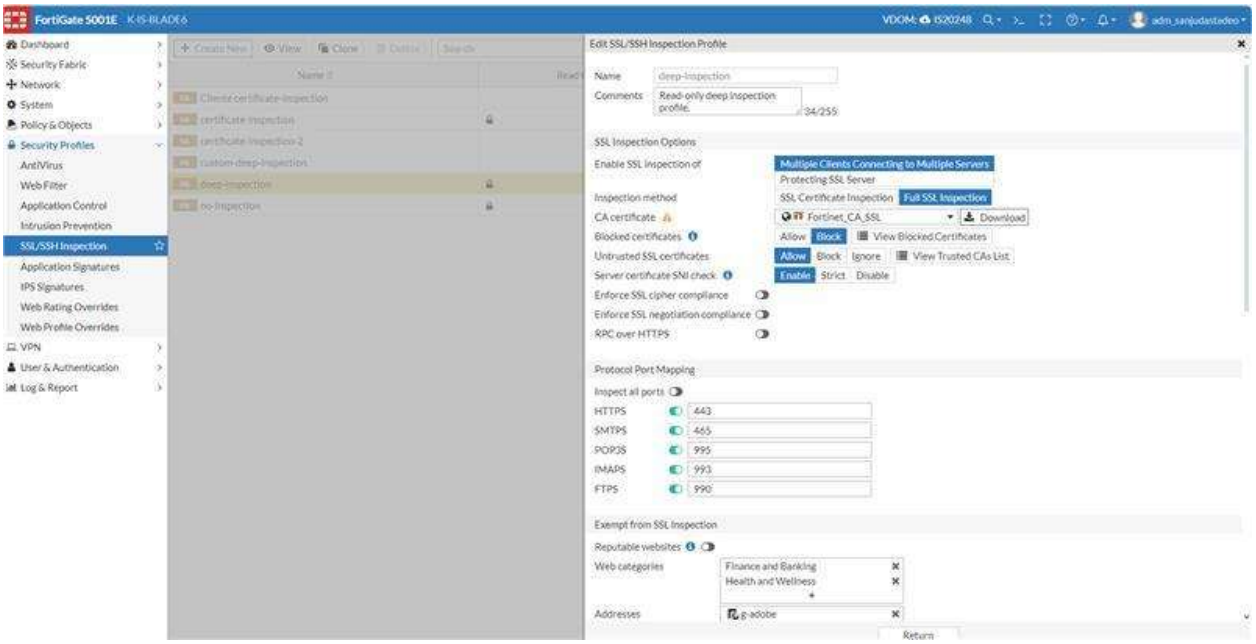


Figura 8 Imagen de La seguridad física de la empresa tecnológica

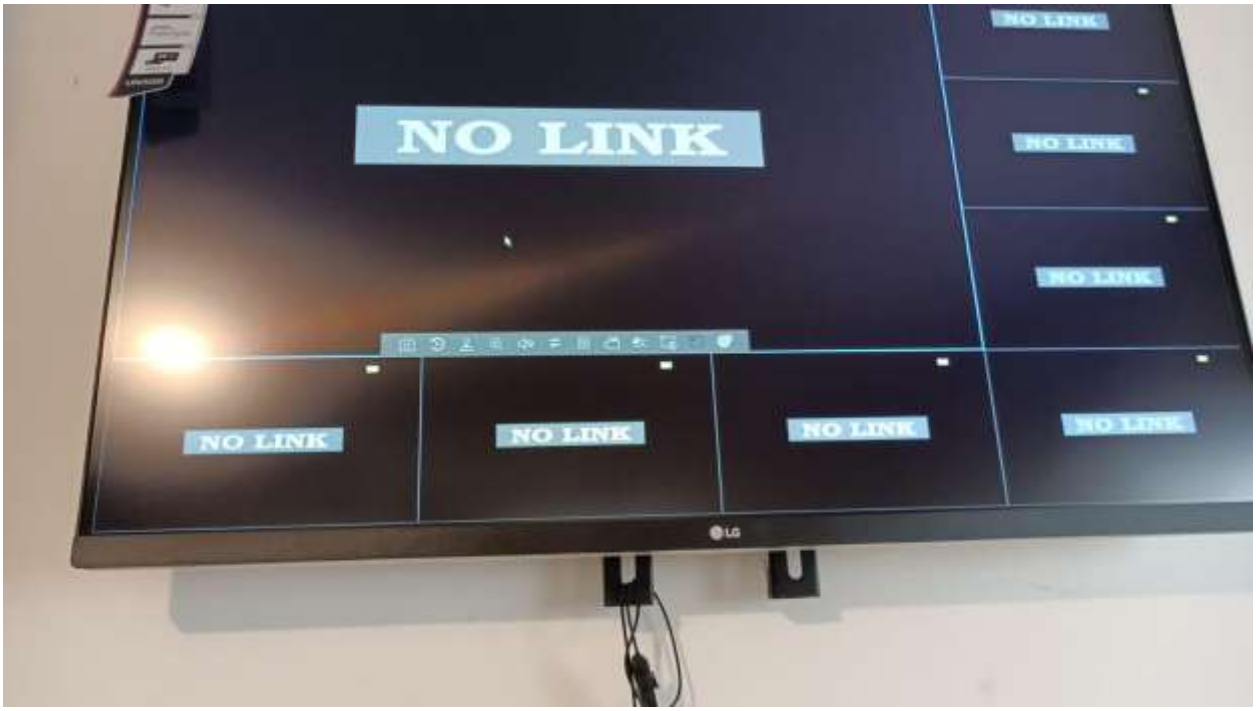


Figura 9 Control de acceso y roles de usuarios

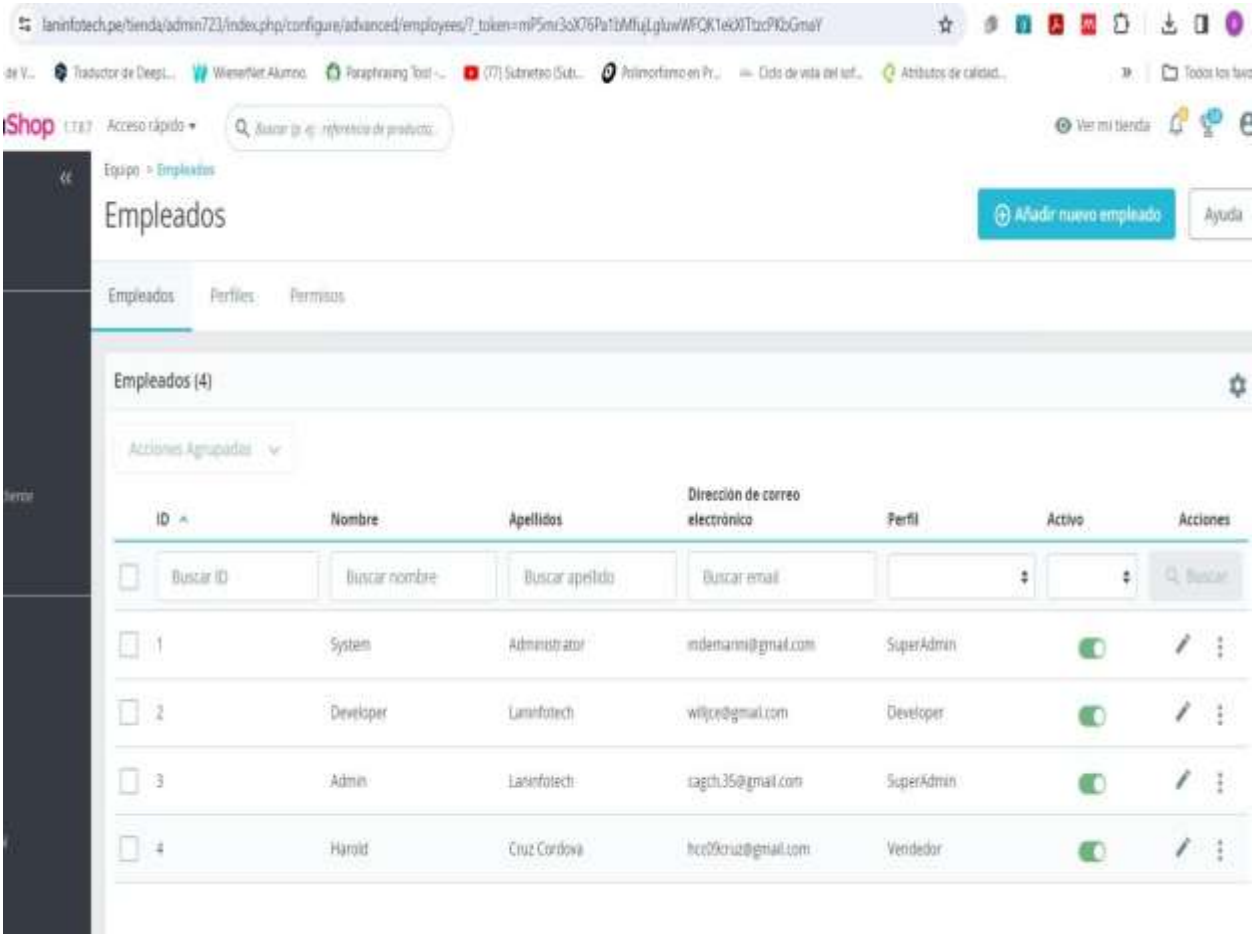


Figura 10 Registros de usuarios

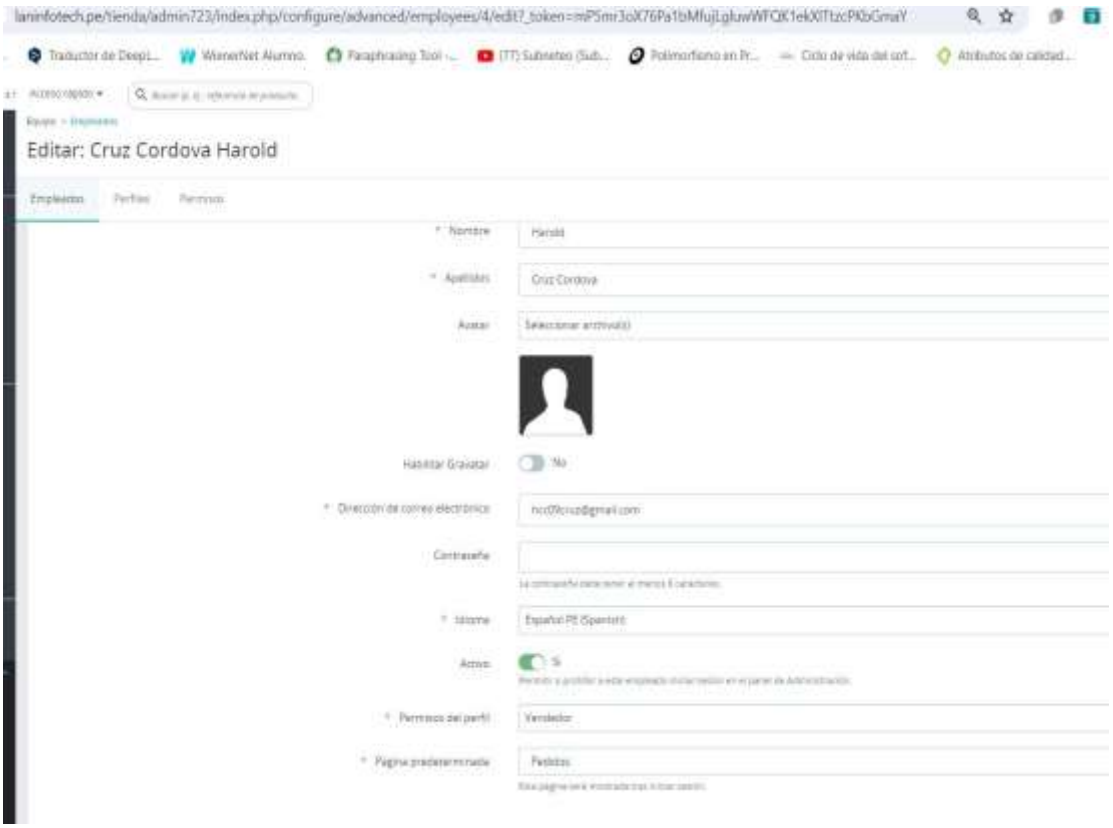
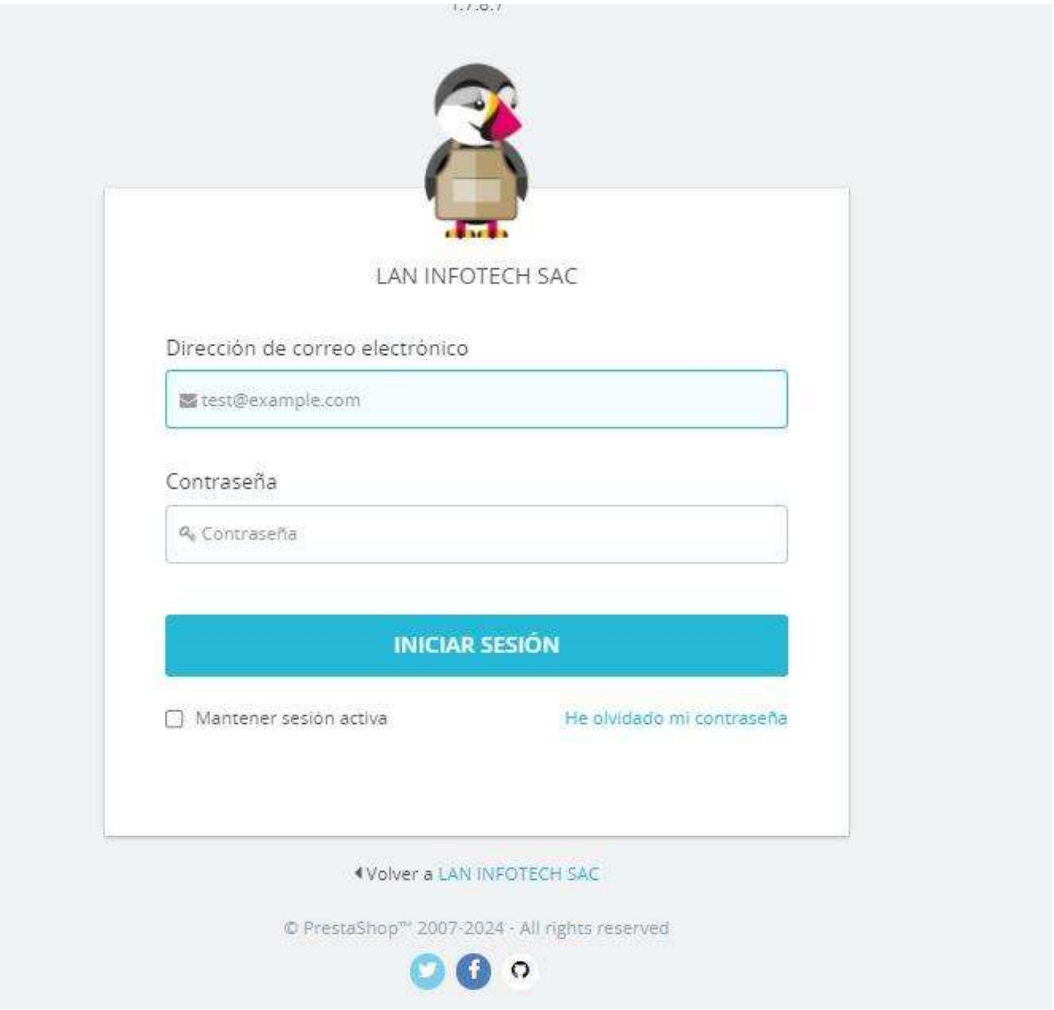


Figura 11 Verificación de accesos de usuarios



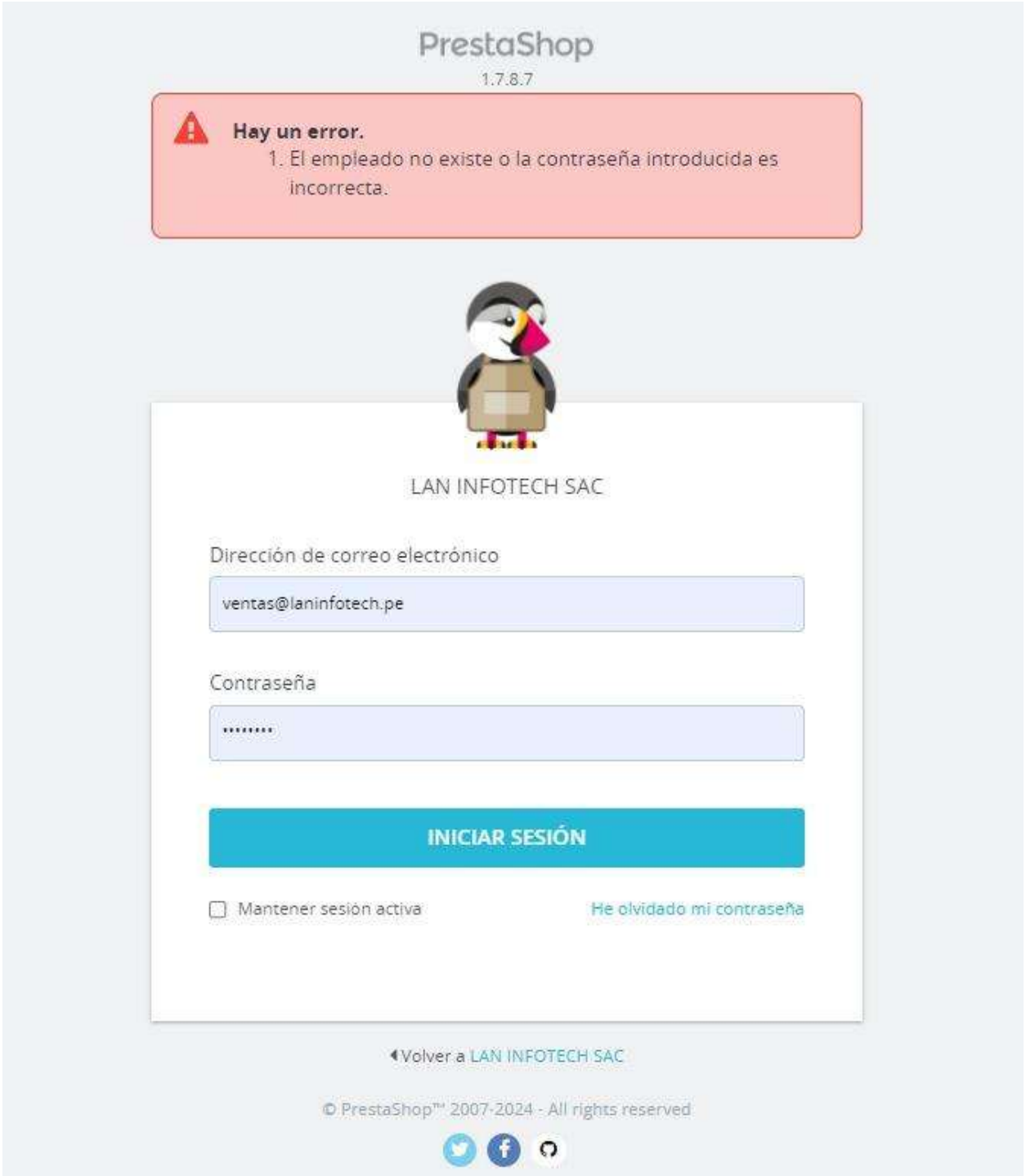

PrestaShop
1.7.8.7
Hay un error.
1. El empleado no existe o la contraseña introducida es incorrecta.
LAN INFOTECH SAC
Dirección de correo electrónico
ventas@laninfotech.pe
Contraseña
INICIAR SESIÓN
Mantener sesión activa
He olvidado mi contraseña
Volver a LAN INFOTECH SAC
© PrestaShop™ 2007-2024 - All rights reserved

Figura 12 Controles de los accesos de terceros

17% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

13% Fuentes de Internet
4% Publicaciones
14% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Texto oculto
169 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

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

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

Fuentes principales

13% Fuentes de Internet
4% Publicaciones
14% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1 Internet
repositorio.uwiener.edu.pe 3%

2 Trabajos entregados
Submitted on 1687209244651 2%

3 Internet
repositorio.unjfsc.edu.pe <1%

4 Internet
repositorio.uta.edu.ec <1%

5 Trabajos entregados
Universidad Cesar Vallejo on 2025-11-02 <1%

6 Internet
repositorio.ucv.edu.pe <1%

7 Internet
www.coursehero.com <1%

8 Internet
www.fadmon.unal.edu.co <1%

9 Trabajos entregados
Vel Tech University on 2023-12-08 <1%

10 Trabajos entregados
Submitted on 1688424302212 <1%

11 Trabajos entregados
Universidad Nacional Abierta y a Distancia, UNAD,UNAD on 2021-05-23 <1%