FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍAS

Tesis

ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024

Presentado por

Autor: De La Cruz Santa Cruz, Claudia

Código ORCID: 0000-0003-0772-4848

Asesor: Dra. Díaz Reátegui, Mónica

Código ORCID: https://orcid.org/0000-0003-4506-7383

Línea de investigación general

Sociedad y transformación digital

Línea de investigación específica

Gestión, negocios y tecno ciencia

Lima, Perú

2024

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

Yo, Claudia De La Cruz Santa Cruz, egresada de la Facultad de Ingeniería y Negocios de la Escuela Académico Profesional de Ingenierías de la Universidad Privada Norbert Wiener, declaro que el trabajo académico "ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024", asesorado por la docente: Dra. Mónica Díaz Reátegui con DNI: 09537647 y con ORCID: 0000-0003-4506-7383, tiene un índice de similitud de 16 (dieciséis) % con código oid: 14912:348014528, 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 pueda ser revisado en búsqueda de plagios
4. El porcentaje señalado es el mismo que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual, me someto a lo dispuesto en las normas del reglamento vigente de la universidad.

Claudia De La Cruz Santa Cruz
DNI: 42922226

Dra. Mónica Díaz Reátegui
DNI: 09537647

Lima, 17 de abril de 2024

ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024

Asesor metodológico

Dr. Flores Zafra, David (**ORCID:** 0000-0001-5846-325X)

Asesor temático

Dra. Mónica Díaz Reátegui (**ORCID:** 0000-0003-4506-7383)

Agradecimiento

Estoy agradecida principalmente con Dios, por iluminar día a día mis pasos para seguir forjando mi camino profesional. A mis padres a quienes honro y agradezco, puesto que, con su dedicación y amor, han formado las bases de mis objetivos.

Dedicatoria

Este proyecto está dedicado para ti, *Abril*, por creer siempre en mí, por tu amor puro e infinito y porque cada día soy mejor por ti amada hija.

Índice

Pág.

Índice de tablas

Pág.

Índice de figuras

Pág.

Resumen

Toda organización debería controlar la seguridad de su información, definiendo un protocolo para responder ante ciberataques. El propósito de esta investigación fue determinar que la implementación de la “ISO 27001” mejora el sistema de gestión de seguridad de la información en una empresa de servicios. Para tal efecto, este estudio fue experimental, con enfoque cuantitativo y de tipo de investigación aplicada, siguiendo la línea de los métodos deductivos, hipotéticos y analíticos.

En referencia a la población, esta fue compuesta por 114 controles extraídos de la norma “ISO 27001”, con una muestra aproximada de 20 controles. Se aplicó la técnica de observación y el instrumento fue la ficha de observación. Con el fin de implementar la “ISO 27001”, se empleó los controles del ANEXO A, a su vez, se empleó como referencia la “ISO 27002”, añadido a ello, se aplicó el ciclo PHVA para la mejora continua de las políticas de seguridad de la información. Se empleó la estadística inferencial aplicando la prueba Wilcoxon puesto que, se presentan indicadores no paramétricos.

Los resultados determinaron que al implementar la “ISO 27001” mejora el sistema de gestión de seguridad de la información, reduciendo la tasa de incidentes que impacta la confidencialidad en un 99%, la tasa de incidentes que impacta la integridad en un 99% y la tasa de incidentes que impacta la disponibilidad en un 99%.

Palabras clave: ISO 27001, SGSI, Sistema de gestión de la seguridad de la información, confidencialidad, integridad y disponibilidad.

Abstract

Every organization should control the security of its information, defining a protocol to respond to cyber attacks. The purpose of this research was to determine that the implementation of "ISO 27001" improves the information security management system in a service company. For this purpose, this study was experimental, with a quantitative approach and applied research type, following the line of deductive, hypothetical and analytical methods.

In reference to the population, it was composed of 114 controls extracted from the "ISO 27001" standard, with an approximate sample of 20 controls. The observation technique was applied and the instrument was the observation sheet. In order to implement "ISO 27001", the controls in ANNEX A were implemented, in turn, "ISO 27002" was implemented as a reference, in addition to this, the PHVA cycle was applied for the continuous improvement of safety policies. security of the information. Inferential statistics were used by applying the Wilcoxon test since non-parametric indicators are presented.

The results determine that by implementing "ISO 27001" the information security management system improves, reducing the rate of incidents that impact confidentiality by 99%, the rate of incidents that impact integrity by 99% and the incident rate that impacts availability by 99%.

Keywords: ISO 27001, ISMS, Information security management system, confidentiality, integrity and availability.

Introducción

Hoy en día la ciberdelincuencia crece a nivel global, puesto que, los ciberdelincuentes son cada vez más ágiles usando diversas ciberamenazas para dañar la seguridad de los datos, es por ello, que la "ISO 27001" permitió la mejora del sistema de gestión de la seguridad de la información (SGSI) en la empresa de servicios, para asegurar los activos de la información. A continuación, se describen los 5 capítulos:

En el **Capítulo I,** se explica cómo se planteó el problema y los objetivos del estudio. Asimismo, explica la justificación teórica, metodológica y práctica.

Asimismo, en el **Capítulo II, s**e desarrolla el marco teórico, en el cual, se explican los antecedentes nacionales e internacionales. Se emplearon teorías y conceptos que sustentan la investigación para ambas variables en las bases teóricas. Finalmente, se crearon hipótesis generales y específicas para la investigación.

Igualmente, en el **Capítulo III,** se explica la metodología, en el cual, explica el enfoque, método, diseño, tipo, población y muestra. Luego, se ejecutó la operacionalización de las variables. Para la constatar la validez y confiabilidad, se empleó técnicas e instrumentos. Finalmente, se detalla el proceso y el análisis de datos, y se resaltan los aspectos éticos empleados.

De la misma manera, en el **Capítulo IV,** se desarrolla el análisis descriptivo. Luego, se realizaron pruebas de consistencia, normalidad y de contraste para las hipótesis. Finalmente, se compararon los resultados alcanzados.

De igual forma, en el **Capítulo V,** se desarrollan las conclusiones y recomendaciones, al detalle para la empresa.

Se adjunta finalmente, las referencias y anexos.

CAPÍTULO I: EL PROBLEMA

1.1 Planteamiento del problema

Actualmente, implementar la norma “ISO 27001” en empresas de servicio ayuda a establecer un marco sólido para asegurar sus activos. A su vez, un Sistema de Gestión de la Seguridad de la Información (SGSI), conduce al aseguramiento de datos críticos y aumentar la productividad de las operaciones. En ese contexto, el SGSI ha sido definido por la “ISO 27001” como el fragmento de un gestor global, basado en un alcance de riesgo de negocio, que determina, implementa, actúa, supervisa, analiza, conserva y mejora la protección de datos (Watkins, 2022). Por ello, la aplicación del sistema de seguridad garantiza a las organizaciones el control de cambios planificados y la revisión del efecto de las alteraciones indeseables, además, permite tomar medidas con el fin de mitigar efectos adversos (ISO/IEC, 2022).

En Europa, se observa una baja tasa de certificaciones “ISO 27001”, como es en el caso de Andorra, que tiene solo una certificación “ISO 27001” en comparación a Estados Unidos que tiene 1,090 certificaciones (Global Standards, 2022). En ese contexto, Europa ha sufrido reiterados ataques cibernéticos, debido a la falta de seguridad en sus sistemas, causando diversos problemas como son la encriptación y bloqueo de archivos y como consecuencia, el colapso de muchas empresas e instituciones (Del Villar, 2021). A nivel de Latinoamérica, el Banco Interamericano de Desarrollo (2020), informó sobre el estado de la ciberseguridad, en el que señala que solo el 7% de las entidades públicas y el 5% de las empresas privadas han implementado la norma “ISO 27001”, lo que evidencia una escasa adopción de medidas de seguridad. En esa línea, los problemas en materia de seguridad informática identificados son los troyanos bancarios, intentos de phishing dirigidos a datos financieros, publicidad no deseada, aplicaciones rastreadoras de individuos y aplicativos que bloquean el dispositivo de la víctima (Valbuena, 2023). A nivel de Perú, se detecta

la carencia de compromiso para cumplir con el uso de la “ISO 27001”, lo que conlleva a ser el cuarto país con más problemas de seguridad informática, estos problemas son el fraude cibernético, ataques de ransomware, intentos de phishing, entre otros, es por ello, que se debe considerar un plan de aseguramiento de información (Revista Economía, 2023). A nivel local, la empresa Nipón Business S.A.C no implementó la norma “ISO 27001”, por ende, dicha entidad no garantiza la disponibilidad y continuidad de sus servicios informáticos, a su vez, ello aumenta el riesgo de interrupciones, la pérdida de datos de clientes, de historias clínicas y de colaboradores de dicha empresa. Por todo lo mencionado, se demuestra que, en Lima no se podría enfrentar adecuadamente las amenazas cibernéticas, ya que, existe poco interés en resguardar la información de sus negocios. Es por ello que, las empresas deben tomar conocimiento sobre cómo proteger su información, recursos físicos y sistemas digitales, de ese modo, el servicio será continuo y eficiente, implementando dicha herramienta para la protección contra ataques no intencionados y salvaguardar sus activos.

Los SGSI son importantes para todo tipo de organización, ya que garantizan la privacidad de los datos y reducen los costos. Sin embargo, la carencia de personal capacitado y la carencia de liderazgo en la alta gerencia son los principales problemas que enfrentan las empresas de servicios al implementar un SGSI. En Europa, por ejemplo, se ha impulsado el uso de modelos cimentados en calificaciones (rating) de seguridad como una parte y una integración de los sistemas de certificaciones actualmente existentes (Carpio, 2021). En Latinoamérica, los resultados del informe desarrollado por ESET (2023), se observa que, en el último año, el 69% de las organizaciones de América Latina experimentaron algún incidente de seguridad. En el caso específico del Perú, se desarrolló una norma enfocada a la seguridad de información y ciberseguridad, que maximice la garantía de la continuidad de actividades (El Peruano, 2021). En

ese contexto, a nivel de Lima, se observa que la empresa en estudio desconoce la importancia de concientizar y promover las buenas y mejores prácticas en cuanto a la protección de información, por lo que, al estar en dicha situación los ciberdelincuentes aprovecharían aquellas debilidades y ejecutarían diversos tipos de ciberataques atentando la información del negocio.

Al no aplicar la "ISO 27001" y un SGSI, se van a presentar diversos problemas en las organizaciones que busquen asegurar su información, por ende, este desafío se presenta en diferentes niveles geográficos. A nivel de Europa, Cambridge Analytica demostró cómo el robo de datos puede ser usado en política con el fin de aprender los patrones de los cibernautas y usarlos para propaganda política, es por ello que, es relevante regirse por normativas como la "ISO 27001" (Russo, 2023). A nivel de Latinoamérica, en Brasil, los ciberataques se incrementaron a un 400% desde el COVID-19, en vista que la población trabajaba desde casa y el marco de seguridad no contemplaba esa realidad, lo cual, afectó a la reputación de varias organizaciones, a la protección de sus activos, al aseguramiento de data delicada de sus consumidores, trabajadores y socios, es por ello que se optó por implementar la actualización de la norma "ISO 27001" ya que es más precisa contra las vulnerabilidades de hoy en día (El Economista, 2022). A nivel de Perú, se ha identificado que las empresas no cuentan con la implementación ni la certificación de la norma "ISO 27001", por ende, se entiende que las organizaciones públicas están trabajando en entornos de alto riesgo, donde podrán sufrir pérdidas de información relevante, afectar procesos, personas y tecnología (Crespo, 2017). En ese sentido, se evidencia que las organizaciones en el Perú aún no toman conciencia de la relevancia del uso de dicha herramienta para resguardar su información.

En referencia a la problemática local que ocurre en la consultoría Nipón Business, se usó la herramienta árbol de problemas (ver figura 1), los problemas que resaltan son: (i) **falta de políticas de seguridad**, a causa de la carencia de un SGSI, lo cual implica que, no existen

medidas para asegurar los datos, como políticas, controles, procedimientos, auditorías o planes de contingencia; (ii) **falta de control de acceso de seguridad**, debido a que no se cuenta con un SGSI implementado que garantice la tríada CID para el aseguramiento de datos que se maneja, ello puede dañar el prestigio de la entidad; (iii) **falta de copias de seguridad**, a causa de no contar con un SGSI, podría provocar la pérdida, alteración o divulgación de datos sensibles, ello puede tener consecuencias negativas tanto legales como operativas; (iv) **falta de protección contra el malware**, a causa de la falta de un SGSI, lo cual implica que, que la empresa estaría expuesta a diversas amenazas, ello conlleva a comprometer el aseguramiento de activos y la continuidad de actividades; (v) **falta de mantenimiento de equipos**, a causa de no contar con un SGSI, se puede sufrir problemas de seguridad, rendimiento y cumplimiento normativo, ello aumenta el riesgo de avería de equipos; (vi) **falta de inventario de activos**, a causa de no contar con un SGSI, no habría control adecuado sobre los recursos que se utilizan para proteger la información, lo cual, imposibilita aplicar medidas de seguridad adecuadas para cada activo. En caso no se resuelva ningún problema mencionado, las consecuencias que se presentarían serían las siguientes: (i) pérdida de reputación e incumplimiento normativo legal, debido a los ataques cibernéticos que causaron la fuga de datos delicados tanto de clientes, proveedores y de la organización; (ii) pérdida de datos sensibles y vulnerabilidades de seguridad, ello ocurre por la fuga de información, los ciberataques, los errores humanos, entre otras causas; (iii) rendimiento deficiente y falta de visibilidad y control, a causa de no contar con un inventario en el que se identifique, clasifique, valore y ubiquen los equipos.

Figura 1

Árbol de problemas.

1.2 Formulación del problema

1.2.1 Problema general

¿De qué manera la implementación de la ISO 27001 mejora el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?

1.2.2 Problemas específicos

PE1: ¿De qué manera la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la disponibilidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?

PE2: ¿De qué manera la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la integridad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?

PE3: ¿De qué manera la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?

1.3 Objetivos de la investigación

1.3.1 Objetivo general

Determinar que la implementación de la ISO 27001 mejora el sistema de gestión de Seguridad de la información en una empresa de servicios, Lima 2024.

1.3.2 Objetivos específicos

OE1: Determinar que la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la disponibilidad de la información en el Sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.

OE2: Determinar que la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la integridad de la información en el Sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.

OE3: Determinar que la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de Seguridad de la información en una empresa de servicios, Lima 2024.

1.4 Justificación de la investigación

El presente proyecto se efectuó para contribuir con información relevante para los futuros estudios enfocados en la aplicación de la ISO27001 para mejorar el SGSI de empresas de servicios, con el fin de proteger la CID de la información.

1.4.1 Teórica

Para este proyecto se tomó como apoyo teórico, dos teorías para cada variable. Para la variable ISO 27001, la respalda la **teoría de la gestión de la calidad**, puesto que, se basa en el ciclo de Deming o PHVA (Planificar, Hacer, Verificar, Actuar), con el que se optimiza el uso de recursos, se garantiza la fidelidad, ofrece protección, mide la eficiencia de procedimientos y

controles y corrige las no conformidades que puedan surgir (Menéndez, 2023). Asimismo, la respalda la **teoría de la ISO 27001**, puesto que la misma Organización Internacional de Normalización (ISO) la aprobó y publicó, otorgando así un marco para implementar y gestionar eficazmente la seguridad de la información en una organización (ISO/IEC, 2013). Para la variable sistema de gestión de la seguridad, la respalda **la teoría de la información**, puesto que, se centra en la medición y representación de la información, las leyes matemáticas que regulan la capacidad de los sistemas de comunicación para transmitir y procesar información (Jiménez, 1995). Seguidamente, la sostiene la **teoría general de sistemas**, ya que, es un enfoque de gestión empresarial que se concentra en optimizar la calidad tanto de productos como de servicios de un negocio (Bertalanffy, 1976).

1.4.2 Metodológica

El enfoque fue cuantitativo, con diseño experimental, puesto que, la aplicación del SGSI según la norma "ISO 27001" permitió alcanzar el objetivo del proyecto. Asimismo, este proyecto contribuyó a que aspirantes a investigadores del tema, puedan contar con la visión del empleo de estadísticas e instrumentos con el fin de identificar los riesgos y amenazas.

1.4.3 Práctica

Este proyecto consistió en aplicar un SGSI empleando seis controles de la "ISO 27001". logrando definir políticas de control de acceso a los sistemas y aplicaciones, restringiendo el acceso a la información, realizando respaldo de la información, definiendo controles contra códigos maliciosos, realizando el inventario de activos y realizando el mantenimiento de los equipos de la empresa en estudio. Finalmente, este sistema ayudó a mejorar la seguridad de la información de la empresa Nipón Business S.A.C.

1.5 Limitaciones de la investigación

Existió una demora por parte de la gerencia general respecto a la entrega de documentos firmados, sin embargo, luego la empresa emitió el documento esperado. Asimismo, se evidenció la ausencia de usuarios para realizar el test de cumplimiento de controles, no obstante, después se logró la reunión con los usuarios y se obtuvo la información deseada.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la investigación

Antecedentes nacionales

Aleman (2023), en su investigación llevada a la práctica en Lima, tuvo como objetivo "determinar en qué medida influye la implementación de la norma "ISO 27001:2013" en el control de seguridad de la información en una consultoría privada". En ese contexto, la metodología que se utilizó fue de tipo aplicada, de naturaleza cuantitativa y de diseño experimental. La población y la muestra estaban constituidas por un total de 78 trabajadores. La técnica utilizada fue la recolección de datos, por lo cual, el instrumento para recolectar información fue la encuesta. Asimismo, para el fragmento estadístico se utilizó la prueba de rangos de Wilcoxon, en el que se observó que para la disponibilidad de la información, el valor de sig. fue 0,000, menor de 0.05, por lo cual, se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1, para la adaptabilidad de la información, el valor de sig. fue 0,000, menor de 0.05, por lo cual, se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1, para la accesibilidad de la información el valor de sig. fue 0,000, menor de 0.05, por lo cual, se rechaza la hipótesis nula H0 y se acepta la hipótesis alternativa H1. El resultado demostró, que la norma brinda una óptima gestión de la disponibilidad de la información al tener un desempeño del 13,0385 % al 87,3718 %. Se concluye que existe una importante mejora en el control de la adaptabilidad, información, accesibilidad, disponibilidad y resguardo con la implementación de la norma "ISO 27001".

Asqui (2023), en su investigación llevada a cabo en Lima tuvo como objetivo "demostrar cómo la "ISO 27001" mejora la seguridad de la información en una empresa de servicios". En ese sentido, se implementó la metodología de investigación aplicada, con enfoque cuantitativo y

diseño de tipo experimental. La población está compuesta por 22 controles y la muestra por 20 controles de seguridad. La técnica utilizada fue la técnica de la observación, por lo tanto, el instrumento para la recolección de información fue la guía de observación. Asimismo, para el fragmento estadístico se utilizó la prueba T-Student, donde se apreció que el valor Sig. es 0.000 en la tasa de incidentes que afectan la confidencialidad, para la tasa de incidentes que afectan la integridad es 0.025 y para la tasa de incidentes que afectan la disponibilidad es 0.000. El resultado arrojó el 61.64% en referencia a la reducción de la tasa de incidentes que afectan a la disponibilidad, el 61.38% que corresponde a la reducción de la tasa de incidentes que afectan la confidencialidad y el 61.73% que corresponde a la reducción de la tasa de incidentes que afectan la integridad. Se concluye que, la implementación de la norma "ISO 27001", mejoró satisfactoriamente la disponibilidad, confidencialidad e integridad de la información de la institución.

Cerezo (2022), en su investigación llevada a cabo en Trujillo, tuvo como objetivo "mejorar la gestión de la seguridad de la información en una empresa de servicios implementando la norma "ISO 27001". En ese mismo contexto, la metodología que se utilizó para el estudio fue el enfoque cuantitativo, con tipo de investigación experimental y de diseño investigativo de tipo preexperimental. La población tomada fue de componentes de la infraestructura IT resultando así en 50 equipos y la muestra fue de 45 componentes. La técnica empleada fue la observación, por lo cual se usaron guías de observación para la recopilación de información. Asimismo, para el fragmento estadístico se utilizó la prueba de rangos de Wilcoxon, en el que se presenta el análisis a los indicadores tasa de vulnerabilidades, tiempo de implementación y tiempo de detección, con valor de significancia de 0,026, 0,001 y 0,000 respectivamente, la prueba T-Students se aplicó al indicador 3, el cual, el contraste de su media

tuvo un valor de significancia de 0,200. Por ello, se rechazaron las hipótesis nulas H0 y se aceptaron las hipótesis alternativas H1. En esa línea, los resultados arrojaron que la evaluación de seguridad informática logró reducir la tasa de vulnerabilidades en un 13,55 %, el tiempo de implementación en un 5,65 % y el tiempo de detección en un 11,97 %. Para finalizar, se concluye que la implementación de la norma "ISO 27001" mejoró la competitividad y el valor comercial de la empresa.

Porras (2019), en su investigación llevada a cabo en Huancayo, tuvo como objetivo "determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riegos en activos de información en una empresa de servicios". En ese sentido, la metodología que se usó fue de tipo aplicada y con diseño experimental. La población tomada fue de 114 controles del Anexo A de la "ISO 27001" y la muestra de 70 controles. La técnica empleada fue la observación, por lo cual se usaron guías de observación para la recopilación de información. A su vez, para el fragmento estadístico se utilizó la prueba de rangos de Wilcoxon en el que, el nivel de significación de los controles de seguridad físicos es de 0,16, para los controles de seguridad lógicos es 0,00 y para los controles de seguridad de gestión es de ,000. El resultado fue positivo logrando el incremento del valor de la gestión de riesgos de la información de un 3,65 a 5,22. Por lo cual, se concluye que, la implementación del sistema de gestión de seguridad de información sí influye en la gestión de riesgos en activos de información.

Apahuasco (2019), en su investigación llevada a cabo Andahuaylas, tuvo como objetivo "evaluar la gestión de seguridad de la información basada en el estándar "ISO 27001" en una empresa de servicios". En ese contexto, la metodología que se utilizó fue de tipo aplicada con enfoque cuantitativo y de diseño experimental. La población y la muestra están compuestas por

15 hosts. La técnica utilizada fue la técnica de la observación, por lo cual, el instrumento para recolectar la información fue la lista de cotejo. Asimismo, para el fragmento estadístico se utilizó la prueba T-Student. El resultado obtenido fue la minimización en un 63.33% de la vulnerabilidad de la información al utilizar la norma "ISO 27001" en una empresa de servicios.

Antecedentes internacionales

Ortiz et al. (2022), en su investigación llevada a cabo en Colombia, tuvo como objetivo diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001/2013, que garantice la integridad, confidencialidad y disponibilidad de la información en una empresa de servicios. En ese mismo contexto, se implementó la metodología de investigación aplicada con enfoque cualitativo como parte de la metodología de estudio. Como parte de los resultados, la entidad evaluada recibió una calificación de 28/100 después de usar el instrumento. Esto indica que hay pocos procesos de gestión de la seguridad y privacidad de la información, lo que crea brechas para las múltiples vulnerabilidades de los sistemas de información. En consecuencia, se determinó que el desarrollo de un Sistema de Gestión de Seguridad de la Información aumentará el nivel de seguridad en el tratamiento de información y en todos los procedimientos que involucren el uso de activos de información. Esto se debe a que permitirá mantener actualizada su infraestructura tecnológica, mejorar la velocidad con la que sus sistemas de información se conectan a la red de datos, evitar la pérdida o daño de información y gestionar planes de acción.

Torres (2020), en su investigación llevada a cabo en Ecuador, tuvo como objetivo "elaborar una propuesta de plan de seguridad informática utilizando la norma "ISO 27001" en una empresa de servicios". En ese mismo contexto, como parte de la metodología de estudio esta se basa en un enfoque cualitativo y aplicada. Las técnicas que se usaron fueron las entrevistas,

encuestas y la observación. La población fue de 4 empleados de la empresa. Además, como parte de los resultados se observó que el 77 % del personal conoce regularmente la seguridad de la información, o no, el 33 % conoce los procedimientos para la defensa y seguridad de la información, pero supera el 50 %, por lo que es necesario implementar una estrategia que permita reducir los riesgos que pongan en peligro la disponibilidad, la integridad y confidencialidad de la información. Se concluyó gracias a una segunda encuesta el impacto positivo al realizar la implementación del SGSI y se percibió la preservación de la confidencialidad, disponibilidad e integridad en la información de la empresa.

Muñoz (2020), en su investigación llevada a cabo en Ecuador, tuvo como objetivo "implementar un plan de gestión de seguridad informática basado en la norma "ISO 27001" para mejorar la seguridad de la información en una empresa de servicios". En ese mismo contexto, como parte de la metodología de estudio será básica y teórica. Las técnicas que se usaron fueron las entrevistas, encuestas y la observación. La población era de 5 empleados de la empresa. Asimismo, después de haber implementado el SGSI basado en norma "ISO 27001" se percibe que el 76% de los empleados afirma que la disponibilidad de la información es satisfactoria, el 80% de los empleados afirma que la integridad de la información es satisfactoria y el 80% de los empleados afirma que la confidencialidad de la información es satisfactoria. Se concluye, que la implementación del SGSI basado en la norma "ISO 27001" para la empresa de servicios cuenta con procedimientos definidos por el departamento de Tecnología de la Información que asegura la información de manera óptima.

Suarez (2021), en su investigación llevada a cabo en Colombia, tuvo como objetivo "analizar el sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015 en una empresa de servicios". En ese sentido, la metodología de estudio fue de tipo

de descriptiva y transversal, con enfoque cuantitativo. La técnica fue la encuesta, por lo cual, el instrumento fue el cuestionario. La población y la muestra fueron de 6 empleados. El estudio concluye que, el SGSI basado en la norma ISO/IEC 27001:2015, se logró establecer mecanismos para concientizar y sensibilizar la cultura en seguridad de información en la empresa de servicios.

Urvina et al. (2019), en su investigación desarrollada en Ecuador, tuvo como propósito "determinar la incidencia de la gestión de la seguridad de la información basada en la norma ISO/IEC 27001 en la información de una institución educativa". En ese sentido, la metodología tiene un enfoque cuantitativo y cualitativo, de investigación aplicada y bibliográfica y de tipo experimental. La técnica usada fue la encuesta y como instrumento el cuestionario. La población y las muestras están compuestos por 25 trabajadores. Asimismo, como resultado fue el chi-cuadrado de 3.84, con el cual, se acepta la hipótesis de investigación siguiente: gestión de seguridad de información basado en norma ISO/IEC 27001, el cual, sí incide en la información del negocio y a su vez, corrobora que existe una relación de dependencia entre las variables.

2.2 Bases teóricas

El estudio está compuesto por las siguientes tres teorías que son el soporte de las variables: (i) **teoría de la información**, según Shannon y Weaver (1949) indican que, se puede simplificar fallas técnicas de transmisión de señales de un lugar a otro, para medir la cantidad de información del mensaje y llegue a su destino con el menor número de distorsiones y errores, por lo cual, se vincula con la variable "ISO 27001" ya que existirá una menor dificultad en la gestión de riesgos de seguridad de información (Jiménez, 1995). Según Johansen (1982) concluye que, mientras más complejos son los sistemas, mayor es la energía que estos destinan a la obtención de la información, a su procesamiento y al almacenaje y/o comunicación, por lo cual, tiene

relación con la variable SGSI, ya que, brindará un control adecuado cuando se deba proteger el activo del negocio. Es decir, que esta teoría se encarga de estudiar el manejo que se le da a la información con el fin de medir la cantidad de información protegida y la eficacia de las medidas de seguridad implementadas (Hurtado, 2011). Por ello, se concluye que la teoría de la información puede ser utilizada para mejorar la gestión de la seguridad de la información y la eficacia del SGSI; (ii) l**a teoría de la gestión de la calidad**, según Deming (1989) afirma que, se debe buscar la excelencia en cuanto a calidad total mediante el aprendizaje y la innovación que brinda el mejoramiento continuo. Por ello, las organizaciones deben aplicar la mejora continua para desarrollar un sistema de gestión de seguridad de la información siguiendo la norma "ISO 27001**"** (ISOTools, 2023); (iii) l**a teoría general de sistemas**, según Bertalanffy (1976) menciona que, los sistemas son entidades complejas compuestas por las conexiones entre partes interconectadas que pueden ser evaluadas una por una. Por lo tanto, se relaciona con la variable "ISO 27001", puesto que, la norma cuenta con 11 secciones, 1 anexo con 114 controles de seguridad de la información, agrupados en 14 dominios. En esa línea, la teoría a través del análisis de las totalidades, se asocia al proceso de mejora, realineando los procesos con las necesidades de seguridad de información requeridas (López, 2017). Por ello, se relaciona con las variables "ISO 27001" y "SGSI", porque, proveen una visión sistémica y medible para contener un nivel de riesgo de seguridad de información aceptable en la organización (Valencia, 2021). Por lo tanto, las variables ISO 27001 y sistema de gestión de la seguridad de la información están interrelacionados y pueden ser interdependientes porque persiguen un objetivo común.

Variable independiente: ISO 27001

La “ISO 27001” define un SGSI, basado en un alcance de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información (Calder, 2016). Para López (2017), es una norma internacional que busca garantizar la seguridad de la información de una organización y de los sistemas y aplicaciones, asegurando su confidencialidad, integridad y disponibilidad. Como característica, especifíca los requisitos idóneos para definir, implementar, mantener y mejorar un SGSI, de acuerdo con las pautas para la aceptación y gestión de riesgos. (ISO/IEC, 2013) . En esa línea, la ISO 27001 puede ser integrado con otras herramientas que permitan evaluar riesgos y verificar antecedentes (Alkilani et al., 2022). Está enfocada en gestionar la seguridad como un proceso continuo en el tiempo. Es la única norma de las dos que puede ser certificada (Watkins, 2022). La ISO 27001 implementa un SGSI que necesita de auditorías periódicas con las que se inspeccionan la puesta en marcha y la supervisión de los controles de seguridad especificados en el SGSI. (Menéndez, 2023). Por tal razón, para que las organizaciones puedan asegurar que su SGSI cumple con los estándares de calidad, eficiencia y confiabilidad se debe usar la norma ISO 27001 ya que ofrece una guía para la protección de información (Wagner, 2012). En conclusión, la norma ISO 27001 es relevante para definir un SGSI que asegure la confidencialidad, integridad y disponibilidad de la información, con lo cual las organizaciones puedan brindar confianza entre clientes, proveedores y empleados.

Evolución de la Norma ISO 27001

La norma “ISO 27001”, ha estado en continuo cambio, incorporando las últimas tendencias en cuanto a seguridad de la información (Wagner, 2012).

British Standard 7799-1:1995: se instituye en el Reino Unido el "código de prácticas para la gestión de la seguridad de la información" (Honan, 2014). No obstante, en 1998 el Instituto Británico de Estándares, añadió una segunda parte a la norma llamado British Standard 7799-2:1998.

British Standard 7799-1:1999: se actualiza y publica la primera parte de BS7799 en 1999 (Honan, 2014). En resumen, se conoce a esta publicación como la primera norma que cuenta con dos partes.

British Standard 7799-2:1999: en esta versión se establece los requisitos para implantar un sistema de gestión de la seguridad de la información (SGSI) certificable (Honan, 2014). Resumiendo, se explica cómo diseñar e implementar un SGSI que gestione y proteja la información de una organización.

British Standard 7799-2:2002: se destacan cambios significativos como: la correspondencia entre los números de las secciones en ambas partes de la norma; la integración del ciclo PHVA; se incluyó una condición para perfeccionar el SGSI de manera continua (Calder, 2009). En conclusión, la norma se modificó y amplió sus secciones.

ISO/IEC 27001:2005: La BS7799-2 era una norma británica de seguridad de la información que varios países usaban. Para hacerla internacional, se publicó el borrador final como la BS7799-2:2005 en octubre de 2005 (Calder, 2009). En conclusión, la norma se usaba en varios países, pero tardó 6 años en ser internacional.

ISO/IEC 27001:2013: se publica la última versión de la ISO 27001 en octubre del 2013. El cambio fue enfocarse en crear un SGSI que se adapte a la organización y sus procesos, y así eliminar la repetición en la especificación y los controles (Calder, 2009). Resumiendo, los miembros del ISO/IEC publicaron una versión con mejoras significativas.

ISO/IEC 27001:2022: esta versión se adapta a los cambios en la seguridad de la información, la ciberseguridad y la privacidad, reduciendo el número de controles de seguridad de la información de 114 a 93, recategorizándolas en: organizacionales, personales, físicos y tecnológicos. De este modo, se renueva el enfoque de evaluación y tratamiento de los riesgos, adaptándose a nuevos escenarios y amenazas de ciberseguridad y la privacidad (Watkins, 2022). En conclusión, en esta versión se enfatiza la importancia de implementar un SGSI que adaptable al contexto y a los procesos de la organización.

Características de la variable ISO 27001

La norma ISO 27001 y la ISO 27002 se complementan entre sí, ello se debe a que, la ISO 27002 es una norma que explica las buenas prácticas para aplicar los controles de seguridad de la información especificadas en el Anexo A de la ISO 27001 (Esteban, 2021). En conclusión, ambas normas proporcionan un marco sólido para gestionar la seguridad de la información en una organización.

La ISO/IEC 27002 no es certificable, es un código de buenas prácticas en materia de seguridad de la información y se organiza en 14 dominios de seguridad, con un total de 35 objetivos y un total de 114 controles (Esteban, 2021). Resumiendo, la norma ISO 27002 no es certificable, ya que no es una norma de gestión, esta norma ofrece directrices detalladas sobre los controles que permitan proteger la información y alcanzar los objetivos del SGSI.

La norma ISO 27001, está enfocada al uso de buenas prácticas en materia de seguridad de la información, mitigación del riesgo, vinculadas a la implementación de un SGSI y que también sigue la filosofía de mejora continua, conocida como PDCA o ciclo Deming, PDCA (Plan-Do-Check-Act) que al castellano son Planificar, Hacer, Verificar y Actuar (Menéndez, 2023). En

conclusión, en conjunto, la norma ISO 27001 y el ciclo de Deming se complementan entre sí y proporcionan un marco sólido para la gestión de la seguridad de la información.

Dimensiones de la variable ISO 27001

Planear: Establecer la política, objetivos, proceso y procedimientos (López, 2017). Se concluye que, en esta etapa inicial se examina la situación actual, se detectan las áreas de mejora, se fijan objetivos y se planifican las acciones y los recursos para lograrlos.

Hacer: Implementar y operar la política (López, 2017). Se concluye que, en esta segunda etapa se pone en marcha el plan, se ejecutan las acciones, se reparten responsabilidades y se controla el avance del proceso.

Verificar: Evaluar y medir el desempeño del proceso (López, 2017). Se concluye que, se miden resultados, se contrastan objetivos, se verifican el nivel de cumplimiento y se hallan los problemas.

Actuar: Emprender acciones correctivas y preventivas con base en los resultados de la auditoría (López, 2017). Se concluye que, se trata de solucionar los problemas, aplicar las soluciones, afianzar las mejoras y normalizar el proceso.

Indicadores de la variable ISO 27001

Inventario de activos, refiere que, se deben identificar y clasificar los activos que procesan y almacenan información, elaborando y actualizando un inventario de estos activos, incluyendo las instalaciones donde se encuentran (ISO/IEC, 2013). Debe incluir tanto los activos físicos como los intangibles, como son el hardware, software, información, infraestructura, entre otros. Es por ello que, se debe definir el nivel de protección, clasificándolos y rotulándolos con el fin de llevar una adecuada gestión. (Mata, 2023). Se concluye que, este control es esencial para identificar riesgos, con el fin de definir las amenazas y vulnerabilidades reales para la protección

de la información.

Políticas de control de acceso, refiere a que, se debe establecer, documentar y aplicar una política que debe ser revisada periódicamente para que cumpla con los requisitos comerciales y de seguridad de la información (ISO/IEC, 2013). Toda organización debe contar con medidas de control de acceso para gestionar los permisos de acceso a los recursos lógicos, como son la asignación de roles y privilegios, implementar listas de control de acceso, entre otros instructivos en materia de seguridad de la información (Mata, 2023). Se concluye que, las políticas son fundamentales para autorizar, controlar y monitorizar a algunos usuarios el acceso a los sistemas de información y servicios.

Restricción de acceso a la información, refiere a que, se debe limitar el acceso a la información y a las funciones del sistema según la política de acceso. (ISO/IEC, 2013). Con el fin de asegurar que solo algunos usuarios con permiso puedan acceder a cierta información de manera correcta y segura (Mata, 2023).En resumen, es importante limitar el acceso a las áreas seguras solo a personas autorizadas, estableciendo controles de seguridad para evitar accesos indebidos y proteger la información.

Mantenimiento de equipos, refiere a que, se deben mantener adecuadamente y regularmente los equipos para prevenir fallas, reducir tiempos de inactividad y prolongar la vida útil de los equipos (ISO/IEC, 2013). Es necesario para garantizar el éxito continuo de los procesos del negocio de una empresa, ya que, permite determinar las vulnerabilidades y debilidades de los sistemas informáticos (Mata, 2023). Se concluye que, es esencial mantener los equipos en óptimas condiciones para salvaguardar la información y prevenir interrupciones operativas.

Controles contra códigos maliciosos, refiere a que, se deben contar con controles de

detección, prevención y recuperación contra malwares y a su vez, capacitar a los usuarios (ISO/IEC, 2013). Dicha monitorización, puede ayudar a identificar diversos ataques y tomar medidas para proteger los sistemas (Mata, 2023). En resumen, estos controles son vitales para prevenir accesos no autorizados, proteger contra malware y asegurar la seguridad de datos y servicios en la red.

Respaldo de la información, refiere a que, es importante realizar copias de seguridad de la información, software e imágenes del sistema de manera periódica y de acuerdo con la política definida. (ISO/IEC, 2013). Tanto la realización de respaldos como la restauración de información, se consideran una herramienta puesto que garantizan la protección de la información (Mata, 2023). Se concluye que, realizar el respaldo de la información es esencial para prevenir la pérdida de información en las organizaciones, definiendo y probando regularmente copias de seguridad de acuerdo con una política definida.

Variable dependiente: Sistema de gestión de seguridad de la información

El concepto básico que sustenta el sistema de gestión de seguridad de la información (SGSI), es el de seguridad de la información (Mata, 2023). El SGSI, cuenta con un conjunto de políticas enfocados en la gestión de la información y riesgos en la tecnología de la comunicación e información (Nabil et al., 2018). Este SGSI, es una herramienta esencial para evaluar y controlar los riesgos asociados con los datos e información manejados por una empresa (Calder, 2009). A su vez, permite la confiabilidad, la integridad y la disponibilidad de la información al ser un proceso sistemático, protocolizado y manejado por los colaboradores de la organización (Mata, 2022). Un SGSI diseñado y ejecutado adecuadamente puede contribuir a evitar que la información confidencial se pierda o filtre (López, 2017). Además, el SGSI nos puede ayudar a proteger la reputación de la organización y garantizar el cumplimiento legal y normativo (Nabil

et al., 2018). En resumen, un SGSI permite proteger y gestionar la seguridad de los activos a través de medidas que mitigarán ataques hacia los activos del negocio.

Pilares del sistema de gestión de seguridad de la información (SGSI)

La ISO/IEC 27001 se fundamenta en tres aspectos esenciales de la seguridad de la información, que se conoce como la tríada de la seguridad de la información (o Tríada CID): la confidencialidad, la disponibilidad y la integridad, porque son la base fundamental para cualquier sistema de gestión de seguridad de la información (Mata, 2022). A continuación, se describe a los tres pilares:

Etapas de la variable sistema de gestión de seguridad de la información

Según Gómez (2011), existen varias etapas en la gestión de seguridad de la información en una organización, a continuación, se detallan:

Etapa 1 - Implantación de medidas básicas de seguridad por sentido común: en esta etapa, la organización se enfocaría en implementar los protocolos de seguridad fundamentales que son comunes, como la creación de backups el control de acceso a los recursos informáticos, entre otros (Gómez, 2011). Es decir, en esta etapa se implantan medidas básicas de seguridad como: copias de seguridad, control de acceso a recursos entre otros.

Etapa 2 - Adaptación a los requisitos del marco legal y de las exigencias de los clientes: en esta segunda etapa, la empresa se da cuenta de la importancia de cumplir con las regulaciones vigentes u otras que surgen de sus relaciones y compromisos con terceros, como clientes, proveedores u otras entidades (Gómez, 2011). Es decir, en esta etapa se cumple con la legislación vigente.

Etapa 3 - Gestión integral de la Seguridad de la información: En la tercera etapa, la organización ya se preocupa por gestionar la seguridad de la información de manera global e

integrada, estableciendo una serie de políticas de seguridad, implementando planes y procedimientos de seguridad, realizando análisis y gestión de riesgos, y creando un plan de continuidad y respuesta a incidentes (Gómez, 2011). Es decir, se establece una gestión global de la seguridad de la información.

Etapa 4 - Certificación de la Gestión de la Seguridad de la Información: Finalmente, en la cuarta etapa se busca certificar la Gestión de la Seguridad de la Información para reconocer las buenas prácticas implementadas por la organización y poder acreditarlo ante terceros, como clientes, administraciones públicas y otras instituciones. Para lograrlo, se utiliza un proceso de certificación que se basa en estándares como ISO 27001 (Gómez, 2011). Se refiere a la certificación de la gestión de la seguridad.

Dimensiones de la variable sistema de gestión de seguridad de la información

Disponibilidad: es la capacidad de almacenar y acceder a la información cuando se necesita. Esto beneficia a la organización, pero también implica controlar los riesgos y la vulnerabilidad. Por eso, la seguridad con contraseñas y permisos es importante (Mata, 2022). Es decir, asegurar que la información esté disponible y accesible para las personas autorizadas cuando la necesiten.

Confidencialidad: el usuario, que es el elemento más propenso a fallar en la cadena, puesto que, maneja la información que requiere ser protegida, la confidencialidad es un aspecto muy difícil y peligroso de garantizar, pues el usuario puede cometer errores, descuidos o actos deliberados que pongan en riesgo la información, se revele a personas o entidades no autorizadas y perjudiquen a la organización (Mata, 2022). En conclusión, los usuarios son los responsables de manejar la información de forma segura y evitar errores, que puedan comprometer la confidencialidad.

Integridad: se refiere La integridad se refiere a que la información no sea alterada por personas o entidades sin permiso, y que los datos sean confiables, exactos y consistentes (Mata, 2022). Esto significa que, la información no sufrirá cambios o modificaciones mientras se transmita.

Indicadores de la variable sistema de gestión de seguridad de la información

Gestión de incidentes: conjunto de acciones a realizar en caso de ciberataque para reducir los daños causados por el mismo (Mata, 2022).

2.3 Formulación de hipótesis

2.3.1 Hipótesis general

"La implementación de la ISO 27001 optimiza el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024".

2.3.2 Hipótesis específica

HE1: La implementación de la ISO 27001 reduce la tasa de incidentes que impacta la disponibilidad en el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024.

HE2: La implementación de la ISO 27001 reduce la tasa de incidentes que impacta la integridad en el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024.

HE3: La implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad en el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024.

CAPÍTULO III: METODOLOGÍA

3.1 Método de la investigación

Para el presente proyecto se utilizaron los métodos deductivo, hipotético y analítico:

El método deductivo: es un procedimiento racional que va de lo general a lo particular. Las conclusiones de este método son verdaderas si las premisas lo son. De este modo, si un fenómeno se aplica a un grupo específico de personas, se puede deducir que se aplica a un miembro de ese grupo (Gómez, 2012).

El método analítico: es un método de investigación que consiste en descomponer el todo en sus partes para observar la naturaleza y los efectos del fenómeno. Este método ayuda a explicar y comprender mejor el fenómeno de estudio y a establecer nuevas teorías (Gómez, 2012).

El método hipotético deductivo: es una teoría que se plantea como no refutada y que se basa en hipótesis derivadas de datos recopilados. Estas hipótesis se someten a deducción y experimentación para llegar a una conclusión (Puebla, 2010).

3.2 Enfoque de la investigación

Para mejorar la seguridad de la información en la entidad en estudio, se manipuló la variable independiente y dependiente. Como resultado, el enfoque utilizado fue el cuantitativo.

Se denomina enfoque cuantitativo cuando se utiliza la recolección de datos informativos con el propósito de contrastar una hipótesis, en base a la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías (Hernández, 2014). Siguiendo esa línea, con los estudios cuantitativos se pretende describir, explicar y predecir los fenómenos investigados, buscando regularidades y relaciones causales entre elementos (variables). Esto significa que la meta principal es la prueba de hipótesis y la

formulación y demostración de teorías (Hernández, 2018).

3.3 Tipo de investigación

La investigación que se empleó es la aplicación real del método, por ende, se establece la metodología de la investigación de tipo aplicada. Estos diseños se usan para hacer experimentos donde el investigador manipula una variable y observa su efecto en otra, controlando otras variables (Hernández et al., 2014). Por ello, se determina como investigación tipo aplicada.

3.4 Diseño de la investigación

En un estudio experimental, se controla el escenario y cambia la variable independiente para observar su efecto sobre una o más variables dependientes (Hernández et al., 2014). En esa línea, se definió el uso de un diseño experimental de tipo pre experimental.

3.5 Población, muestra y muestreo

Población

En el presente estudio, la población está compuesta por 114 controles del anexo A de la ISO 27001, los cuales fueron observados utilizando guías de observación para el pre y post test con el fin de mejorar de la seguridad de la información de la entidad en estudio.

Para Vara (2012), la población es el conjunto de personas u objetos que comparten una o más características, se encuentran en un lugar o territorio y cambian con el tiempo.

Muestra

Según Vara (2012), “la muestra (n), es el conjunto de casos extraídos de la población, seleccionados por algún método racional y siempre parte de la población”.

Para encontrar la muestra, la fórmula es la siguiente:

$$n = \frac{Z^2 pqN}{e^2 N + Z^2 PQ}$$

Donde:

n: tamaño total de muestra

e: error en estimación permitido el valor será 6.95%

Z: valor en tabla distribución nivel de confianza será de 0.674

N -> tamaño de la población el valor será 114 controles

P -> probabilidad en éxito permitido será de 50%

q -> probabilidad en fracaso permitido será de 50%

A continuación, se calculó la muestra utilizando la fórmula anterior:

$$n = \frac{114x(0.674)2x0.5x0.5}{(6.95)2x(114-1)+(0.674)2x0.5x0.5}$$

n= 19.63 => 20 controles de la norma ISO 27001

Muestreo

Según Vara (2012), el muestreo es el proceso de extraer una muestra a partir de una población.

Además, lo define también como muestreo aleatorio, el cual utiliza el azar y las estadísticas para determinar el tamaño y la selección de cada integrante de la muestra. En resumen, para el presente estudio se optó utilizar el total de la población.

3.6 Variables y operacionalización

Para el proyecto de investigación actual se definen las siguientes variables:

Variable independiente: ISO 27001

La **definición conceptual** de la ISO 27001, ofrece orientación para gestionar la seguridad de la información de una empresa. Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información. Es aplicable a todo tipo de organización (ISO/IEC, 2013).

La **definición operacional** de la ISO 27001, brinda a las organizaciones un conjunto de procesos, políticas y controles que se implementan para gestionar la seguridad de la información

que se requieren para mitigar, prevenir y evaluar riesgos. La variable dependiente en la empresa de servicios, se somete a los controles denominados en este proyecto que se presentan en la tabla 1.

Variable dependiente: sistema de gestión de seguridad de información.

La **definición conceptual** de sistema de gestión de seguridad de información, es la de un conjunto de políticas, procedimientos y pautas, así también, como de recursos y actividades relacionados entre sí, que son gestionados por una empresa para proteger su información crucial (Mata, 2022).

La **definición operacional** de un sistema de gestión de seguridad de información, se centra en la gestión de los incidentes de seguridad de la información. La tasa de incidentes se mide a través de indicadores de seguridad, como son la tasa de incidente que impacta la confidencialidad, integridad y disponibilidad de la información. En ese contexto, los 3 pilares en mención serán medidos por los indicadores que a continuación se mencionan en la tabla 1.

3.7 Técnicas e instrumentos de recolección de datos

3.7.1 Técnica

La observación es un poderos método, con el cual, se produce información en condiciones parcialmente controladas y en el que se podrá manipular las variables (Huaire Inacio et al., 2022). Es decir, que al utilizar esta técnica se podrá contrastar mediante un pre y un post test de la variable independiente y dependiente.

3.7.2 Instrumentos

Para Ortiz (2003), la guía de observación es aquel instrumento diseñado para registrar sistemáticamente los aspectos relevantes de un objeto o fenómeno observable.

3.7.3 Validación

Según Vara (2012), para validar un contenido, se requiere del juicio de expertos en la materia; conocido también como "criterio de jueces". Para ello, los especialistas asegurarán que la variable a estimar tenga un contenido completo, confirmando que los indicadores sean los idóneos. La cantidad de expertos consultados debe ser de 3 a 10. (Vara, 2012). Para este proyecto, los instrumentos serán evaluados por 3 expertos (ver anexo 5).

3.7.4 Confiabilidad

Se aplicó la frecuencia acumulada, que son los subtotales que se van acumulando en cada categoría, estos pueden expresarse en porcentajes (Sánchez et al., 2018).

Se empleó rangos para su medición a través de un instrumento con el que se obtienen resultados sólidos (Hernández et al., 2014).

Se define Test-retest, al método de medición el cual usa un mismo instrumento de medición en varias ocasiones para evaluar al mismo conjunto de elementos luego de un determinado tiempo (Hernández et al., 2014). Debido a que los datos provinieron de la misma empresa de servicios, su confiabilidad de la misma es verídica.

3.8 Plan de procesamiento y análisis de datos

Esta etapa se desarrolló usando el formato "Statistical Package Off Social Sciences" (SPSS), para capturar y desarrollar el análisis de datos recopilados.

Respecto al sistema estadístico SPSS, Medina (2019) indica que, es un sistema de experiencia adaptable y amigable para entornos estadísticos y procesos de datos externos. Puede procesar desde gráficos de frecuencia sencillos hasta análisis estadísticos más complejos, como pruebas estadísticas y otros procesos más amplios y complejos.

Las etapas del sistema SPSS son seis, estas son: (i) la etapa inicial es la recopilación de datos, en la cual se recopilan los datos disponibles, actualizados y de calidad, estos datos están almacenados en la nube y la data podrá estar estructurada y no estructurada; (ii) la segunda etapa consiste en la preparación de datos, en esta fase se prepara la información detectando errores y descartando información repetitiva e incompleta, posteriormente se selecciona la información necesaria y puntual con la que se trabaja; (iii) la tercera etapa es la introducción de datos, aquí la información será útil ya que se visualizará; (iv) en la cuarta etapa limpieza de datos, la información se prepara y se optimiza con el fin de realizar la actividad prevista de diagnóstico o estudio de la interpretación realizada; (v) la quinta etapa consiste en la interpretación de datos, en el que se utiliza el resultado de las etapas anteriores para obtener una data representada por gráficas o tablas con el fin de garantizar un mejor entendimiento de la información y finalmente; (vi) la sexta etapa almacenamiento de datos, se almacenó toda la data procesada.

3.9 Aspectos éticos

La información solicitada se trabajó de manera confidencial y sólo se utilizó para este proyecto, se respetó el horario laboral de los usuarios que intervendrán en la ejecución del proyecto, la solicitud de información que sirvió para fines de investigación fue por medio del correo electrónico y se guardó absoluta confidencia respecto a la información que brindó la empresa en estudio. Asimismo, según lo establecido por la Universidad Norbert Wiener el porcentaje de similitud debe ser menor al 20%, en esa línea, el presente trabajo tiene un valor del 17% (ver anexo 8), por lo tanto, sí se cumple con lo requerido.

CAPÍTULO IV: RESULTADOS

4.1. Análisis descriptivo

4.1.1. Análisis descriptivo de resultados de la tasa de incidentes que impacta la confidencialidad

En lo que concierne con el indicador de la tasa de incidentes que impacta confidencialidad de la información, los resultados descriptivos detallados en la tabla 1, indican que, la tasa de incidentes que impacta la confidencialidad tiene como mínimo 88 (88%) y como máximo 100,00 (100%), la suma es de 1488,00 y como resultado se tiene una media de 99,2000 que corresponde al PreTest. Luego de haber implementado la ISO 27001, se obtuvo un mínimo de ,00 (00%) y el máximo de 13,00 (13%), como suma tiene 182,00 y como resultado una media de 1333 de la tasa de incidentes que impacta la confidencialidad correspondiente al PosTest.

Tabla 1

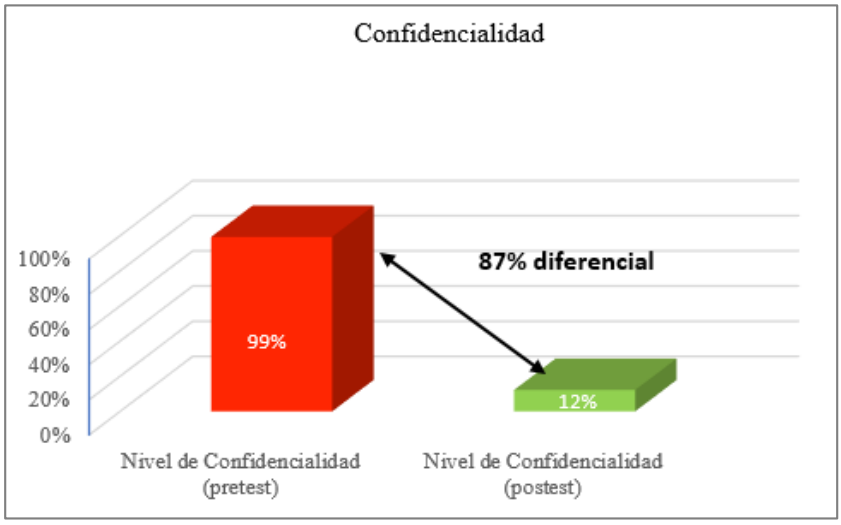
Estadísticos descriptivos de la tasa de incidentes que impacta la confidencialidad.

	N	**Mínimo**	**Máximo**	**Suma**	**Media**	**Desv. Desviación**
Pre_Nivel_Confidencialidad	15	88,00	100,00	1488,00	99,2000	3,09839
Post_Nivel_Confidencialidad	15	,00	13,00	182,00	13,33	35659
N válido (por lista)	15					

Según la tabla 1, se muestra que después de la implementación de la ISO 27001 redujo la tasa de incidentes que impacta la confidencialidad de la información.

Figura 2

Tasa de incidentes que impactan la confidencialidad



Interpretación: La tabla 4 y la figura 2, reafirma que existe un diferencial de 87% para la tasa de incidentes que impactan la confidencialidad de la información. Es decir, el pre-test arroja un promedio estadístico del 99.22% y para el post-test el 12.13%. Para resumir, se corrobora como parte del análisis de investigación que hay una reducción respecto a la tasa de incidentes que impacta la confidencialidad del 88%.

4.1.2. Análisis descriptivo de resultados de la tasa de incidentes que impacta la integridad

Referente a la tasa de incidentes que impacta la integridad de la información, los resultados descriptivos detallados en la tabla 2, indican que, la tasa de incidentes tiene un mínimo de 88,00 (88%) y el máximo es de 100,00 (100%), tiene como suma 117,0 y como resultado se tiene una media de 11,7000 respecto a la tasa de incidentes que impacta la integridad correspondiente al PreTest. Luego de haber implementado la ISO 27001, se obtuvo un mínimo de ,00 (0%) y máximo de 13,00 (13%), como suma tiene 182,00 y como resultado una media de 12,1333 de la tasa de incidentes que impactan la integridad que corresponde al PosTest.

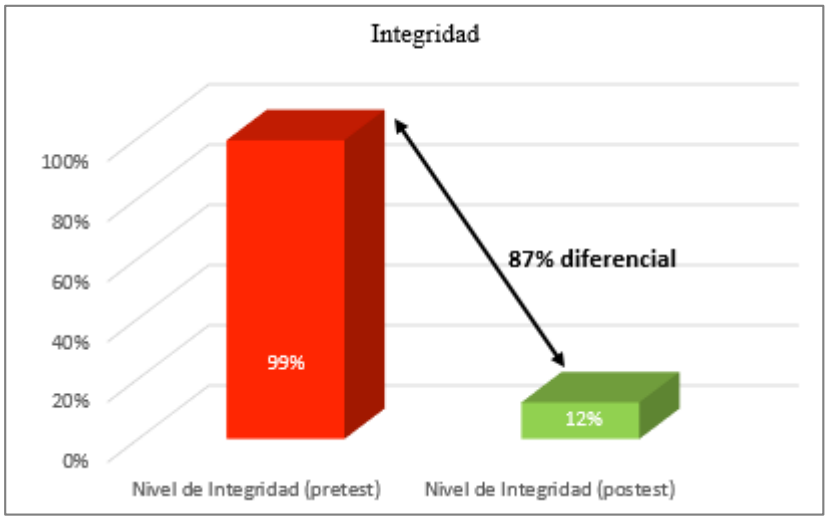
Tabla 2

Estadísticos descriptivos de la tasa de incidentes que impacta la integridad.

	N	Mínimo	Máximo	Suma	Media	Desv. Desviación
Pre_Nivel_Integridad	15	88,00	100,00	11488,00	99,2000	3,09839
Post_Nivel_Integridad	15	,00	13,00	182,00	12,1333	3,35659
N válido (por lista)	15					

Figura 3

Tasa de incidentes que impactan la integridad.



Interpretación: La tabla 4 y la figura 3, reafirma que existe un diferencial de 87% para la tasa de incidentes que impactan la integridad de la información. Es decir, el pre-test arroja un promedio estadístico del 99.22% y para el post-test el 12.13%. Para resumir, se corrobora como que existe una reducción respecto a la tasa de incidentes del 88%.

4.1.3. Análisis descriptivo de resultados de la tasa de incidentes que impacta la disponibilidad

Referente a la tasa de incidentes que impacta la disponibilidad de la información, los resultados descriptivos detallados en la tabla 3, indican que, existe el mínimo es de 88,00 (88%) y el máximo es de 100,00 (100%), tiene como suma 1488,00 y como resultado se tiene una media de 99,2000 que corresponde al PreTest. Luego de haber implementado la ISO 27001, se obtuvo el mínimo de ,00 (0%) y máximo de 13,00 (13%), como suma tiene 133,00 y como resultado una media de 99,2000 de la tasa de incidentes que impacta la disponibilidad que corresponde al PosTest.

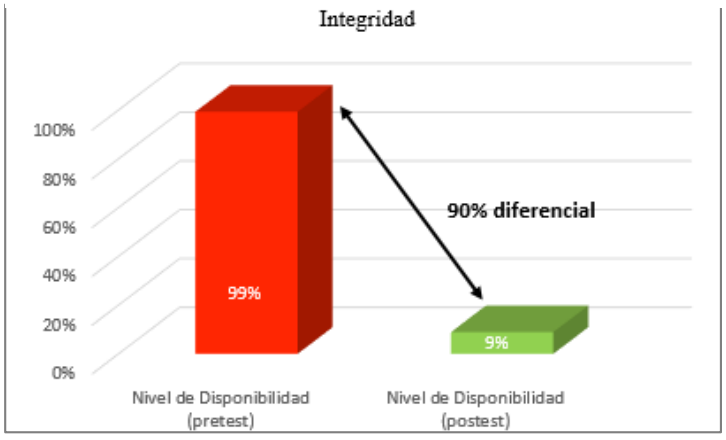
Tabla 3

Estadísticos descriptivos de la tasa de incidentes que impacta la disponibilidad.

	N	Mínimo	Máximo	Suma	Media	Desv. Desviación
Pre_Nivel_Disponibilidad	15	88,00	100,00	1488,00	99,2000	3,09839
Post_Nivel_Disponibilidad	15	,00	13,00	133,00	8,8667	3,68136
N válido (por lista)	15					

Figura 4

Tasa de incidentes que impactan la disponibilidad



Interpretación: La tabla 4 y la figura 4, reafirma que existe un diferencial de 90% para la tasa de incidentes que impactan la disponibilidad de la información. Es decir, el pre-test arroja un promedio estadístico del 99.22% y para el post-test el 8.86%. Para resumir, se corrobora como parte del análisis de investigación que existe una reducción de la tasa de incidentes del 99.90%.

Tabla 4

Frecuencias estadísticas.

Estadísticos

		Pre_Nivel_Confidencialidad	Post_Nivel_Confidencialidad	Pre_Nivel_Integridad	Post_Nivel_Integridad	Pre_Nivel_Disponibilidad	Post_Nivel_Disponibilidad
N	Válido	15	15	15	15	15	15
	Perdidos	6	6	6	6	6	6
Media		99,2000	12,1333	99,2000	12,1333	99,2000	8,8667
Mediana		100,0000	13,0000	100,0000	13,0000	100,0000	10,0000
Moda		100,00	13,00	100,00	13,00	100,00	10,00
Desv. Desviación		3,09839	3,35659	3,09839	3,35659	3,09839	3,68136
Varianza		9,600	11,267	9,600	11,267	9,600	13,552
Rango		12,00	13,00	12,00	13,00	12,00	13,00
Mínimo		88,00	,00	88,00	,00	88,00	,00
Máximo		100,00	13,00	100,00	13,00	100,00	13,00
Suma		1488,00	182,00	1488,00	182,00	1488,00	133,00

4.2. Análisis Inferencial

4.2.1. Confiabilidad

Figura 5

Consistencia de la tasa de incidentes que impacta la confidencialidad.

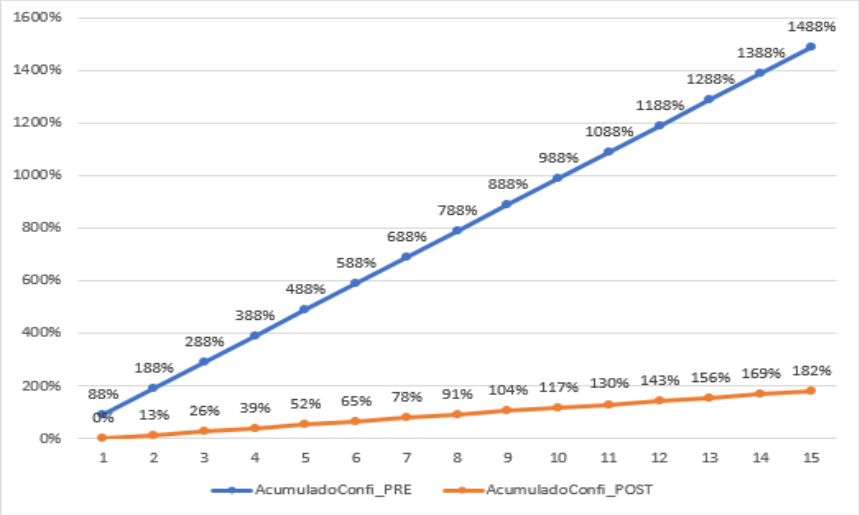


Figura 6

Consistencia de la tasa de incidentes que impacta la integridad.

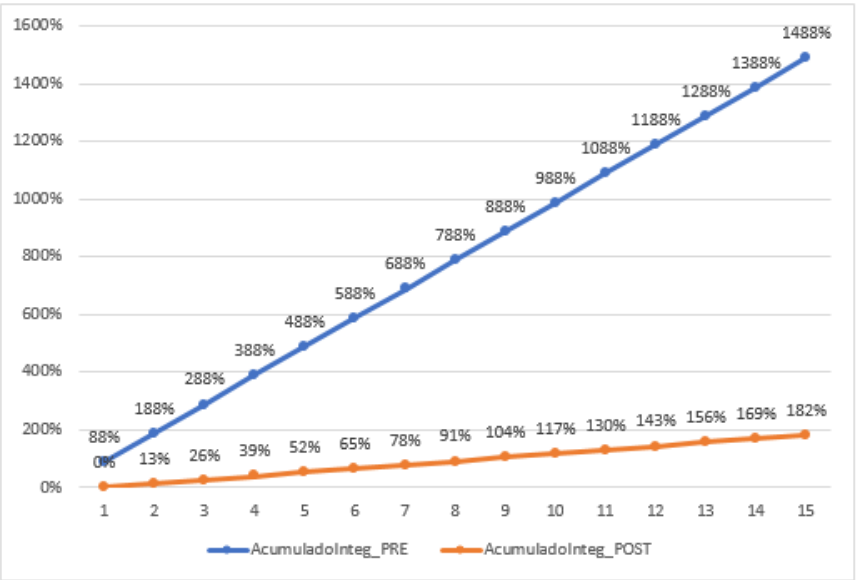
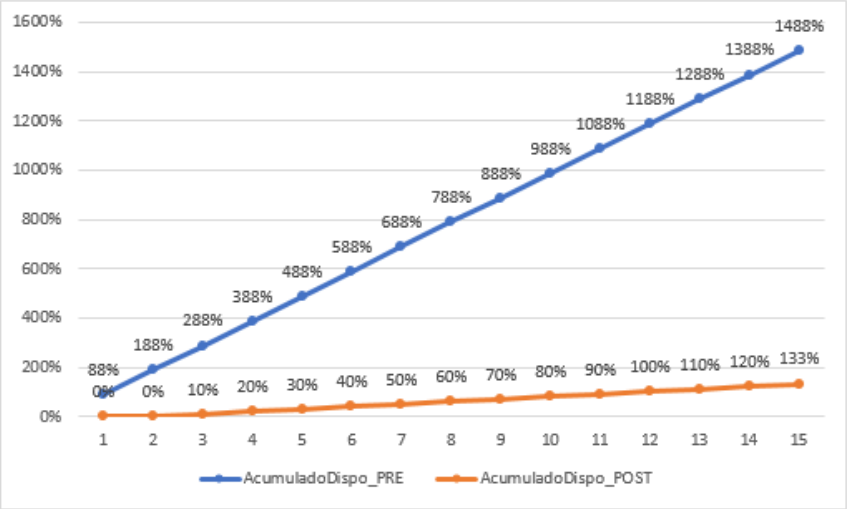


Figura 7

Consistencia de la tasa de incidentes que impacta la disponibilidad.



4.3. Prueba de Normalidad

Según lo observado en la tabla 5, se aplicó la prueba de normalidad, cuya muestra es igual a 15, de tal forma que, se aplicó la prueba Shapiro-Wilk. En ese sentido, se observa que el pretest es sig. = 0.000 < 0.05 para todos los indicadores y el postest es sig. = 0.000 < 0.05 para todos los indicadores por ello se aplica una prueba no paramétrica (Wilcoxon).

Tabla 5

Prueba de Normalidad

	Kolmogorov-Smirnova			**Shapiro-Wilk**		
	Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Pre_Nivel_Confidencialidad	,535	15	,000	,284	15	,000
Pre_Nivel_Integridad	, 535	15	,000	, 284	15	,000
Pre_Nivel_Disponibilidad	, 535	15	,000	, 284	15	,000
Post_Nivel_Confidencialidad	, 535	15	,000	, 284	15	,000
Post_Nivel_Integridad	, 535	15	,000	, 284	15	,000

Post_Nivel_Disponibilidad	,488	15	,000	,527	15	,000

a Corrección de significación de Lilliefors

4.4. Prueba de Hipótesis

a) Contrastación para la variable: tasa de incidentes que impacta la confidencialidad.

Definición de variables

TIICa = Tasa de incidentes que impacta la confidencialidad sin la aplicación.

TIICb= Tasa de incidentes que impacta la confidencialidad propuesta.

Hipótesis estadística

Hipótesis Ho = Tasa de incidentes que impacta la confidencialidad sin la aplicación es menor o igual que Tasa de incidentes que impacta la confidencialidad propuesta.

$$\boldsymbol{Ho}= \text{TIICa} - \text{TIICb} \leq \mathbf{0}$$

Hipótesis Ha = Tasa de incidentes que impacta la confidencialidad sin la aplicación es diferente que Tasa de incidentes que impacta la confidencialidad propuesta.

$$\boldsymbol{Ha}= \text{TIICa} - \text{TIICb} \neq \mathbf{0}$$

Nivel de confianza

El nivel de confianza será del 95% (1- α= 0.95).

“Se aplicó la prueba no paramétrica de Wilcoxon”.

Tabla 6

Prueba de rangos con signos de Wilcoxon

		N	Rango promedio	Suma de rangos
Post_Nivel_Confidencialidad - Pre_Nivel_Confidencialidad	Rangos negativos	15a	8,00	120,00
	Rangos positivos	0b	,00	00
	Empates	0c		
	Total	15		

a Post_Nivel_Confidencialidad < Pre_Nivel_Confidencialidad

b Post_Nivel_Confidencialidad > Pre_Nivel_Confidencialidad

c Post_Nivel_Confidencialidad = Pre_Nivel_Confidencialidad

Tabla 7

Estadístico de prueba del indicador Nivel de Confidencialidad.

	Post_Nivel_Confidencialidad - Pre_Nivel_Confidencialidad
Z	-3,771b
Sig. asintótica(bilateral)	,000

a Prueba de rangos con signo de Wilcoxon

b Se basa en rangos negativos.

Según la tabla 7, se tiene un valor Z de -3,771b y una sig. (bilateral) de ,000 cuyo valor es menor a 0.05, para este caso se rechaza la hipótesis nula y se acepta la hipótesis alterna. A su vez, en la tabla 6, se observa que el rango promedio entre la pre-test y post-test tiene una diferencia de 8,00 y se tiene una diferencia en la suma de rangos de 120,00. Se concluye que, sí hay una reducción de la tasa de incidentes que impacta la confidencialidad.

a) Contrastación para la variable: tasa de incidentes que impacta la integridad.

Definición de variables

TIIIa = Tasa de incidentes que impacta la integridad sin la aplicación.

TIIIb = Tasa de incidentes que impacta la integridad propuesta.

Hipótesis estadística

Hipótesis Ho = Tasa de incidentes que impacta la integridad sin la aplicación es menor o igual que la Tasa de incidentes que impacta la integridad propuesta.

$$\boldsymbol{Ho}= \text{TIIIa} - \text{TIIIb} \leq \mathbf{0}$$

Hipótesis Ha = Tasa de incidentes que impacta la integridad sin la aplicación es diferente que Tasa de incidentes que impacta la integridad propuesta.

$$\boldsymbol{Ha}= \text{TIIIa} - \text{TIIIb} \neq \mathbf{0}$$

Nivel de confianza

El nivel de confianza será del 95% (1- α= 0.95).

"Se aplicó la prueba no paramétrica de Wilcoxon".

Tabla 8

Prueba Wilcoxon de la tasa de incidentes que impacta la integridad.

		N	Rango promedio	Suma de rangos
Post_Nivel_Integridad - Pre_Nivel_Integridad	Rangos negativos	15a	8,00	120,00
	Rangos positivos	0b	,00	,00
	Empates	0c		
	Total	15		

a Post_Nivel_Integridad < Pre_Nivel_Integridad

b Post_Nivel_Integridad > Pre_Nivel_Integridad

c Post_Nivel_Integridad = Pre_Nivel_Integridad

Tabla 9

Estadístico de prueba de la tasa de incidentes que impacta la integridad.

	Post_Nivel_Integridad - Pre_Nivel_Integridad
Z	-3,771b
Sig. asintótica(bilateral)	,000

a Prueba de rangos con signo de Wilcoxon

b Se basa en rangos negativos.

Según la tabla 9, se tiene un valor Z de -3,771b y una sig. (bilateral) de 0.000 cuyo valor es menor a 0.05, para este caso se rechaza la hipótesis nula y se acepta la hipótesis alterna. A su vez, en la tabla 8, se observa que el rango promedio entre la pre-test y post-test tiene una diferencia de 8,00 y se tiene una diferencia en la suma de rangos de 120,00. Se concluye que, sí hay una reducción en la tasa de incidentes que impacta la integridad.

a) Contrastación para la variable: la tasa de incidentes que impacta la disponibilidad.

Definición de variables

TIIDa = Tasa de incidentes que impacta la disponibilidad sin la aplicación.

TIIDb= Tasa de incidentes que impacta la disponibilidad propuesta.

Hipótesis estadística

Hipótesis Ho = Tasa de incidentes que impacta la disponibilidad sin la aplicación es menor o igual que la Tasa de incidentes que impacta la disponibilidad propuesta.

$$\boldsymbol{Ho}= \text{TIIDa} - \text{TIIDb} \leq \mathbf{0}$$

Hipótesis Ha = Tasa de incidentes que impacta la disponibilidad sin la aplicación es diferente que la Tasa de incidentes que impacta la disponibilidad propuesta.

$$\boldsymbol{Ha}= \text{TIIDa} - \text{TIIDb} \neq \mathbf{0}$$

Nivel de confianza

El nivel de confianza será del 95% (1- α= 0.95).

"Se aplicó la prueba no paramétrica de Wilcoxon".

Tabla 10

Prueba Wilcoxon de la tasa de incidentes que impacta la disponibilidad.

		N	Rango promedio	Suma de rangos
Post_Nivel_Disponibilidad - Pre_Nivel_Disponibilidad	Rangos negativos	15a	8,00	120,00
	Rangos positivos	0b	,00	,00
	Empates	0c		
	Total	15		

a Post_Nivel_Disponibilidad < Pre_Nivel_Disponibilidad

b Post_Nivel_Disponibilidad > Pre_Nivel_Disponibilidad

c Post_Nivel_Disponibilidad = Pre_Nivel_Disponibilidad

Tabla 11

Estadístico de prueba de la tasa de incidentes que impacta la disponibilidad.

	Post_Nivel_Disponibilidad - Pre_Nivel_Disponibilidad
Z	-3,623b
Sig. asintótica(bilateral)	,000

a Prueba de rangos con signo de Wilcoxon

b Se basa en rangos negativos.

Según la tabla 11, se tiene un valor Z de -3,623b y una sig. (bilateral) de 0.000 cuyo valor es menor a 0.05, para este caso se rechaza la hipótesis nula y se acepta la hipótesis alterna. A su vez, en la tabla 10, se observa que el rango promedio entre la pre-test y post-test tiene una diferencia de 8,00 y se tiene una diferencia en la suma de rangos de 120,00. Se concluye que, sí hay una reducción de la tasa de incidentes que impacta la disponibilidad.

4.5 Discusión de resultados.

En alusión a lo demostrado en las bases teóricas y antecedentes. Se corrobora la aceptación de la hipótesis en la cual, demostrando que la implementación de la "ISO 27001" optimiza el SGSI en una empresa de servicios, dicha entidad carecía de un nivel adecuado de seguridad, es por ello que, ocurrían incidentes que impactaban negativamente en la confidencialidad, integridad y disponibilidad de la información. Al implementar la ISO 27001, la seguridad de la información mejoró un promedio de 99%, debido a que, el promedio de seguridad inicial era del 11%, reduciendo un 99% los incidentes que impactan la seguridad de la información. Mantiene una relación con el estudio desarrollado por Asqui (2023), en su investigación que tuvo como objetivo "demostrar cómo la ISO 27001 mejora la seguridad de la información en una institución educativa. Los resultados arrojaron un incremento de 61.64% en general. Para finalizar, coincide con lo mencionado por Wagner (2012), en el que recomienda a las organizaciones asegurar su SGSI usando la norma ISO 27001 ya que ofrece una guía para la protección de información.

La finalidad principal de la investigación se basó en "determinar que la implementación de la ISO 27001 mejora el sistema de gestión de Seguridad de la información en una empresa de servicios, Lima 2024". Como parte de los resultados estadísticos de los indicadores y dimensiones de la variable "Sistema de gestión de seguridad de la información", se evidenció la reducción del 99% de incidentes que impacta la confidencialidad, un 99% de incidentes que impacta la integridad y un 99% de incidentes que impacta la disponibilidad de la información, y finalmente, una considerable reducción total de incidentes de seguridad de un 99% aproximadamente. Por esta razón, los resultados obtenidos, coinciden parcialmente con el aporte de Aguirre (2018), el cual, desarrolló un estudio que tuvo como objeto mejorar la seguridad de la información. Los resultados indicaron que, la disponibilidad incrementó un 25.61%; es decir

pasó de 72,33% a 97.94%; asimismo, la integridad incrementó en un 23.88%; es decir pasó de 74.06% a 97.94%; finalmente, la confidencialidad incrementó un 19.28%, es decir pasó de 77.39% a 96.7%. Vale decir, con la implementación de la "ISO 27001", la tasa de incidentes de la confidencialidad, integridad y disponibilidad se redujeron significativamente en función al "SGSI". Finalmente, coincide con Aleman (2023), el cual realizó un estudio sobre la "ISO 27001", en el cual evidencia que la implementación de la norma "ISO 27001:2013", mejoró considerablemente su seguridad.

Se corrobora la aceptación de la hipótesis en la cual, demuestra que, la implementación de la "ISO 27001" reduce la tasa de incidentes que impacta la disponibilidad de la información en el SGSI de una empresa de servicios, la cual demuestra que sin aplicar los controles de la "ISO 27001" obtuvo un promedio de 99% de incidentes, dicho promedio se redujo a un 9% luego de la implementación. Es decir, se evidencia una reducción en la tasa de incidentes que impacta la integridad de la información al implementar la "ISO 27001". Los resultados arrojaron que la implementación de la norma reduce la tasa de incidentes que impacta la integridad, puesto que, de tener un 99% se redujo a 9% obteniendo así una mejora del 90%. En general, se corrobora que la implementación de la norma "ISO 27001" optimiza la integridad de la información en la empresa de servicios. Para finalizar, coincide con lo mencionado por Pablos et al (2012), en el que declara que la "ISO 27001" orienta en el desarrollo de un SGSI, ya que ofrece garantizar la integridad de la información de una entidad.

El estudio corrobora la aceptación de la hipótesis en la cual, se indica que, la implementación de la "ISO 27001" reduce la tasa de incidentes que impacta la integridad de la información en el SGSI de una empresa de servicios, la cual demuestra que sin aplicar los controles de la "ISO 27001" obtuvo un promedio de 99% de incidentes, dicho promedio se

redujo a un 12% luego de su aplicación. Es decir, se evidencia una reducción de la tasa de incidentes que impacta la integridad de la información al implementar la “ISO 27001”. Los resultados arrojaron que la implementación de la norma redujo la tasa de incidentes que impacta la integridad, puesto que, de tener un 99% se redujo a 12% obteniendo así una mejora del 87%. En general, se corrobora que la implementación de la norma “ISO 27001” optimiza la integridad de la información en la empresa de servicios. Para finalizar, coincide con lo mencionado por Mata (2022), en el que afirma que la norma “ISO 27001” cuenta con controles para fortalecer la integridad de la información crucial de una empresa.

Se corrobora la aceptación de la hipótesis en la cual, demuestra que, la implementación de la “ISO 27001” reduce la tasa de incidentes que impacta la confidencialidad de la información en el SGSI de una empresa de servicios, la cual demuestra una tasa de incidentes del 99% sin aplicar los controles de la “ISO 27001”, dicho promedio se redujo a un 12% luego de su implementación. Es decir, se evidencia una reducción de la tasa de incidentes que impacta la confidencialidad de la información al implementar la norma. Los resultados arrojaron que la implementación reduce la tasa de incidentes que impacta la confidencialidad de la información, puesto que, de tener un 99% se redujo a 12% obteniendo así una mejora del 87%. En general, se corrobora que la implementación de la norma “ISO 27001” reduce la tasa de incidentes que impacta la confidencialidad de la información en la empresa de servicios. Para finalizar, coincide con lo mencionado por Pablos et al (2012), los cuales mencionan que, la norma “ISO 27001” orienta en el desarrollo de un SGSI, ya que ofrece fortalecer la confidencialidad de la información de una organización.

CAPÍTULO V: Conclusiones y Recomendaciones

5.1 Conclusiones

Primera: Al implementar la ISO 27001, se consiguió mejorar el sistema de gestión de seguridad de la información en la empresa NIPON BUSINESS S.A.C. Según los resultados del PreTest y PostTest de los indicadores que corresponden a la tasa de incidentes que impacta a la confidencialidad, tasa de incidentes que impacta a la integridad y a la tasa de incidentes que impacta a la disponibilidad, obteniendo un promedio de 99% de reducción de incidentes, en comparación al promedio inicial que era del 11%.

Segunda: Se evidenció que, al implementar políticas y un control de acceso de seguridad, basados en la ISO 27001, se logró reducir la tasa de incidentes que impacta la confidencialidad en un 12%. En conclusión, la empresa garantiza mantener una buena reputación y el cumplimiento del normativo legal.

Tercera: Se evidenció que, al implementar un sistema de copias y restauración de datos basados en la ISO 27001, se logró reducir la tasa de incidentes que impacta la integridad al 12%. En conclusión, la empresa garantiza una mayor seguridad y confianza al personal de la empresa.

Cuarta: Se evidenció que, al efectuar el mantenimiento e inventarios de sus equipos siguiendo las políticas basadas en la ISO 27001, se logró reducir la tasa de incidentes que impacta la disponibilidad en un 9%. En conclusión, la empresa garantiza un rendimiento eficiente y un control adecuado de sus activos.

5.2 Recomendaciones

Primera: En primera instancia se recomienda a la gerencia, que se realice un seguimiento constante de la aplicación de las políticas en todas las áreas, procesos del negocio e involucrar al personal nuevo y realizando evaluaciones trimestrales con el fin de mitigar incidentes que puedan dañar la seguridad y que para que, en el futuro se logre por la certificación internacional.

Segunda: Se recomienda a la gerencia, capacitar a los colaboradores sobre las vulnerabilidades y amenazas que puedan dañar los activos de información integrándolo con las políticas de la ISO 27001, con el fin de mitigar la tasa de incidentes que afecten la confidencialidad de la información.

Tercera: Se recomienda al jefe de TI, seguir implementando las políticas y controles faltantes basados en la ISO 27001, aplicando el método de mejora continua, para aumentar los niveles de integridad y de esta manera seguir cubriendo toda la arquitectura informática de seguridad de manera plena y general.

Cuarta: Se recomienda al jefe de TI, seguir efectuando el mantenimiento e inventarios de los activos según las políticas basadas en la ISO 27001, con el fin de mitigar la tasa de incidentes que afecten la disponibilidad de la información.

CAPÍTULO VI: Referencias

Aguirre, J. (2018). *Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina.* Universidad César Vallejo, Lima. https://hdl.handle.net/20.500.12692/35308

Aleman Balladares, F. (2023). *Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023.* Universidad César Vallejo, Lima, Perú. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/106824/Aleman_BFY-SD.pdf

Alkilani, & Qusef. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Comput*. doi:https://peerj.com/articles/cs-810/

Apahuasco Saccaco, E. (2019). *Evaluación del sistema de seguridad de la Información en la organización DISAV S.A.C. aplicando lineamientos ISO 27001.* Universidad Nacional José María Arguedas, Andahuaylas, Perú. https://repositorio.unajma.edu.pe/handle/20.500.14168/496

Asqui Zevallos, J. (2023). *27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022.* Universidad Privada Norbert Wiener, Lima, Perú. https://hdl.handle.net/20.500.13053/8519

Banco interamericano de desarrollo. (2020). *Banco interamericano de desarrollo*. http://dx.doi.org/10.18235/0002513

Bertalanffy, L. (1976). *Teoría general de los sistemas.* Fondo de Cultura Económica. https://www.google.com.pe/books/edition/Teor%C3%ADa_general_de_los_sistemas/1JLsAQAACAAJ?hl=es

Calder, A. (2009). *Implementing Information Security Based on ISO 27001/ISO 27002.* van Haren Publishing.

Calder, A. (2016). *Nine steps to success.* Amersfoort – NL.

Carpio, M. (09 de 09 de 2021). *Real Instituto El Cano*. Real Instituto El Cano: https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari77-2021-carpio-la-calificacion-de-seguridad-de-sistemas-de-informacion-en-europa.pdf

Cerezo, J. (2022). *Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A. en Ecuador*. Trujillo. https://hdl.handle.net/20.500.12692/102607

Crespo, E. (2017). Ecu@Risk, una metodología para la gestión de riesgo aplicada a las MPYMES. *ENFOQUE UTE Revista*. doi:https://doi.org/10.29019/enfoqueute.v8n1.140

Del Villar, J. (8 de setiembre de 2021). *Idty*. https://www.idty.com/es-la/5-de-los-mayores-ataques-de-ciberseguridad-en-los-ultimos-anos

El Economista. (2022). *Actualizan norma ISO contra ciberataques en las organizaciones*. https://www.eleconomista.com.mx/tecnologia/Actualizan-norma-ISO-contra-ciberataques-en-las-organizaciones-20221022-0026.html

El Peruano. (2021). *Diario El Peruano*. Diario El Peruano: https://elperuano.pe/noticia/121344-modifican-el-reglamento-para-la-gestión-de-la-seguridad-de-la-seguridad-de-la-infrmacion-y-la-ciberseguridad

ESET. (2021). *ESET*. https://web-assets.esetstatic.com/wls/2021/06/ESET-security-report-LATAM2021.pdf

ESET. (31 de 08 de 2023). *ESET*. ESET: https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/el-69-de-las-organizaciones-de-latinoamrica-sufrio-algun-incidente-de-seguridad-durante-el-ultimom-a/

Esteban Paúl, Á., García Martín, J., Torres Carbonell, J., & García Roger, C. (2021). *Administración electrónica. Aspectos jurídicos, organizativos y técnicos.* Aranzadi. https://books.google.com.pe/books/about/Administración_electrónica_Aspectos_ju.html?id=A61BEAAAQBAJ&redir_esc=y

Global Standards. (20 de 10 de 2022). *Global Standards*. Global Standards: https://www.globalstd.com/blog/iso-survey-2021

Gómez, Á. (2011). *Seguridad en Equipos Informáticos.* RA-MA Editorial. https://www.google.com.pe/books/edition/MF0486_3_Seguridad_en_Equipos_Inform%C3%A1ti/o6W6EAAAQBAJ?hl=es&gbpv=0

Gómez, S. (2012). *Metodología de la investigación.* RED TERCER MILENIO S.C.

Hernández Sampieri, C., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación.* Mc Graw-Hill Education.

Hernández, M., & Baquero, E. (2020). *Ciclo de vida de desarrollo ágil de software seguro.* Fundación Universitaria Los Libertadores. https://www.google.com.pe/books/edition/Ciclo_de_vida_de_desarrollo_%C3%A1gil_de_sof/XdQ7EAAAQBAJ?hl=es&gbpv=0

Hernández, R. (2018). *Metodología de la investigación.* McGraw-Hill Interamericana.

Honan, B. (2014). *ISO27001 in a Windows Environment.* IT Governance Publishing. https://www.google.com.pe/books/edition/ISO27001_in_a_Windows_Environment/fmM3DwAAQBAJ?hl=es-419&gbpv=0

Huaire Inacio, E., Marquina Luján, R., Horna Calderón, V., Llanos Miranda, K., Herrera Álvarez, Á., Rodríguez Sosa, J., & Villamar Romero, R. (2022). *Tesis fácil. El arte de dominar el método científico.* ANALÉCTICA.

Hurtado, D. (2011). *Teoría General de Sistemas: un enfoque hacia la ingeniería de sistemas 2Ed*. Lulu.com. https://www.google.com.pe/books/edition/Teoria_General_de_Sistemas_Un_Enfoque_Ha/Ww41AwAAQBAJ?hl=es&gbpv=0

ISO/IEC. (2013). *Information technology — Security Information technology — Security management systems — Requirements.* Ginebra: ISO copyright office.

ISO/IEC. (2022). *ISO/IEC 27001:2022(E).* Switzerland: ISO/IEC.

ISOTools. (2023). *ISOTools*. https://www.isotools.us/normas/riesgos-y-seguridad/iso-27001/

Johansen , O. (1982). *Introducción a la teoría general de sistemas.* Limusa. https://www.google.com.pe/books/edition/Introducci%C3%B3n_a_la_teor%C3%ADa_general_de_si/4bVvTLvHVzMC?hl=es&gbpv=0

López, R. (2017). *Sistema de Gestión de la seguridad informática.* Fondo editorial Areandino.

Mata García , A. (2023). *Seguridad de Equipos Informáticos. Edición 2024.* España: Ra-Ma S.A. Editorial y Publicaciones. https://www.google.com.pe/books/edition/Seguridad_de_Equipos_Informáticos_Edici/iHzoEAAAQBAJ?hl=es-419&gbpv=0

Mata García, A. E. (2022). *E-Book - Kali Linux para Hackers.* Madrid: RA-MA S.A. Editorial y Publicaciones.

Nabil, M., & Susanto, H. (2018). *Information Security Management Systems.* Apple Academic Press.

Organización para la Cooperación y el Desarrollo Económicos. (2021). *Guía Práctica sobre Confidencialidad y Gestión de la Seguridad de la Información.* OCDE.

Ortiz Uribe, F. (2003). *Diccionario de metodolog¡a de la investigación científica.* México: Limusa.

Ortiz, R., & Prada, G. (2022). *Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de tecnologías de la información y la comunicación del hospital San Vicente de Paúl de Fresno.* Fresno. https://repository.unad.edu.co/handle/10596/51482

Porras Ruiz, M. (2019). *Sistema de gestión de seguridad de la información para la gestión de riesgos en activos de información.* Universidad Peruana Los Andes, Huancayo, Perú. https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2604/T037_45702501_T.pdf

Presidencia del consejo de ministros. (2012). *Gob.pe.* Gob.pe: www.gob.pe/institucion/midis/normas-legales/270075-129-2012-pcm

Puebla, C. (2010). *Universidad de Valparaiso.* http://mbeuv.files.wordpress/2010/09/4-metodo-hipotetico-deductivo.pdf

Revista Economía. (2022). Ciberataques en el Perú incrementaron en un 15% durante el 2021. *Revista Economía.* https://www.revistaeconomia.com/ciberataques-en-el-peru-incrementaron-en-un-15-durante-el-2021/

Revista Economía. (12 de setiembre de 2023). ¿Tu empresa está creciendo? 6 claves para fortalecer tu ciberseguridad y evitar ataques informáticos. https://www.revistaeconomia.com/tu-empresa-esta-creciendo-6-claves-para-fortalecer-tu-ciberseguridad-y-evitar-ataques-informaticos/

Russo, A. (2023). *Alexander*. Los 10 ciberataques más famosos de la historia: https://blog.hackmetrix.com/los-10-ciberataques-mas-famosos-de-la-historia/

Sánchez Carlessi, H., Reyes Romero, C., & Mejía Sáenz, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística.* Lima: Universidad Ricardo Palma.

Suarez Barros, L. (2021). *Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015- en la empresa Magdaniel LTDA. en el Distrito Especial, Turístico y Cultural de Riohacha – Colombia.* Universidad de La Guajira, Riohacha , Colombia. https://repositoryinst.uniguajira.edu.co/handle/uniguajira/407

Trujillo, F. (2023). *ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una institución pública, Lima 2023.* Lima. https://hdl.handle.net/20.500.12692/120927

Urvina Barrionuevo, K., & Cuenca León, W. (2019). *Seguridad de la Información basado en la Norma ISO/IEC 27001 y su incidencia en las Instituciones de Educación Superior de la ciudad de Machala.* Universidad Técnica de Ambato, Machala, Ecuador. http://repositorio.uta.edu.ec/jspui/handle/123456789/29844

Valbuena, S. (23 de agosto de 2023). *Infobae*. https://www.infobae.com/tecno/2023/08/24/panorama-cibernetico-2023-america-latina-bajo-asedio-de-los-criminales-por-aumento-de-ataques/

Vara Horna, A. (2012). *Desde la idea hasta la sustentación: 7 pasos para una tesis exitosa.* Lima: Instituto de Investigación de la Facultad de Ciencias Administrativas y Recursos Humanos. Universidad de San Martin de Porres.

von Bertalanffy , K. (1928). *La Teoría General de Sistemas*. https://psicologiaymente.com/psicologia/teoria-general-de-sistemas-ludwig-von-bertalanffy

von Bertalanffy, L. (1950). *La teoría general de sistemas.* https://fad.unsa.edu.pe/bancayseguros/wp-content/uploads/sites/4/2019/03/Teoria-General-de-los-Sistemas.pdf

Wagner, K.-P., Vieweg, I., Hüttl, T., Backin, D., & Werner, C. (2012). *Einführung Wirtschaftsinformatik.* Gabler Verlag.

Watkins, S. (2022). *ISO/IEC 27001:2022 - An introduction to information security and the ISMS standard*. Reino Unido: IT Governance Ltd.

CAPÍTULO VII: Anexos

Anexo 1: Matriz de consistencia

<table>
<tr><td colspan="5">Título: ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.
Autor: De La Cruz Santa Cruz, Claudia</td></tr>
<tr><th>Formulación del problema</th><th>Objetivos</th><th>Hipótesis</th><th>Variables</th><th>Diseño metodológico</th></tr>
<tr><td>Problema general:
¿De qué manera la implementación de la ISO 27001 mejora el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?</td><td>Objetivo general:
Demostrar que la implementación de la ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.</td><td>Hipótesis general:
La implementación de la ISO 27001 optimiza el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.</td><td>Variable Independiente:
ISO 27001
Dimensiones:
- Planificación
- Ejecución
- Verificación
- Actuar</td><td rowspan="2">Tipo de Investigación:
Aplicada.

Método y diseño de la investigación:
Investigación experimental, deductiva, hipotética y analítica.</td></tr>
<tr><td>Problemas específicos:</td><td>Objetivos específicos:</td><td>Hipótesis específicas:</td><td>Variable Dependiente:
Sistema de gestión de seguridad de la información</td></tr>
</table>

PE1: ¿De qué manera la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024? **PE 2:** ¿De qué manera la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la integridad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?	**OE1:** Demostrar que la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024. **OE2:** Demostrar que la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la integridad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.	**HE1:** La implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024. **HE2:** La implementación de la ISO 27001 la tasa de incidentes que impacta la integridad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.	**Dimensiones:** 1. Disponibilidad. 2. Integridad. 3. Confidencialidad.	**Población y Muestra:** Población: 114 Muestra: 20

PE3: ¿De qué manera la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024?	**OE 3:** Demostrar que la implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.	**HE3:** La implementación de la ISO 27001 reduce la tasa de incidentes que impacta la confidencialidad de la información en el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.		

Anexo 2. Matriz de operacionalización de variables

Tabla 12

Matriz de operacionalización de la variable ISO 27001

Variable independiente: ISO 27001 **Definición operacional:** **Matriz de operacionalización de la variable ISO 27001**					
Dimensiones	Definición conceptual	Definición operacional	Indicadores	Escala de medición	Escala valorativa (niveles o rangos)
-Planificación -Ejecución -Verificación -Actuar	La ISO 27001, orienta en el SGSI de una organización. Para asegurar la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2013).	La ISO 27001, brinda a las organizaciones procesos, políticas y controles para mitigar, prevenir y evaluar riesgos.	9.1.1 Políticas de control de acceso. 9.4.1 Restricción de acceso a la información. 12.3.1 Respaldo de la información. 12.2.1. Controles contra códigos maliciosos. 8.1.1 Inventario de activos. 11.2.4. Mantenimiento de equipos. (ISO/IEC, 2013)		

Tabla 13

Matriz de operacionalización de la variable Sistema de gestión de seguridad de la información.

Variable dependiente: Sistema de gestión de seguridad de la información

Definición operacional:

Matriz de operacionalización de la variable Sistema de gestión de seguridad de la información

Dimensiones	Definición conceptual	Definición operacional	Indicadores	Escala de medición	Escala valorativa (niveles o rangos)
- Disponibilidad - Integridad - Confidencialidad (Mata, 2022).	El SGSI, son un grupo políticas, pautas, procedimientos, recursos y actividades relacionados entre sí, para proteger su información crucial (Mata, 2022).	El SGSI, permite gestionar los incidentes de seguridad de la información. La tasa de incidentes se mide a través de indicadores de seguridad, como son la tasa de incidente que impacta la confidencialidad, integridad y disponibilidad de la información.	- Tasa de incidente que impacta la confidencialidad. - Tasa de incidente que impacta la integridad. - Tasa de incidente que impacta la disponibilidad. (Mata, 2022)	Porcentaje	Razón

Tabla 14

Variables y operacionalización

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Escala de medición	Escala valorativa (niveles o rangos)
ISO 27001	La ISO 27001, orienta en el SGSI del negocio. Para asegurar la CID (confidencialidad, integridad y disponibilidad) de la información. (ISO/IEC, 2013)	La ISO 27001, brinda a las organizaciones procesos, controles y políticas, para asegurar la información requerida para mitigar, prevenir y evaluar riesgos.	-Planificación -Ejecución -Verificación -Actuar	9.1.1 Políticas de control de acceso. 9.4.1 Restricción de acceso a la información. 12.3.1 Respaldo de la información. 12.2.1. Controles contra códigos maliciosos. 8.1.1 Inventario de activos. 11.2.4. Mantenimiento de equipos. (ISO/IEC, 2013)		
Sistema de gestión de la seguridad de la información	El SGSI, es la agrupación de políticas, pautas, procedimientos, y de recursos y actividades relacionados entre sí, para proteger su información crucial (Mata, 2022).	El SGSI, permite gestionar los incidentes de seguridad de la información. La tasa de incidentes se mide a través de indicadores de seguridad, como son la tasa de incidente que impacta la confidencialidad, integridad y disponibilidad de la	-Disponibilidad -Integridad -Confidencialidad (Mata, 2022).	- Tasa de incidentes que impacta la confidencialidad. - Tasa de incidentes que impacta la integridad. - Tasa de incidentes que impacta la disponibilidad. (Mata, 2022).	Porcentaje	Razón

		información.				

Anexo 3: Instrumentos

TEST DE CUMPLIMIENTO DE CONTROLES:

Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

TEST DE CUMPLIMIENTO

Objetivo: Test de cumplimiento de controles ISO 27001.

N°	**TPRE-001**	**Variable:** Sistema de gestión de seguridad de la información
Fecha Pre-test: 01/12/2023 - 08/12/2023		**ANEXO A ISO 27001**
Puntuación: 0 - 0.5 - 1		
Nivel de madurez: porcentaje		

	Pre-test	Puntuación			
	Controles	Completo	Parcial	Ninguno	Total
CONFIDENCIALIDAD	**9. Control de accesos**				
	9.1.1. Políticas de control de acceso.				
	1.- ¿Existen políticas específicas de seguridad de la información para los usuarios?				
	2.- ¿Se determinó quienes tienen acceso a la información, a qué información y bajo cuáles circunstancias?				
	9.4.1. Restricción de acceso a la información.				
	1.- ¿Se definieron lineamientos para restringir la información a los usuarios según sus actividades?				
	2.- ¿Se han tomado medidas preventivas al acceso no autorizado a la información?				
	Nivel de madurez de Confidencialidad				
INTEGRIDAD	**12. Seguridad de las operaciones**				
	12.2.1. Controles contra códigos maliciosos.				
	1.- ¿Los recursos informáticos cuentan con Antivirus para la detección de software malicioso o malware?				
	2.- ¿Existen lineamientos que ayuden a controlar la infección de códigos maliciosos?				
	12.3.1 Respaldo de la información.				
	1.- ¿Existe un sistema de copias de respaldo de la información?				
	2.- ¿Existen pruebas de restauración de copias de respaldo de la información?				
	Nivel de madurez de Integridad				
DISPONIBILIDAD	**8. Gestión de activos**				
	8.1.1 Inventario de activos.				
	1.- ¿Existen lineamientos para proteger, registrar y actualizar los activos del negocio?				
	2.- ¿Existe una clasificación para los activos de información?				
	11. Seguridad física y ambiental				
	11.2.4. Mantenimiento de equipos.				
	1.- ¿Existen lineamientos en materia de seguridad en oficinas y equipos?				
	2.- ¿Existen lineamientos en el caso ingresen equipos de cómputo de terceros?				
	Nivel de madurez de Disponibilidad				

Universidad Norbert Wiener
Powered by Arizona State University

FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD
"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

TEST DE CUMPLIMIENTO

Objetivo: Test de cumplimiento de controles ISO 27001.

N°	**TPOST-001**	**Variable:** Sistema de gestión de seguridad de la información	
Fecha Pre-test: 01/12/2023 - 08/12/2023		**ANEXO A ISO 27001**	
Puntuación: 0 - 0.5 - 1			
Nivel de madurez: porcentaje			

	Post-test	Puntuación			
	Controles	**Completo**	**Parcial**	**Ninguno**	**Total**
CONFIDENCIALIDAD	**9. Control de accesos**				
	9.1.1. Políticas de control de acceso.				
	1.- ¿Existen políticas específicas de seguridad de la información para los usuarios?				
	2.- ¿Se determinó quienes tienen acceso a la información, a qué información y bajo cuáles circunstancias?				
	9.4.1. Restricción de acceso a la información.				
	1.- ¿Se definieron lineamientos para restringir la información a los usuarios según sus actividades?				
	2.- ¿Se han tomado medidas preventivas al acceso no autorizado a la información?				
	Nivel de madurez de Confidencialidad				
INTEGRIDAD	**12. Seguridad de las operaciones**				
	12.2.1. Controles contra códigos maliciosos.				
	1.- ¿Los recursos informáticos cuentan con Antivirus para la detección de software malicioso o malware?				
	2.- ¿Existen lineamientos que ayuden a controlar la infección de códigos maliciosos?				
	12.3.1 Respaldo de la información.				
	1.- ¿Existe un sistema de copias de respaldo de la información?				
	2.- ¿Existen pruebas de restauración de copias de respaldo de la información?				
	Nivel de madurez de Integridad				
DISPONIBILIDAD	**8. Gestión de activos**				
	8.1.1 Inventario de activos.				
	1.- ¿Existen lineamientos para proteger, registrar y actualizar los activos del negocio?				
	2.- ¿Existe una clasificación para los activos de información?				
	11. Seguridad física y ambiental				
	11.2.4. Mantenimiento de equipos.				
	1.- ¿Existen lineamientos en materia de seguridad en oficinas y equipos?				
	2.- ¿Existen lineamientos en el caso ingresen equipos de cómputo de terceros?				
	Nivel de madurez de Disponibilidad				

GUÍA DE OBSERVACIÓN PRETEST:

Figura 8

Guía de Observación Pretest en vacío de Confidencialidad.

Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

Guía de Observación	
Objetivo: Medir la tasa de incidentes que impactan la confidencialidad.	
N° PRC-001	**Fecha Pre-test:** 01/12/2023 - 08/12/2023
Fórmula: TINIC = (CINC/TINC)*100	**Variable:** Sistema de gestión de seguridad de la información
TINIC: Tasa de incidentes que impacta la confidencialidad	**Dimensión:** Confidencialidad
CINC: Cantidad de incidentes de confidencialidad	**Libro:** Sistema integrado de gestión en seguridad - **Autor:** Correa
TINC: Total de Incidentes de confidencialidad	**ANEXO A ISO 27001**

Pre-test				
	Controles	CINC	TINC	TINIC
CONFIDENCIALIDAD	**9. Control de accesos**			
	9.1.1. Políticas de control de acceso.			
	9.4.1. Restricción de acceso a la información.			
			Promedio	

Figura 9

Guía de Observación Pretest en vacío de Integridad.

Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

Guía de Observación	
Objetivo: Medir la tasa de incidentes que impactan la integridad.	
N° PRI-001	**Fecha Pre-test:** 01/12/2023 - 08/12/2023
Fórmula: TINII = (CINI/TINI)*100	**Variable:** Sistema de gestión de seguridad de la información
TINII: Tasa de incidentes que impacta la integridad	**Dimensión:** Integridad
CINI: Cantidad de incidentes de integridad	**Libro:** Sistema integrado de gestión en seguridad - **Autor:** Correa
TINI: Total de Incidentes de integridad	**ANEXO A ISO 27001**

Pre-test				
	Controles	CINI	TINI	TINII
INTEGRIDAD	**12. Seguridad de las operaciones**			
	12.2.1. Controles contra códigos maliciosos.			
	12.3.1 Respaldo de la información.			
			Promedio	

Figura 10

Guía de Observación Pretest en vacío de Disponibilidad.

Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

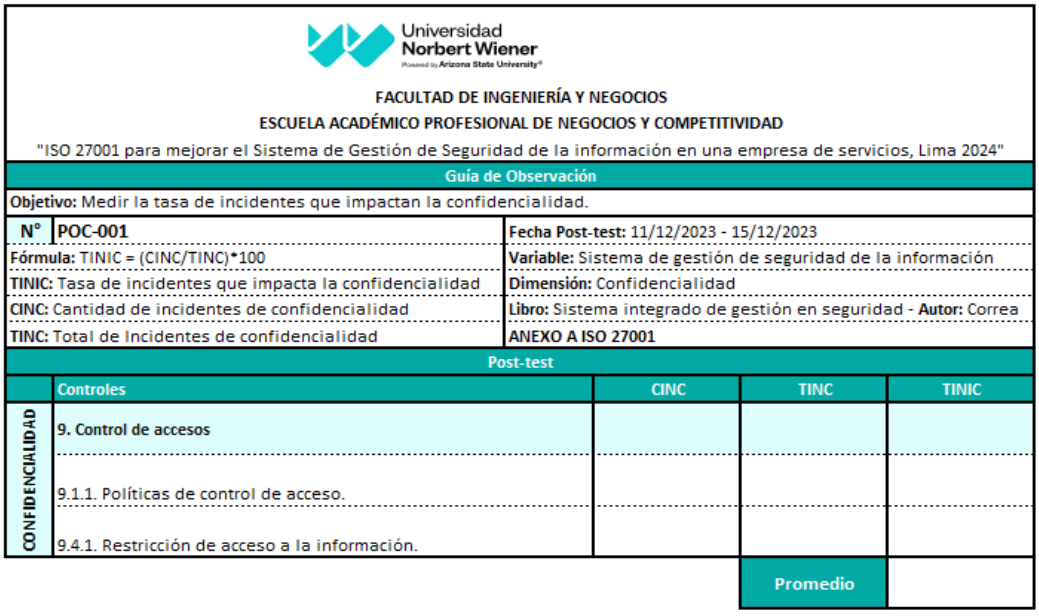
"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

Guía de Observación			
Objetivo: Medir la tasa de incidentes que impactan la disponiblidad.			
N°	**PRD-001**	**Fecha Pre-test:** 01/12/2023 - 08/12/2023	
Fórmula: TINID = (CIND/TIND)*100		**Variable:** Sistema de gestión de seguridad de la información	
TINID: Tasa de incidentes que impacta la disponibilidad		**Dimensión:** Disponibilidad	
CIND: Cantidad de incidentes de disponibilidad		**Libro:** Sistema integrado de gestión en seguridad - **Autor:** Correa	
TIND: Total de Incidentes de disponibilidad		**ANEXO A ISO 27001**	
Pre-test			
	Controles	**CIND**	**TIND**	**TINID**
INTEGRIDAD	**12. Seguridad de las operaciones**			
	12.2.1. Controles contra códigos maliciosos.			
	12.3.1 Respaldo de la información.			
			Promedio	

GUÍA DE OBSERVACIÓN POST-TEST:

Figura 11

Guía de Observación Post-test en vacío de Confidencialidad.



Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

Guía de Observación			
Objetivo: Medir la tasa de incidentes que impactan la confidencialidad.			
N°	**POC-001**	**Fecha Post-test:** 11/12/2023 - 15/12/2023	
Fórmula: TINIC = (CINC/TINC)*100		**Variable:** Sistema de gestión de seguridad de la información	
TINIC: Tasa de incidentes que impacta la confidencialidad		**Dimensión:** Confidencialidad	
CINC: Cantidad de incidentes de confidencialidad		**Libro:** Sistema integrado de gestión en seguridad - **Autor:** Correa	
TINC: Total de Incidentes de confidencialidad		**ANEXO A ISO 27001**	
Post-test			
	Controles	**CINC**	**TINC**	**TINIC**
CONFIDENCIALIDAD	**9. Control de accesos**			
	9.1.1. Políticas de control de acceso.			
	9.4.1. Restricción de acceso a la información.			
			Promedio	

Figura 12

Guía de Observación Post-test en vacío de Integridad.

Universidad Norbert Wiener
Powered by Arizona State University

FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD
"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

Guía de Observación	
Objetivo: Medir la tasa de incidentes que impactan la integridad.	
N° **POI-001**	**Fecha Post-test:** 11/12/2023 - 15/12/2023
Fórmula: TINII = (CAII/TII)*100	**Variable:** Sistema de gestión de seguridad de la información
TINII: Tasa de incidentes que impacta la integridad	**Dimensión:** Integridad
CINI: Cantidad de incidentes de integridad	**Libro:** Sistema integrado de gestión en seguridad - **Autor:** Correa
TINI: Total de Incidentes de integridad	**ANEXO A ISO 27001**

Post-test				
	Controles	CINI	TINI	TINII
INTEGRIDAD	**12. Seguridad de las operaciones**			
	12.2.1. Controles contra códigos maliciosos.			
	12.3.1 Respaldo de la información.			
			Promedio	

Figura 13

Guía de Observación Post-test en vacío de Disponibilidad.

Universidad Norbert Wiener
Powered by Arizona State University

FACULTAD DE INGENIERÍA Y NEGOCIOS
ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD
"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

Guía de Observación	
Objetivo: Medir la tasa de incidentes que impactan la disponibilidad.	
N° **POD-001**	**Fecha Post-test:** 11/12/2023 - 15/12/2023
Fórmula: TINID = (CIND/TIND)*100	**Variable:** Sistema de gestión de seguridad de la información
TINID: Tasa de incidentes que impacta la disponibilidad	**Dimensión:** Disponibilidad
CIND: Cantidad de incidentes de disponibilidad	**Libro:** Sistema integrado de gestión en seguridad - **Autor:** Correa
TIND: Total de Incidentes de disponibilidad	**ANEXO A ISO 27001**

Post-test				
	Controles	CIND	TIND	TINID
INTEGRIDAD	**12. Seguridad de las operaciones**			
	12.2.1. Controles contra códigos maliciosos.			
	12.3.1 Respaldo de la información.			
			Promedio	

CONSOLIDADO DEL PRETEST Y POSTTEST:

Figura 14

Formato del consolidado en vacío.

Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

CONSOLIDADO							
	PRETEST				POSTEST		
Ficha de registro	Tasa de incidentes Confidencialidad (pretest)	Tasa de incidentes Integridad (pretest)	Tasa de incidentes Disponibilidad (pretest)	Ficha de registro	Tasa de incidentes Confidencialidad (postest)	Tasa de incidentes Integridad (postest)	Tasa de incidentes Disponibilidad (postest)
RESULTADO PRETEST:				RESULTADO POSTEST:			

Figura 15

Formato del consolidado lleno.

Universidad Norbert Wiener

FACULTAD DE INGENIERÍA Y NEGOCIOS

ESCUELA ACADÉMICO PROFESIONAL DE NEGOCIOS Y COMPETITIVIDAD

"ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024"

CONSOLIDADO							
	PRETEST				POSTEST		
Ficha de registro	Tasa de incidentes Confidencialidad (pretest)	Tasa de incidentes Integridad (pretest)	Tasa de incidentes Disponibilidad (pretest)	Ficha de registro	Tasa de incidentes Confidencialidad (postest)	Tasa de incidentes Integridad (postest)	Tasa de incidentes Disponibilidad (postest)
PRC-001	88%	88%	88%	POC-001	0%	0%	0%
PRC-002	100%	100%	100%	POC-002	13%	13%	0%
PRC-003	100%	100%	100%	POC-003	13%	13%	10%
PRC-004	100%	100%	100%	POC-004	13%	13%	10%
PRC-005	100%	100%	100%	POC-005	13%	13%	10%
PRI-001	100%	100%	100%	POI-001	13%	13%	10%
PRI-002	100%	100%	100%	POI-002	13%	13%	10%
PRI-003	100%	100%	100%	POI-003	13%	13%	10%
PRI-004	100%	100%	100%	POI-004	13%	13%	10%
PRI-005	100%	100%	100%	POI-005	13%	13%	10%
PRD-001	100%	100%	100%	POD-001	13%	13%	10%
PRD-002	100%	100%	100%	POD-002	13%	13%	10%
PRD-003	100%	100%	100%	POD-003	13%	13%	10%
PRD-004	100%	100%	100%	POD-004	13%	13%	10%
PRD-005	100%	100%	100%	POD-005	13%	13%	13%
RESULTADO PRETEST:	99%	99%	99%	RESULTADO POSTEST:	12%	12%	9%

Anexo 4: Validez del instrumento

CARTA DE PRESENTACIÓN

Doctora: Díaz Reátegui, Mónica

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Es muy grato comunicarme con usted para expresarle mi saludo y, asimismo, hacer de su conocimiento que, siendo estudiante del programa del curso extracurricular de investigación formativa, requiero validar los instrumentos a fin de recoger la información necesaria para desarrollar mi investigación, con la cual optaré el grado de Ingeniera de Sistemas e Informática.

El título nombre de mi proyecto de investigación es "ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024" y, debido a que es imprescindible contar con la aprobación de docentes especializados para aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de ingeniería de sistemas.

El expediente de validación que le hago llegar contiene:

- Carta de presentación
- Matriz de consistencia (anexo 1)
- Matriz de operacionalización de las variables
- Certificado de validez de contenido de los instrumentos
- Instrumentos de recolección de datos

Expresándole los sentimientos de respeto y consideración, me despido de usted, no sin antes agradecer por la atención que dispense a la presente.

Atentamente,

Claudia De La Cruz Santa Cruz

DNI: 42922226

ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024

Nº	DIMENSIONES/ítems Variable 2: Sistema de Gestión de Seguridad de la Información	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existen políticas específicas de seguridad de la información para los usuarios	x		x		x		
2	Se determinó quienes tienen acceso a la información, a qué información y bajo cuáles circunstancias	x		x		x		
3	Se definieron lineamientos para restringir la información a los usuarios según sus actividades	x		x		x		
4	Se han tomado medidas preventivas al acceso no autorizado a la información	x		x		x		
	DIMENSION: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
5	Los recursos informáticos cuentan con Antivirus para la detección de software malicioso o malware	x		x		x		
6	Existen lineamientos que ayuden a controlar la infección de códigos maliciosos	x		x		x		
7	Existe un sistema de copias de respaldo de la información	x		x		x		
8	Existen pruebas de restauración de copias de respaldo de la información	x		x		x		
	DIMENSIÓN: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9	Existen lineamientos para proteger, registrar y actualizar los activos del negocio	x		x		x		
10	Existe una clasificación para los activos de información	x		x		x		
11	Existen lineamientos en materia de seguridad en oficinas y equipos	x		x		x		
12	Existen lineamientos en el caso ingresen equipos de cómputo de terceros	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: Dr./Mg. Mónica Díaz Reátegui

DNI: 09537647

Correo electrónico institucional: monica.diaz@uwiener.edu.pe

Especialidad del validador:

Metodólogo [ ]

Temático [x]

Estadístico [ ]

16 de enero de 2024

Firma del experto informante

Documentos para validar los instrumentos de medición a través de juicio de expertos

CARTA DE PRESENTACIÓN

Magister: Menacho Navarrete, Karem

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Es muy grato comunicarme con usted para expresarle mi saludo y, asimismo, hacer de su conocimiento que, siendo estudiante del programa del curso extracurricular de investigación formativa, requiero validar los instrumentos a fin de recoger la información necesaria para desarrollar mi investigación, con la cual optaré el grado de Ingeniera de Sistemas e Informática.

El título nombre de mi proyecto de investigación es "ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024" y, debido a que es imprescindible contar con la aprobación de docentes especializados para aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de ingeniería de sistemas.

El expediente de validación que le hago llegar contiene:

- Carta de presentación
- Matriz de consistencia (anexo 1)
- Matriz de operacionalización de las variables
- Certificado de validez de contenido de los instrumentos
- Instrumentos de recolección de datos

Expresándole los sentimientos de respeto y consideración, me despido de usted, no sin antes agradecer por la atención que dispense a la presente.

Atentamente,

Claudia De La Cruz Santa Cruz

DNI: 42922226

ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024

N°	DIMENSIONES/ítems Variable 2: Sistema de Gestión de Seguridad de la Información	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existen políticas específicas de seguridad de la información para los usuarios	X		X		X		
2	Se determinó quienes tienen acceso a la información, a qué información y bajo cuáles circunstancias	X		X		X		
3	Se definieron lineamientos para restringir la información a los usuarios según sus actividades	X		X		X		
4	Se han tomado medidas preventivas al acceso no autorizado a la información	X		X		X		
	DIMENSION: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
5	Los recursos informáticos cuentan con Antivirus para la detección de software malicioso o malware	X		X		X		
6	Existen lineamientos que ayuden a controlar la infección de códigos maliciosos	X		X		X		
7	Existe un sistema de copias de respaldo de la información	X		X		X		
8	Existen pruebas de restauración de copias de respaldo de la información	X		X		X		
	DIMENSIÓN: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9	Existen lineamientos para proteger, registrar y actualizar los activos del negocio	X		X		X		
10	Existe una clasificación para los activos de información	X		X		X		
11	Existen lineamientos en materia de seguridad en oficinas y equipos	X		X		X		
12	Existen lineamientos en el caso ingresen equipos de cómputo de terceros	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: Dr./Mg.Karem Menacho Navarrete

DNI: 24002602

Correo electrónico institucional: karem.menacho@uwiener.edu.pe

Especialidad del validador:

Metodólogo [ ]

Temático [X]

Estadístico [ ]

17 de enero de 2024

Firma del experto informante

CARTA DE PRESENTACIÓN

Magíster: Córdova Forero, Julio Alfredo Martin

Presente

Asunto: VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.

Es muy grato comunicarme con usted para expresarle mi saludo y, asimismo, hacer de su conocimiento que, siendo estudiante del programa del curso extracurricular de investigación formativa, requiero validar los instrumentos a fin de recoger la información necesaria para desarrollar mi investigación, con la cual optaré el grado de Ingeniera de Sistemas e Informática.

El título nombre de mi proyecto de investigación es "ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024" y, debido a que es imprescindible contar con la aprobación de docentes especializados para aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de ingeniería de sistemas.

El expediente de validación que le hago llegar contiene:

- Carta de presentación
- Matriz de consistencia (anexo 1)
- Matriz de operacionalización de las variables
- Certificado de validez de contenido de los instrumentos
- Instrumentos de recolección de datos

Expresándole los sentimientos de respeto y consideración, me despido de usted, no sin antes agradecer por la atención que dispense a la presente.

Atentamente,

Claudia De La Cruz Santa Cruz

DNI: 42922226

ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la información en una empresa de servicios, Lima 2024

N°	DIMENSIONES/ítems Variable 2: Sistema de Gestión de Seguridad de la Información	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION: Confidencialidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existen políticas específicas de seguridad de la información para los usuarios	X		X		X		
2	Se determinó quienes tienen acceso a la información, a qué información y bajo cuáles circunstancias	X		X		X		
3	Se definieron lineamientos para restringir la información a los usuarios según sus actividades	X		X		X		
4	Se han tomado medidas preventivas al acceso no autorizado a la información	X		X		X		
	DIMENSION: Integridad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
5	Los recursos informáticos cuentan con Antivirus para la detección de software malicioso o malware	X		X		X		
6	Existen lineamientos que ayuden a controlar la infección de códigos maliciosos	X		X		X		
7	Existe un sistema de copias de respaldo de la información	X		X		X		
8	Existen pruebas de restauración de copias de respaldo de la información	X		X		X		
	DIMENSIÓN: Disponibilidad	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9	Existen lineamientos para proteger, registrar y actualizar los activos del negocio	X		X		X		
10	Existe una clasificación para los activos de información	X		X		X		
11	Existen lineamientos en materia de seguridad en oficinas y equipos	X		X		X		
12	Existen lineamientos en el caso ingresen equipos de cómputo de terceros	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: Dr./Mg. Cordova Forero Julio Alfredo

DNI: 09924829

Correo electrónico institucional: julio.cordova@uwiener.edu.pe

Especialidad del validador:

Metodólogo [ ]

Temático [x]

Estadístico [ ]

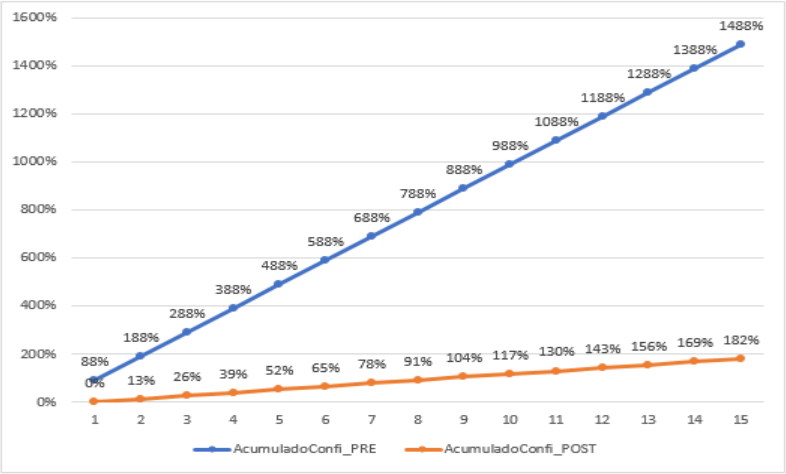
21 de enero de 2024

Firma del experto informante

Anexo 5: Confiabilidad del instrumento

Figura 16

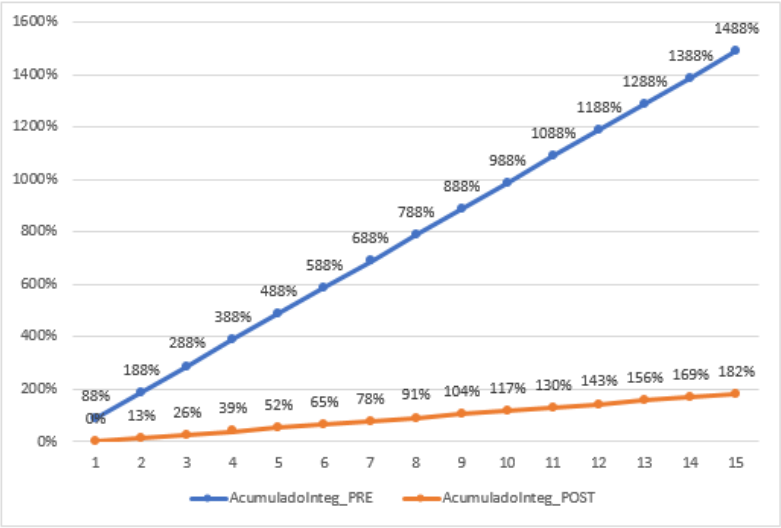
Confiabilidad de la tasa de incidentes que impactan la confidencialidad.



La Figura 27 muestra una tendencia creciente en la tasa de incidentes de confidencialidad, lo que indica la consistencia de los datos. La prueba de doble masas confirma que los datos acumulados son confiables.

Figura 17

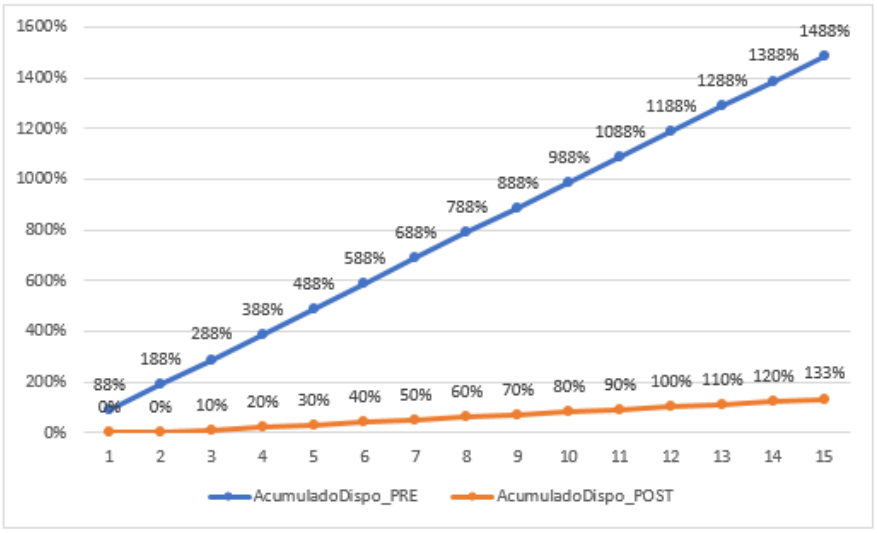
Confiabilidad de la tasa de incidentes que impactan la integridad.



La Figura 28 muestra una tendencia creciente en la tasa de incidentes de integridad, lo que indica la consistencia de los datos. La prueba de doble masas confirma que los datos acumulados son confiables.

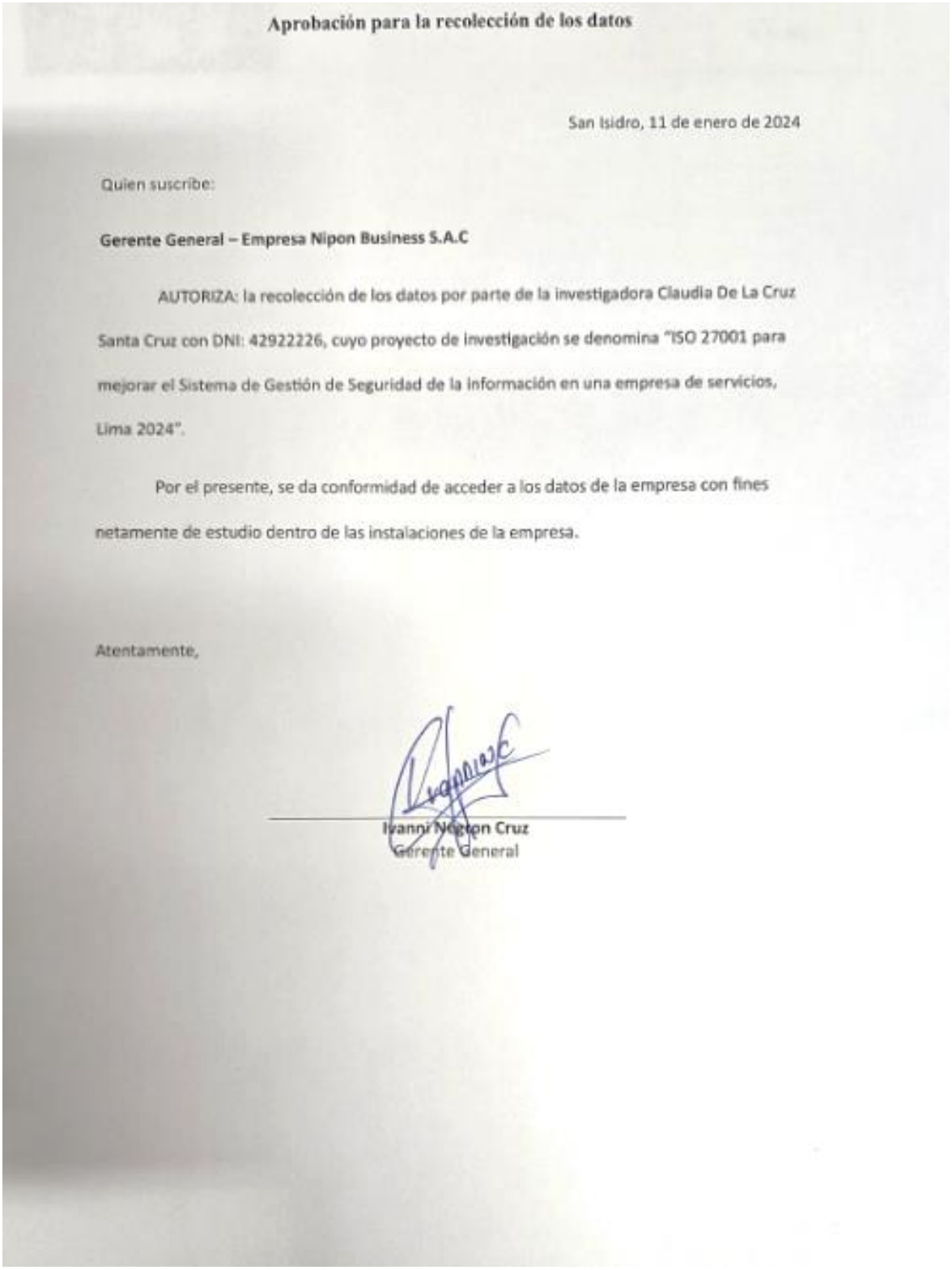
Figura 18

Confiabilidad de la tasa de incidentes que impactan la disponibilidad.



La Figura 29 muestra una tendencia creciente en la tasa de incidentes de disponibilidad, lo que indica la consistencia de los datos. La prueba de doble masas confirma que los datos acumulados son confiables.

Anexo 6: Carta de aprobación de la institución para la recolección de los datos



Aprobación para la recolección de los datos

San Isidro, 11 de enero de 2024

Quien suscribe:

Gerente General – Empresa Nipon Business S.A.C

AUTORIZA: la recolección de los datos por parte de la investigadora Claudia De La Cruz Santa Cruz con DNI: 42922226, cuyo proyecto de investigación se denomina "ISO 27001 para mejorar el Sistema de Gestión de Seguridad de la Información en una empresa de servicios, Lima 2024".

Por el presente, se da conformidad de acceder a los datos de la empresa con fines netamente de estudio dentro de las instalaciones de la empresa.

Atentamente,

Ivanni Negron Cruz
Gerente General

Anexo 7: Desarrollo de la solución

RFP (Request for Proposal)

"Sistema de Gestión de Seguridad de la Información (SGSI)"

2023-SG-01

INDICE

I. OBJETIVO

Disponer los lineamientos requeridos que permitan implementar los controles del "Anexo A" de la "ISO 27001", para que los procesos del "Sistema de Gestión de Seguridad de la información (SGSI)", brinden el soporte necesario para gestionar el aseguramiento de la información de la empresa Nipón Business S.A.C.

II. ALCANCE

Las disposiciones del presente manual de políticas, son de aplicación obligatoria para todo el personal que requiera consultar información acerca del SGSI y su aplicación dentro de la organización.

III. POLÍTICAS

DOMINIO "8. GESTIÓN DE ACTIVOS"

OBJETIVO DE CONTROL "8.1.Responsabilidad por los activos"

CONTROL "8.1.1.Inventario de activos"

a. Nipón Business S.A.C., se compromete a asegurar, registrar y actualizar los activos de información que estén implicados en los procedimientos que repercute el SGSI.

b. Acorde a lo establecido en el "Inventario de activos de la información", dichos activos se clasificarán como "altos" y "medios", por ende, deberán incluirse en el SGSI implantado. En caso la categoría sea "bajo", dicho activo será analizado y recategorizado en una próxima evaluación auditora.

DOMINIO "9. CONTROL DE ACCESOS"

OBJETIVO DE CONTROL "9.1.Requisitos para el control de accesos"

CONTROL "9.1.1.Políticas de control de acceso"

Se disponen los lineamientos para controlar los accesos en las "Políticas de control de acceso para usuarios".

OBJETIVO DE CONTROL "9.4. Control de acceso al sistema y aplicación"

CONTROL "9.4.1. Restricción de acceso a la información"

La empresa estableció los lineamientos de la restricción de acceso a la información contemplada en el documento llamado "Restricción de acceso a la información".

DOMINIO "11. SEGURIDAD FÍSICA Y AMBIENTAL"

OBJETIVO DE CONTROL "11.2.Seguridad de los equipos"

CONTROL "11.2.4.Mantenimiento de equipos"

a. Los lineamientos en materia de seguridad y mantenimiento de equipos están establecidos en el documento "Seguridad y mantenimiento de equipos".

b. Si los equipos de cómputo son de terceros, la empresa hace responsable a los terceros, considerando la protección de la información de la empresa.

DOMINIO "12. SEGURIDAD DE LAS OPERACIONES"

OBJETIVO DE CONTROL "12.2.Protección contra código malicioso"

CONTROL "12.2.1.Controles contra código malicioso"

a. Se dispone que, los equipos en general se les protegerá usando un software Antivirus.

b. El usuario y la Jefatura de TI, son responsables de proteger que el Antivirus no se deshabilite y se mantenga actualizado.

c. Con el fin de ejecutar una adecuada administración contra código malicioso se seguirán los siguientes criterios:

- Queda prohibido descargar, instalar o intentar instalar programas en los equipos de Nipón Business S.A.C., sin la autorización de la Jefatura de TI.
- Si se detectan códigos maliciosos en un dispositivo informático de la empresa, se tendrá que comunicar inmediatamente a la Jefatura de TI para que se desarrolle el protocolo definido.

- Se requiere implementar herramientas actualizadas que detecten y eliminen código malicioso automáticamente.
- Se requiere tener un plan de recuperación plasmado en un mapa de procesos ante cualquier incidencia que un "código malicioso" pueda generar.

OBJETIVO DE CONTROL "12.3.Respaldo"

CONTROL "2.3.1.Respaldo de la información"

Copias de respaldo de la información

- La Jefatura de TIC, debe corroborar la ejecución de copias de seguridad utilizando el Procedimiento establecido en el documento "Respaldo de la información".

Plan de prueba para restaurar copias de respaldo

- La Jefatura de TI, ejecutará el plan de prueba para restaurar copias de respaldo año tras año, mínimo 1 vez.
- El plan de prueba corroborará que la recuperación de datos grabados sea exitosa, de forma que, se garantice su propósito.

- Dichas pruebas los encargados deberán firmar y documentar debidamente, en el documento "FORM-01 – Acta de verificación de copias de seguridad".

IV. CONTROL DE CAMBIOS

Descripción	Versión	Fecha de Aprobación	Responsable
Primera versión	v1.0	01/12/2023	Jefatura de TI

V. RFP (Request for Proposal)

INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

1. OBJETIVO

Disponer los lineamientos que aseguren una gestión estándar del inventario de activos de la información en Nipón Business S.A.C.

2. ALCANCE

Primero procede con el "control de riesgos de seguridad de la información", luego culmina con el "registro y actualización de los formatos" correspondientes, a su vez, se aplica transversalmente a los procedimientos que conforman el alcance del SGSI y considera el valor y procesamiento de los riesgos, según la "ISO/IEC 27001".

3. TÉRMINOS, DEFINICIONES Y ABREVIATURAS

Abreviaturas:

- CID: "Confidencialidad, integridad y disponibilidad".

- SGSI: "Sistema de Gestión de Seguridad de la Información".

- **Activos de información:** Recurso contenedor de data que es considerada valiosa, esta puede ser física o digital, el cual, deberá ser protegido ante riesgos y amenazas. Como activo de información se considera al personal, información, hardware, software, entre otros.

- **Amenaza:** Evento o situación que puede causar daño a los activos de información de una organización.

- **Confidencialidad:** Principio que garantiza que la información sensible no sea revelada a terceros no autorizados; es decir, que solo puede ser conocida por el emisor y el receptor.

- **Disponibilidad:** Principio que garantiza que la información sensible sea asequible y utilizable para los usuarios con autorización en cualquier momento del día, cuando y donde sea requerido.

- **Evento (suceso):** Acontecimiento relevante detectado por un programa o persona.

    - Un evento se conforma de uno o más acontecimientos y contar con varias causas.

- Un evento puede referirse a una situación que no se materializa.

- Usualmente se refiere a "incidente " o "accidente".

- **Integridad:** Principio que permite salvaguardar la inalterabilidad y exactitud de los activos.

- **Proceso:** Grupo de tareas que interactúan entre sí y que transforman las entradas en salidas.

- **SGSI (Sistema de gestión de seguridad de la información):** componente del sistema de control global que se enfoca en los riesgos y tiene el objetivo de disponer, implantar, mantener y mejorar la seguridad.

- **Vulnerabilidad:** Debilidad detectada en un activo y que podría ser explotado por ataques.

4. INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

La efectividad de este proceso demanda que los propietarios de información de los diversos departamentos se involucren.

4.1 Inventario de activos de información

Su ejecución demanda entrevistar a los colaboradores principales de aquellos procedimientos establecidos en el alcance del SGSI, luego de ello, se llenará la información en el formato "FORM-2 – Inventario de activos de la información", lo siguiente:

a. Año: año de registro del activo en la matriz.

b. Proceso involucrado: descripción del procedimiento relacionado con activos de información.

A. Identificación de activos

Código del activo: Se refiere a la generación de un identificador de acuerdo con la disposición que se presenta a continuación:

AI.año.númerocorrelativo

- **AI:** sigla de "activo de información".
- **Año:** año de registro.
- **Número correlativo:** comienza desde el número "1".

Clase de activo: Refiere a su esencia (ver figura 1).

Figura 1

Clase de activo de información

N°	Clase de activo	Detalle
1	**Primario**	Procesos e información que corresponden al núcleo del negocio.
2	**De soporte**	Son todos los activos que penden de los primarios.

Tipo del activo: según su naturaleza (ver figura 2).

Figura 2

Tipo de activo de información

Clase	Tipo
Activo primario	Proceso y actividades del negocio
	Información física y/o digital
Activo de soporte	Contenedor
	Hardware
	Personal
	Servicio
	Sitio
	Software

Nombre de activo: Es el nombre asignado.

Descripción del activo: Es la breve explicación del activo identificado.

f. Propietario del activo: persona y/o área responsable de la producción, procesamiento, mantenimiento y aseguramiento del activo.

g. Custodio del activo: personal responsable de salvaguardar un activo.

h. Ubicación: ubicación "física o lógica" del activo. Para la ubicación física, se detalla el sitio y para la ubicación lógica, se detalla el archivo o del servidor de su alojamiento.

i. Clasificación: la clasificación se realiza siguiendo el siguiente criterio:

- Si el activo tiene calificación alta, quiere decir que, contiene información confidencial.
- Calificación media, quiere decir que, contiene información interna.
- Calificación baja, es decir, compuesto por información pública.

Figura 3: Clasificación

Nivel	Descripción
Pública	Se refiere a la información que se considera pública y que está disponible para los miembros de la organización y para el público en general, sin estar sujeta a ningún tipo de restricción
Interna	Se refiere a la información que solo está disponible para los miembros de la organización y que el acceso de personal externo (auditores, entidades reguladoras, consultores externos) se puede permitir de manera controlada y sujeto a condiciones específicas de acceso.
Confidencial	Es aquella información reservada que requiere autorización expresa de la Alta Dirección o del propietario del activo de información para que se pueda acceder o utilizar.

B. Valoración del activo

Calificación CID: Según el "nivel de confidencialidad, integridad y disponibilidad", se calificará el activo de información (ver figura 4).

Figura 4: Calificación CID

Nivel	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)
Bajo (1)	Activo cuya información puede ser difundida al público en general, sin embargo, **sólo será modificada por personas autorizadas.**	Activo cuya información que, **al ser modificada, de forma intencional o casual**, por personas o procesos autorizados o no autorizados **provoca daños de pequeña magnitud**.	Activo cuya información que, si no está disponible **no compromete procesos operativos importantes** de la empresa.
Medio (2)	Activo cuya información puede ser difundida **sólo al personal de las áreas que la gestionan** y modificada sólo por personal autorizado.	Activo cuya información que**, al ser modificada, intencional o casualmente**, por personas o procesos autorizados o **no autorizados provoca daños de mediana magnitud.**	Activo cuya información, es vital para la continuidad de la empresa. De no estar disponible, **existen canales alternativos** para contrarrestarlo.
Alto (3)	Activo cuya información será difundida sólo a fuentes autorizadas, controladas y debidamente identificadas. Será modificada y leída por un grupo reducido de personas autorizadas y claramente identificadas.	Activo cuya información que, al ser modificada, intencional o casualmente, por personas o procesos autorizados o no autorizados provoca daños de gran magnitud en la empresa.	Activo cuya información que utiliza es indispensable para la continuidad de la empresa.

Valor del activo: Es la estimación del "Valor del Activo" (VdA), es decir, el total de los valores de calificación en referencia a la "Confidencialidad, integridad y disponibilidad", para ello se aplica el siguiente cálculo:

$$VdA = C + I + D$$

Tasación del activo: Es el intervalo de tasación del activo (ver figura 5).

Figura 5: Calificación del activo de información

Valor	Tasación	Descripción
3 – 4	Bajo	Activos secundarios, que constituyen información para la toma de decisiones de un área específica. No compromete ningún proceso crítico de la organización.
5 – 6	Medio	Constituye un soporte para los activos importantes de la organización. La información puede estar replicada en varias fuentes o existen medios alternos. Puede comprometer los procesos críticos de la organización.
7 – 9	Alto	Activo importante para la organización. Su disponibilidad es necesaria para los procesos críticos de la organización.

C. Revisión de activos

Estado del activo: Sirve para identificar el estado del activo y se registra como "activo" o "dado de baja".

Fecha de baja: Es la fecha de registro que se dio de baja el activo.

4.2 Formato

	FORMATO
	FORM-2 – Inventario de activos de la información

Fecha de actualización de matriz:	Responsable de actualización de matriz:	

ACTIVOS DE LA INFORMACIÓN

Año	Código del activo	Clase del activo	Tipo de activo	Nombre del activo	Descripción del activo	Propietario del activo	Custodio del activo	Ubicación del activo (física o lógica)	Clasificación	Clasificación CID			Valor del activo	Tasación del activo	Estado del activo	Fecha de baja del activo
										Confidencialidad	Integridad	Disponibilidad				

Políticas de control de acceso para usuarios

POLÍTICAS DE CONTROL DE ACCESO PARA USUARIOS

OBJETIVO

Disponer las políticas y lineamientos del "Sistema de Gestión de Seguridad de la Información (SGSI)" necesarias para implantar la "ISO27001", para lograr los objetivos establecidos.

ALCANCE

La política se aplicará de forma transversal de los departamentos, empleados que estén en planilla o brinden servicios a la empresa NIPON BUSINESS S.A.C.

POLÍTICA DE CONTROL DE ACCESOS

- Toda cuenta de usuario será "única y exclusiva" para cada trabajador, el cual, será responsable por toda actividad que sea ejecutada con dicha cuenta.

- La implementación de contraseñas fuertes es necesaria en los sistemas de información.

- Está estrictamente prohibido tratar de acceder a la "infraestructura tecnológica" utilizando la cuenta de otra persona.

- La asignación del "nivel de acceso a un sistema de información" se realizará en función de:
    - Su clasificación.
    - Las funciones o rol.
    - El perfil estandarizado.
    - Revisión periódica.
    - Eliminación y alteración de los privilegios de acceso.

- Las sesiones de conexión de los sistemas de información, deberán desconectarse automáticamente tras un periodo definido de inactividad.

- El acceso a los aplicativos informáticos será asignado según la identificación previa de requerimientos de la entidad y de la seguridad.

- Los activos informáticos se asignarán a un encargado para que salvaguarde el buen uso de los mismos.
- Los accesos con altos privilegios (usuarios administradores) serán de igual modo controlados a mediante un procedimiento formal.
- Se revisará periódicamente que los permisos de las cuentas de personal desvinculado fueron re-vocados y/o inactivados.
- Se revisará regularmente que los permisos otorgados al personal sean los apropiados según las tareas que realizan.
- La entrada a repositorios con código fuente debe ser regulada por la Jefatura de TI.

Restricción de acceso a la información

NIPON BUSINESS S.A.C	**RFP (Request for Proposal) "SGSI"**	CÓDIGO	2023-SG-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

1. OBJETIVO

Disponer lineamientos en referencia a la "Restricción de acceso a la información" de propiedad de NIPON BUSINESS S.A.C., con el fin de garantizar la CID (confidencialidad, integridad y disponibilidad) de la información.

2. ALCANCE

Comprende a todo el personal que labora o hace uso de programas informáticos, sistemas o aplicaciones de propiedad de NIPON BUSINESS S.A.C.

3. RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

- Solo se dará acceso a ciertas funciones de las aplicaciones informáticas y a su información, únicamente al personal de apoyo y usuarios autorizados.
- Se debe controlar los derechos de acceso, como son la lectura, escritura, borrado y ejecución.

- Se debe garantizar que los sistemas de aplicación gestores de información sensible, solo contengan la información correspondiente para el uso de la salida y que, se envíen únicamente, a los terminales y sitios autorizados. Así mismo, se debe revisar de forma periódica dichas salidas, para garantizar la supresión de información redundante.

Mantenimiento de equipos

NIPON BUSINESS S.A.C	**RFP (Request for Proposal) "SGSI"**	CÓDIGO	2023-SG-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

MANTENIMIENTO DE EQUIPOS

1. OBJETIVO

Hacer de conocimiento a todo el personal sobre los lineamientos en referencia al cuidado de equipos pertenecientes a NIPON BUSINESS S.A.C., para garantizar así la CID (confidencialidad, integridad y disponibilidad) de la información.

2. ALCANCE

Comprende a todos los colaboradores o a los que hacen uso de las aplicaciones informáticas de propiedad de la empresa.

3. DEFINICIONES

- **Equipos de cómputo:** Dispositivo electrónicos que permiten el procesamiento de información.

- **Equipo de comunicación:** Dispositivo electrónico empleado para transmitir mensajes de voz y/o datos.

- Usuario: Personal nombrado o contratado que desarrolla actividades o funciones en nombre o al servicio de NIPON BUSINESS S.A.C.

- Personal externo: Aquellos contratistas, proveedores, fiscalizadores, consultores y visitantes.

- Incidentes de seguridad de los equipos de cómputo: hecho o evento que podría dañar la salvaguarda e integridad de los dispositivos informáticos.

4. RESPONSABILIDADES

- Área de sistemas e informática y personal nombrado o contratado de la empresa.

5. SEGURIDAD EN EL MANTENIMIENTO DE EQUIPOS

- Realizar mantenimiento de los dispositivos informáticos según recomendaciones definidas por el fabricante.

- Se deben documentar aquellas fallas tanto reales como sospechosas.

- Deberá documentarse el mantenimiento preventivo y de reparación de los dispositivos.

- Solo personal autorizado podrá realizar la reparación y mantenimiento de los equipos.

- Se debe comunicar oportunamente la realización de mantenimiento preventivo de equipos.

- En caso de haber equipos de terceros dentro de los ambientes de la empresa, el área de TI deberá normar al respecto, considerando la seguridad de la información.

- En el caso que los usuarios requieran el cambio de algún equipo, deberán solicitarlo únicamente al área de TI.

NIPON BUSINESS S.A.C	**RFP (Request for Proposal) "SGSI"**	CÓDIGO	2023-SG-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

Controles contra código malicioso

CONTROLES CONTRA CÓDIGO MALICIOSO

1. OBJETIVO

Establecer los controles contra código malicioso o malwares, para garantizar la CID (confidencialidad, integridad y disponibilidad) de la información de la empresa NIPON BUSINESS S.A.C.

2. ALCANCE

Comprende a todos los colaboradores que hacen uso de las aplicaciones informáticas de propiedad de la empresa.

3. CONTROLES CONTRA CÓDIGO MALICIOSO

a. Disponer que los equipos estén protegidos con la instalación de un software Antivirus.

b. El usuario y la Jefatura de TI, son responsables de garantizar que el software antivirus no se desactive bajo ninguna circunstancia y que esté actualizado.

c. Para el control contra códigos maliciosos se deberán seguir los siguientes lineamientos.

- Prohibir la descarga, instalación o intento de instalación de software sin autorización de la Jefatura de TI.
- El colaborador que detecte código malicioso en un dispositivo informático, debe notificar inmediatamente a la Jefatura de TI para implementen el procedimiento correspondiente.
- Es necesario disponer de herramientas esenciales y actualizadas que posibiliten la detección y eliminación automática de software malicioso.
- Es necesario disponer de procedimientos para la restauración de información en caso exista una incidencia generada por software malicioso.

Respaldo de la información

NIPON BUSINESS S.A.C	**RFP (Request for Proposal) "SGSI"**	CÓDIGO	2023-SG-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

RESPALDO DE LA INFORMACIÓN

1. OBJETIVO

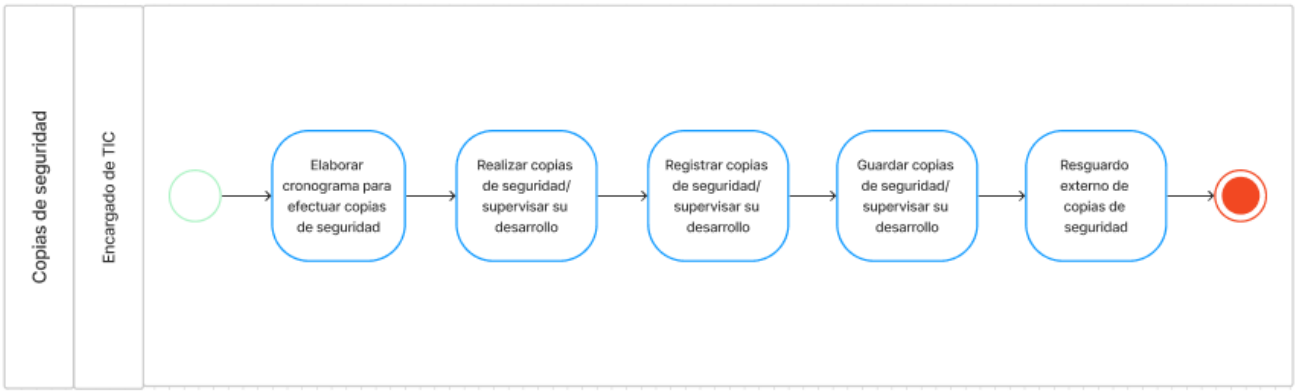
Disponer de lineamientos para la ejecución y verificación de las copias de seguridad de la información de NIPON BUSINESS S.A.C.

2. ALCANCE

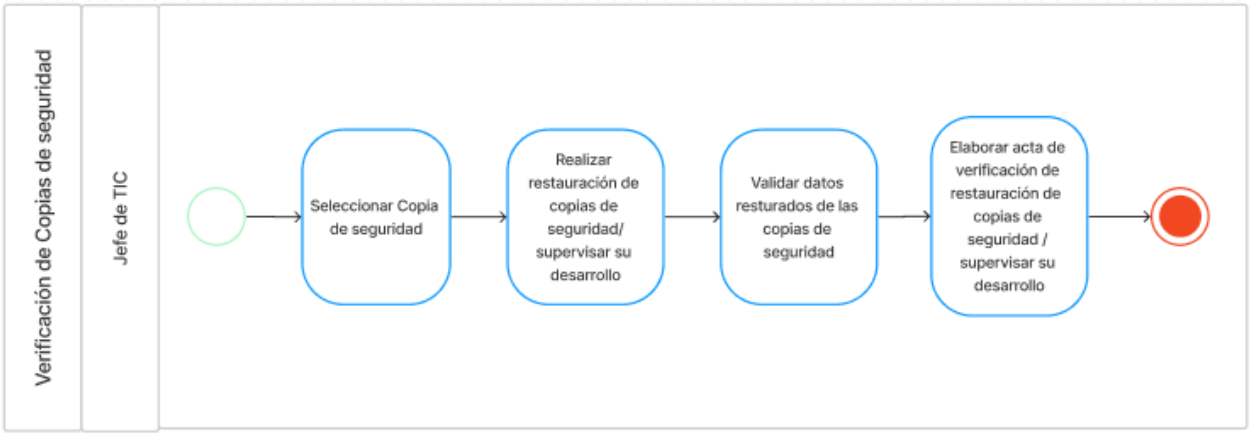
El área que ejecutará los lineamientos de respaldo de la información es el área TIC.

3. DIAGRAMAS DE MODELO PROCESOS

- **DIAGRAMA DE FLUJO DE COPIAS DE SEGURIDAD**



- **DIAGRAMA DE FLUJO DE VERIFICACIÓN DE COPIAS DE SEGURIDAD**



5.1 Evidencias de aplicación de controles

Evidencia 1:

CONTROL "8.1.1.Inventario de activos"
Formato Form2-Inventario de activos de la información

Año	Código del activo	Clase del activo	Tipo de activo	Nombre del activo	Descripción del activo	Propietario del activo
2023	AI.2023.001	Primario	Información digital	Documentos digitales	Documentos generados por la empresa.	Nipon Business S.A.C
2023	AI.2023.002	De Soporte	Hardware	Computadora Desktop ENKORE	Dispositivo informático - ENKORE Serial No.8RR6FF0	Nipon Business S.A.C
2023	AI.2023.003	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.7D127D60	Nipon Business S.A.C
2023	AI.2023.004	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.8C517B70	Nipon Business S.A.C
2023	AI.2023.005	De Soporte	Hardware	Computadora Desktop ENKORE	Dispositivo informático - ENKORE Serial No.2R72FF0	Nipon Business S.A.C
2023	AI.2023.006	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.9B431B70	Nipon Business S.A.C
2023	AI.2023.007	De Soporte	Software	Página web	Archivos en PHP, CSS para la web en construcción	Nipon Business S.A.C
2023	AI.2023.008	Primario	Proceso y actividades del negocio	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.5T424D80	Nipon Business S.A.C
2023	AI.2023.009	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.3U566W56	Nipon Business S.A.C

Custodio del activo	Ubicación del activo (física o lógica)	Clasificación	Clasificación CID			Valor del activo	Tasación del activo	Estado del activo	Fecha de baja del activo
			Confidencialidad	Integridad	Disponibilidad				
Ivanni Negron	AI.2023.002-Unidad C, carpeta Nipon, subcarpeta C	Confidencial	3	3	3	9	Alto	Activo	-
Ivanni Negron	2do Piso	Interna	2	3	3	8	Alto	Activo	-
Roberto Fueros	Unidad C, carpeta Nipon, subcarpeta Contabilidad	Confidencial	3	3	3	9	Alto	Activo	-
Julio Gonzalez	2do Piso	Interna	2	3	2	7	Alto	Activo	-
Karina Rojas	1er Piso	Interna	2	3	3	8	Alto	Activo	-
Melissa Reyes	1er Piso	Interna	2	2	2	6	Medio	Activo	-
Mario Peña B.	Unidad D, carpeta Xampp, subcarpeta NiponWeb	Interna	2	2	2	6	Medio	Activo	-
Giovanni Tuesta	Unidad C, carpeta Nipon, subcarpeta Estrategia	Confidencial	3	3	3	9	Alto	Activo	-
Jaime Alvarado	1er Piso	Interna	2	3	2	7	Alto	Activo	-

FORMATO

FORM-2 – Inventario de activos de la información

Fecha de actualización de matriz:	Responsable de actualización de matriz:	Responsable de TIC

ACTIVOS DE LA INFORMACIÓN

Año	Código del activo	Clase del activo	Tipo de activo	Nombre del activo	Descripción del activo	Propietario del activo	Custodio del activo	Ubicación del activo (física o lógica)	Clasificación	Clasificación CID			Valor del activo	Tasación del activo	Estado del activo	Fecha de baja del activo
										Confidencialidad	Integridad	Disponibilidad				
2023	AI.2023.001	Primario	Información digital	Documentos digitales	Documentos generados por la empresa.	Nipon Business S.A.C	Ivanni Negron	AI.2023.002-Unidad C, carpeta Nipon, subcarpeta C	Confidencial	3	3	3	9	Alto	Activo	-
2023	AI.2023.002	De Soporte	Hardware	Computadora Desktop ENKORE	Dispositivo informático - ENKORE Serial No.8RR6FF0	Nipon Business S.A.C	Ivanni Negron	2do Piso	Interna	2	3	3	8	Alto	Activo	-
2023	AI.2023.003	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.7D127D60	Nipon Business S.A.C	Roberto Fueros	Unidad C, carpeta Nipon, subcarpeta Contabilidad	Confidencial	3	3	3	9	Alto	Activo	-
2023	AI.2023.004	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.8C517B70	Nipon Business S.A.C	Julio Gonzalez	2do Piso	Interna	2	3	2	7	Alto	Activo	-
2023	AI.2023.005	De Soporte	Hardware	Computadora Desktop ENKORE	Dispositivo informático - ENKORE Serial No.2R72FF0	Nipon Business S.A.C	Karina Rojas	1er Piso	Interna	2	3	3	8	Alto	Activo	-
2023	AI.2023.006	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.9B431B70	Nipon Business S.A.C	Melissa Reyes	1er Piso	Interna	2	2	2	6	Medio	Activo	-
2023	AI.2023.007	De Soporte	Software	Página web	Archivos en PHP, CSS para la web en construcción	Nipon Business S.A.C	Mario Peña B.	Unidad D, carpeta Xampp, subcarpeta NiponWeb	Interna	2	2	2	6	Medio	Activo	-
2023	AI.2023.008	Primario	Proceso y actividades del negocio	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.5T424D80	Nipon Business S.A.C	Giovanni Tuesta	Unidad C, carpeta Nipon, subcarpeta Estrategia	Confidencial	3	3	3	9	Alto	Activo	-
2023	AI.2023.009	De Soporte	Hardware	Laptop TOSHIBA	Dispositivo informático - TOHIBA Serial No.3U566W56	Nipon Business S.A.C	Jaime Alvarado	1er Piso	Interna	2	3	2	7	Alto	Activo	-

Mario Peña B.
Responsable de TIC

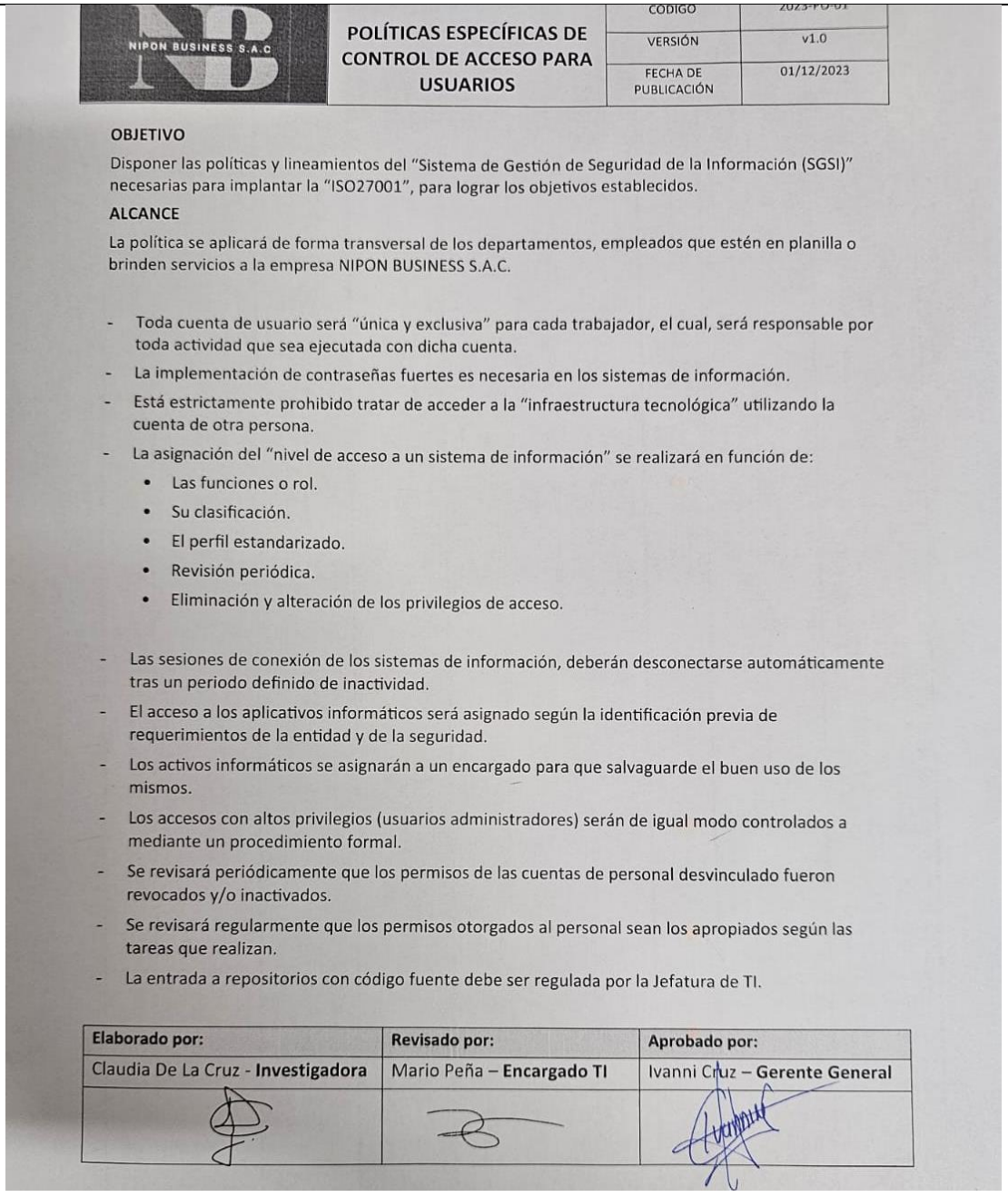
Activo registrado: Laptop TOSHIBA

Custodio: Melissa Reyes

Estado: Activo

Evidencia 2:

CONTROL "9.1.1.Políticas de control de acceso"
Políticas de control de acceso para usuarios



NIPON BUSINESS S.A.C	POLÍTICAS ESPECÍFICAS DE CONTROL DE ACCESO PARA USUARIOS	CÓDIGO	2023-PO-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

OBJETIVO

Disponer las políticas y lineamientos del "Sistema de Gestión de Seguridad de la Información (SGSI)" necesarias para implantar la "ISO27001", para lograr los objetivos establecidos.

ALCANCE

La política se aplicará de forma transversal de los departamentos, empleados que estén en planilla o brinden servicios a la empresa NIPON BUSINESS S.A.C.

- Toda cuenta de usuario será "única y exclusiva" para cada trabajador, el cual, será responsable por toda actividad que sea ejecutada con dicha cuenta.
- La implementación de contraseñas fuertes es necesaria en los sistemas de información.
- Está estrictamente prohibido tratar de acceder a la "infraestructura tecnológica" utilizando la cuenta de otra persona.
- La asignación del "nivel de acceso a un sistema de información" se realizará en función de:
  - Las funciones o rol.
  - Su clasificación.
  - El perfil estandarizado.
  - Revisión periódica.
  - Eliminación y alteración de los privilegios de acceso.

- Las sesiones de conexión de los sistemas de información, deberán desconectarse automáticamente tras un periodo definido de inactividad.
- El acceso a los aplicativos informáticos será asignado según la identificación previa de requerimientos de la entidad y de la seguridad.
- Los activos informáticos se asignarán a un encargado para que salvaguarde el buen uso de los mismos.
- Los accesos con altos privilegios (usuarios administradores) serán de igual modo controlados a mediante un procedimiento formal.
- Se revisará periódicamente que los permisos de las cuentas de personal desvinculado fueron revocados y/o inactivados.
- Se revisará regularmente que los permisos otorgados al personal sean los apropiados según las tareas que realizan.
- La entrada a repositorios con código fuente debe ser regulada por la Jefatura de TI.

Elaborado por:	Revisado por:	Aprobado por:
Claudia De La Cruz - **Investigadora**	Mario Peña – **Encargado TI**	Ivanni Cruz – **Gerente General**

Evidencia 3:

CONTROL "9.4.1. Restricción de acceso a la información"

Restricción de acceso a la información

NIPON BUSINESS S.A.C	RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	CÓDIGO	2023-PO-02
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	02/12/2023

OBJETIVO

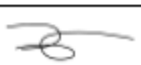
Disponer lineamientos en referencia a la "Restricción de acceso a la información" de propiedad de NIPON BUSINESS S.A.C., con el fin de garantizar la CID (confidencialidad, integridad y disponibilidad) de la información.

ALCANCE

Comprende a todo el personal que labora o hace uso de programas informáticos, sistemas o aplicaciones de propiedad de NIPON BUSINESS S.A.C.

RESTRICCIÓN DE ACCESO A LA INFORMACIÓN

- Solo se dará acceso a ciertas funciones de las aplicaciones informáticas y a su información, únicamente al personal de apoyo y usuarios autorizados.
- Se debe controlar los derechos de acceso, como son la lectura, escritura, borrado y ejecución.
- Se debe garantizar que los sistemas de aplicación gestores de información sensible, solo contengan la información correspondiente para el uso de la salida y que, se envíen únicamente, a los terminales y sitios autorizados. Así mismo, se debe revisar de forma periódica dichas salidas, para garantizar la supresión de información redundante.

Elaborado por:	Revisado por:	Aprobado por:
Claudia De La Cruz - Investigadora	Mario Peña – Encargado TI	Ivanni Cruz – Gerente General
		

Evidencia 4:

CONTROL "11.2.4. Mantenimiento de equipos"
Lineamiento para mantenimiento de equipos

NIPON BUSINESS S.A.C	MANTENIMIENTO DE EQUIPOS	CÓDIGO	2023-PO-03
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	02/12/2023

OBJETIVO

Hacer de conocimiento a todo el personal sobre los lineamientos en referencia al cuidado de equipos pertenecientes a NIPON BUSINESS S.A.C., para garantizar así la CID (confidencialidad, integridad y disponibilidad) de la información.

ALCANCE

Comprende a todos los colaboradores o a los que hacen uso de las aplicaciones informáticas de propiedad de la empresa.

DEFINICIONES

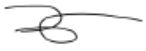
- **Equipos de cómputo:** Dispositivo electrónicos que permiten el procesamiento de información.
- **Equipo de comunicación:** Dispositivo electrónico empleado para transmitir mensajes de voz y/o datos.
- **Usuario:** Personal nombrado o contratado que desarrolla actividades o funciones en nombre o al servicio de NIPON BUSINESS S.A.C.
- **Personal externo:** Aquellos contratistas, proveedores, fiscalizadores, consultores y visitantes.
- **Incidentes de seguridad de los equipos de cómputo:** hecho o evento que podría dañar la la salvaguarda e integridad de los dispositivos informáticos.

RESPONSABILIDADES

- Área de sistemas e informática y personal nombrado o contratado de la empresa.

SEGURIDAD EN EL MANTENIMIENTO DE EQUIPOS

- Realizar mantenimiento de los dispositivos informáticos según recomendaciones definidas por el fabricante.
- Se deben documentar aquellas fallas tanto reales como sospechosas.
- Deberá documentarse el mantenimiento preventivo y de reparación de los dispositivos.
- Solo personal autorizado podrá realizar la reparación y mantenimiento de los equipos.
- Se debe comunicar oportunamente la realización de mantenimiento preventivo de equipos.
- En caso de haber equipos de terceros dentro de los ambientes de la empresa, el área de TI deberá normar al respecto, considerando la seguridad de la información.
- En el caso que los usuarios requieran el cambio de algún equipo, deberán solicitarlo únicamente al área de TI.

Elaborado por:	Revisado por:	Aprobado por:
Claudia De La Cruz - **Investigadora**	Mario Peña – **Encargado TI**	Ivanni Cruz – **Gerente General**
		

Evidencia 5:

CONTROL "12.2.1. Controles contra código malicioso"
Controles contra código malicioso

NIPON BUSINESS S.A.C	CONTROLES CONTRA CÓDIGO MALICIOSO	CÓDIGO	2023-PO-04
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

OBJETIVO

Establecer los controles contra código malicioso o malwares, para garantizar la CID (confidencialidad, integridad y disponibilidad) de la información de la empresa NIPON BUSINESS S.A.C.

ALCANCE

Comprende a todos los colaboradores que hacen uso de las aplicaciones informáticas de propiedad de la empresa.

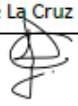
CONTROLES CONTRA CÓDIGO MALICIOSO

a. Disponer que los equipos estén protegidos con la instalación de un software Antivirus.

b. El usuario y la Jefatura de TI, son responsables de garantizar que el software antivirus no se desactive bajo ninguna circunstancia y que esté actualizado.

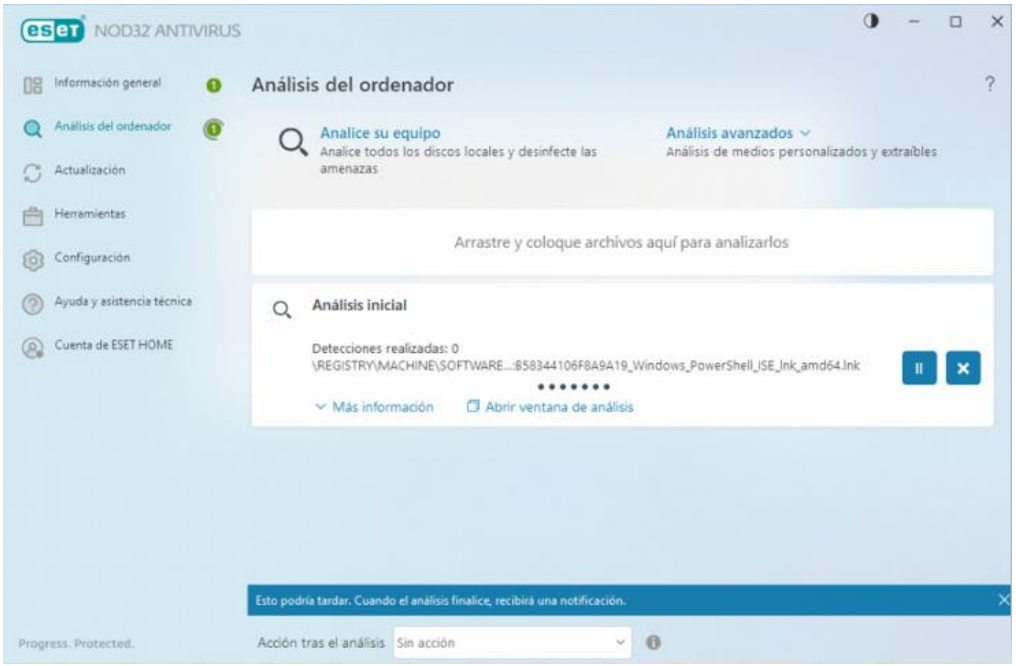
c. Para el control contra códigos maliciosos se deberán seguir los siguientes lineamientos.

- Prohibir la descarga, instalación o intento de instalación de software sin autorización de la Jefatura de TI.
- El colaborador que detecte código malicioso en un dispositivo informático, debe notificar inmediatamente a la Jefatura de TI para implementen el procedimiento correspondiente.
- Es necesario disponer de herramientas esenciales y actualizadas que posibiliten la detección y eliminación automática de software malicioso.
- Es necesario disponer de procedimientos para la restauración de información en caso exista una incidencia generada por software malicioso.

Elaborado por:	Revisado por:	Aprobado por:
Claudia De La Cruz - **Investigadora**	Mario Peña – **Encargado TI**	Ivanni Cruz – **Gerente General**
		

- Se procedió a ejecutar la instalación del antivirus ESET.

- A continuación, se analiza el dispositivo informático.



NIPON BUSINESS S.A.C	**RFP (Request for Proposal) "SGSI"**	CÓDIGO	2023-SG-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

Evidencia 6:

CONTROL "2.3.1.Respaldo de la información"
Respaldo de la información

NIPON BUSINESS S.A.C	MANTENIMIENTO DE EQUIPOS	CÓDIGO	2023-PO-03
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	02/12/2023

OBJETIVO

Hacer de conocimiento a todo el personal sobre los lineamientos en referencia al cuidado de equipos pertenecientes a NIPON BUSINESS S.A.C., para garantizar así la CID (confidencialidad, integridad y disponibilidad) de la información.

ALCANCE

Comprende a todos los colaboradores o a los que hacen uso de las aplicaciones informáticas de propiedad de la empresa.

DEFINICIONES

- **Equipos de cómputo:** Dispositivo electrónicos que permiten el procesamiento de información.
- **Equipo de comunicación:** Dispositivo electrónico empleado para transmitir mensajes de voz y/o datos.
- **Usuario:** Personal nombrado o contratado que desarrolla actividades o funciones en nombre o al servicio de NIPON BUSINESS S.A.C.
- **Personal externo:** Aquellos contratistas, proveedores, fiscalizadores, consultores y visitantes.
- **Incidentes de seguridad de los equipos de cómputo:** hecho o evento que podría dañar la la salvaguarda e integridad de los dispositivos informáticos.

RESPONSABILIDADES

- Área de sistemas e informática y personal nombrado o contratado de la empresa.

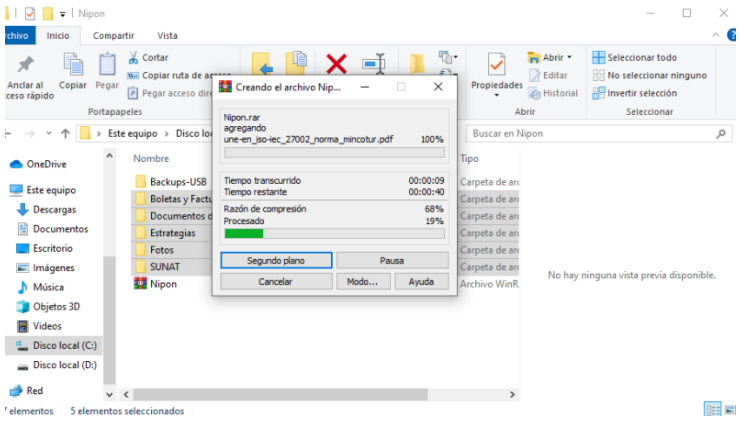
SEGURIDAD EN EL MANTENIMIENTO DE EQUIPOS

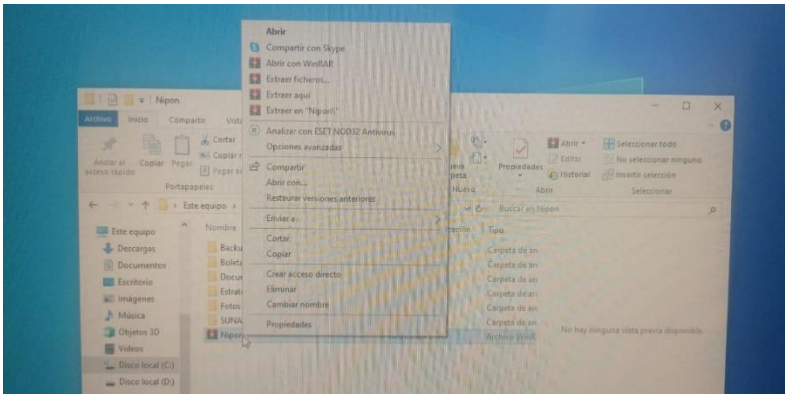
- Realizar mantenimiento de los dispositivos informáticos según recomendaciones definidas por el fabricante.
- Se deben documentar aquellas fallas tanto reales como sospechosas.
- Deberá documentarse el mantenimiento preventivo y de reparación de los dispositivos.
- Solo personal autorizado podrá realizar la reparación y mantenimiento de los equipos.
- Se debe comunicar oportunamente la realización de mantenimiento preventivo de equipos.
- En caso de haber equipos de terceros dentro de los ambientes de la empresa, el área de TI deberá normar al respecto, considerando la seguridad de la información.
- En el caso que los usuarios requieran el cambio de algún equipo, deberán solicitarlo únicamente al área de TI.

Elaborado por:	Revisado por:	Aprobado por:
Claudia De La Cruz - Investigadora	Mario Peña – Encargado TI	Ivanni Cruz – Gerente General

REALIZAR COPIA DE SEGURIDAD

- Se procede a realizar la copia de seguridad de la información del activo con código AI.2023.02, supervisado por el encargado de TI.

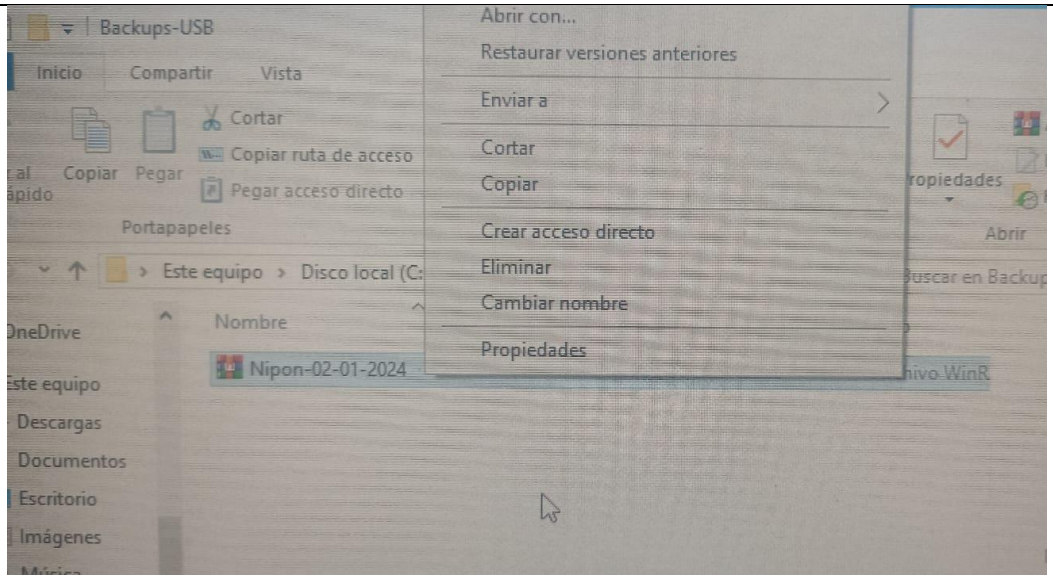




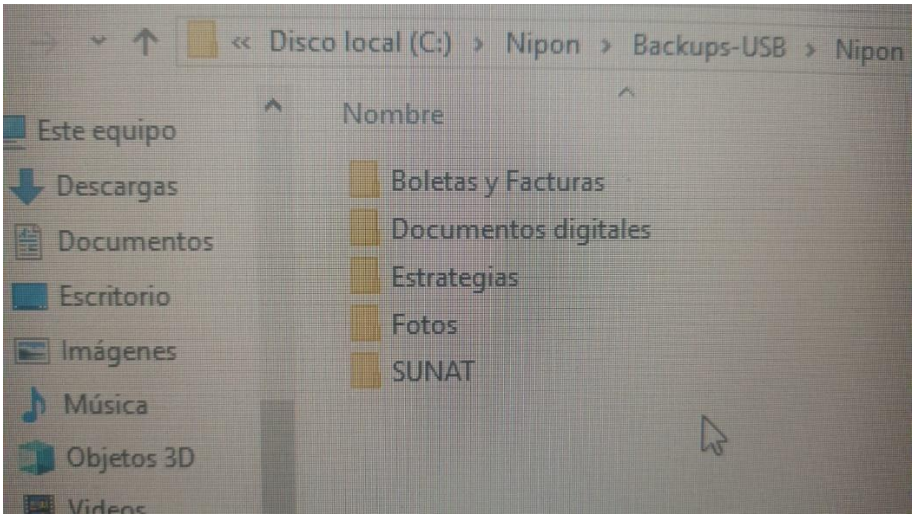
- A continuación, el encargado de TI guarda la copia de seguridad de la información en dos dispositivos externos (USB).
  - USB 1: custodiado por el encargado de TI.
  - USB 2: custodiado por la gerente general de la empresa.

VERIFICACIÓN DE LA COPIA DE SEGURIDAD

- Seleccionar la copia de seguridad y realizar restauración supervisada por el encargado TI.



- Validar datos restaurados de las copias de la seguridad.



- Elaborar acta de verificación.

ACTA DE VERIFICACIÓN DE COPIA DE SEGURIDAD

Fecha: 02/01/2024	Encargado de TI: Manuel Peña Bocanegra
Hora de inicio: 10:00 am.	Hora fin: 10:20 am.
Ejecutado por: Manuel Peña Bocanegra	Lugar: San Isidro

A las 10:00 am., se procedió a realizar la copia de seguridad de la información del equipo informático con código AI.2023.02. Asimismo, se hicieron 2 copias de esta información y fueron guardadas en los dispositivos externos "USB – 01" y "USB - 02".

Además, se procedió a la verificación de las 2 copias de seguridad, en el que se corroboró que su ejecución fue exitosa.

Observaciones: Ninguna_____.

Mario Peña Bocanegra
Encargado de TI

NIPON BUSINESS S.A.C	**RFP (Request for Proposal) "SGSI"**	CÓDIGO	2023-SG-01
		VERSIÓN	v1.0
		FECHA DE PUBLICACIÓN	01/12/2023

Anexo 8: Reporte de similitud de Turnitin

● 16% de similitud general

Principales fuentes encontradas en las siguientes bases 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

FUENTES PRINCIPALES

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

1	repositorio.uwiener.edu.pe Internet	4%
2	repositorio.ucv.edu.pe Internet	2%
3	uwiener on 2023-11-08 Submitted works	1%
4	repositorio.uta.edu.ec Internet	<1%
5	repository.unad.edu.co Internet	<1%
6	uwiener on 2024-03-14 Submitted works	<1%
7	Submitted on 1689806895993 Submitted works	<1%
8	metropol.gov.co Internet	<1%