UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo Sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor:
Mauricio Antonio Bazán Obregón
Tutores:
Mg. Renato Mauricio Toasa Guachi PhD. Maryory Urdaneta Herrera

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Renato Mauricio Toasa Guachi con C.I: 1804724167 en calidad de Tutor del proyecto de investigación titulado: Propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A

Elaborado por: Mauricio Antonio Bazán Obregón, C.I: 1723546840, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL),** como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENATO MAURICIO
TOASA GUACHI

_____

Renato Mauricio Toasa Guachi

APROBACIÓN DEL TUTOR

Yo, Maryory Urdaneta Herrera con C.I: 1759316126 en calidad de Tutora del proyecto de investigación titulado: Propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A

Elaborado por: Mauricio Antonio Bazán Obregón, C.I: 1723546840, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL),** como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
MARYORY URDANETA HERRERA

_____

Maryory Urdaneta Herrera

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Mauricio Antonio Bazán Obregón con C.I: 1723546840 autor/a del proyecto de titulación denominado: Propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., 7 de marzo del 2024

Nombre: Mauricio Antonio Bazán Obregón

Firmado electrónicamente por:
MAURICIO ANTONIO
BAZAN OBREGON

_____

Firma

ORCID 0009-0003-0637-0133

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El presente proyecto está enmarcado en una propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S.A

El factor humano es un componente esencial dentro de los esquemas de la tecnología de información, es por lo que mediante la alineación de las normas técnicas ISO/IEC 38500 (gobernanza de tecnologías) que está basada en seis principios sobre el uso adecuado de las Tecnologías de la Información y las Comunicaciones (TIC) dentro de ello está el principio del factor humano en donde se resalta la importancia de contar con personal capacitado. Así mismo complementarlo con la ISO/IEC 27001 referente a los requisitos para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) (Ibarra y Cordero, 2022)

En esta línea, el tema de estudio aborda una proposición que se enfoca en políticas de seguridad de la información (PSI) que constituyen criterios, normativas y directrices que deben seguir los colaboradores que utilizan la infraestructura de una empresa. De acuerdo con IRONTEC (2022) las PSI están conformados en un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información y que a su vez se estructura de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan.

Los documentos de una política de seguridad deben ser dinámicos, es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon (Ibarra y Cordero, 2022). Para definir políticas de seguridad se debe realizar identificaciones y análisis previos que permitan conocer a que riesgos está expuesta la información de una organización en la que se incluyan todos los procesos, sistemas y personal de esta (Tigse, 2020).

La empresa “WILPRO S.A” opera en los servicios de seguridad privada, venta e instalación de sistemas de alarma e iluminación; evidenciando en una primera valoración que esta maneja un gran flujo de información sobre sus clientes, por lo que desde que decidieron incursionar en la transformación digital desde el año 2020, es decir hace tres años implementaron un Sistema de Gestión de Informático. Pese a ello, desde su implementación hasta hoy no han establecido políticas que resguarden todo este flujo de información que manejan.

Según la Encuesta de Seguridad de la Información 2023 realizada en Ecuador, el 87% de las empresas participantes (tanto públicas como privadas) dijeron tener un plan de incidentes sólido. Sin embargo, el 13% de las empresas participantes no cuentan con gestión y monitoreo de la seguridad informática ni de la información, y empresas de esta proporción son los objetivos de este estudio. (Deloitte Ecuador, 2023)

Problema de investigación

La seguridad informática basa sus principios en la protección de la confidencialidad, la integridad y el acceso a la información de una organización en particular. Según Pérez (2023), "la evidencia muestra que no importa cuántos controles técnicos se implementen, las organizaciones seguirán experimentando violaciones de seguridad" (p. 8).

Hoy en día, la información es un activo esencial para el óptimo funcionamiento de las empresas y organizaciones, la seguridad requiere de una importante inversión para evitar brechas y dar un correcto tratamiento al riesgo en los sistemas de información. De manera similar a esta visión, Silva (2022) mencionó que "la pérdida o robo de información debido a vulnerabilidades del sistema es el delito de más rápido crecimiento a nivel mundial, causando enormes pérdidas económicas a nivel empresarial" (p. 29).

En este sentido, autores como Barrera (2019) enfatizan que la fragilidad de los sistemas de información incluye las consecuencias de las limitaciones tecnológicas que amenazan el flujo de información. Es importante que las empresas gestionen su almacenamiento de forma digital, sobre todo cuando existe una gran cantidad de información y la forma en que una misma organización se comunica y transmite información a través de la red puede ser peligrosa y provocar fuga de datos (Quilachamín, 2023).

La empresa "WILPRO S.A" es una empresa privada que opera desde hace ocho años en el Ecuador, en la ciudad de Quito, sector Sur, oferta servicios de seguridad privada, instalación de sistemas de alarma e iluminación. La empresa a partir del 2020 dio paso a la implementación de optimizar su información y datos, esto a partir de la transformación digital lo que permitió que ahora todos sus procesos se manejen desde plataformas tecnológicas y sobre todo mediante el uso de TICS.

Pese al éxito después migrar su información y el cambio de procesos manuales a procesos automatizados la empresa no planificó políticas de seguridad que le permitiera resguardar los activos relacionados al flujo de datos e información, lo que ocasiona un inherente riesgo de vulneración de sus datos. A partir de esta exposición, se entiende que el factor humano como

elemento esencial dentro de los SGSI, por lo que además de planificar políticas es fundamental contar con un personal capacitado para enfrentar todas las tecnologías y sistemas que funcionan dentro de la empresa. En esta línea y debido a que la organización maneja un gran flujo de información sobre sus clientes y al no contar con un SGSI, no existen políticas o procedimientos formalmente documentados y ampliamente difundidos que incluyan controles similares a los de seguridad de la información.

Objetivo general

Proponer un manual de políticas de uso adecuado de tecnologías de la información enfocados en mitigar los riesgos asociados al factor humano utilizando como marco de referencia los principios y directrices establecidos en las normas ISO/IEC 38500 e ISO/IEC 27001.

Objetivos específicos

- Contextualizar los fundamentos teóricos sobre los términos básicos determinantes en el proyecto y normas ISO/IEC 38500 e ISO/IEC 27001 para mitigar los riesgos asociados al factor humano.
- Diagnosticar el estado situacional actual de la empresa para mitigar las brechas de seguridad que son directamente atribuibles a acciones o errores humanos.
- Diseñar un manual de políticas de seguridad informática específicas que aborden debilidades humanas, basándose en los principios de ISO/IEC 38500 e ISO/IEC 27001.
- Valorar a través del criterio de especialistas la efectividad de estas políticas de acuerdo con las necesidades de la organización.

Vinculación con la sociedad y beneficiarios directos:

De acuerdo con los ODS (su abreviatura significa: Objetivos de Desarrollo Sostenible de las Naciones Unidas), este trabajo está alineado con el ODS 9, la implementación de un manual para el correcto uso de tecnologías y la aplicación de diferentes controles basados en las normas ISO/IEC 27001e ISO/IEC 38500 ayudará a la empresa a innovar en el campo de la seguridad informática, haciéndola más competitiva y reduce las brechas que la vuelven vulnerable.

La vinculación con la sociedad reside en formar, capacitar y diseñar un manual de políticas de uso adecuado de tecnologías de la información enfocados en mitigar los riesgos asociados al factor humano utilizando como marco de referencia los principios y directrices establecidos en las normas ISO/IEC 38500 e ISO/IEC 27001. El proyecto surge como una solución para la empresa objeto de estudio (WILPRO S.A), para que esta pueda administrar su flujo de información,

recursos humanos, finanzas, investigación, desarrollo, procedimientos y gestión gerencial eficientes PSI.

En este sentido, la necesidad creciente de las empresas de contar con PSI y establecerlas de forma eficiente dentro de sus sistemas de información como activo fundamental de las organizaciones resulta como prioridad, dentro de este entorno se enmarca el factor humano el cual debe ser capacitado para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), en definitiva, cuidar y proteger la información de cualquier riesgo informático que se pueda presentar. Los sistemas de información de una organización pueden ser vulnerables a ataques debido a factores como errores u omisiones no intencionales derivadas de la interacción humana, la empresa aún puede agrandar estas brechas por falta de interés en temas como; capacitación del personal, la falta de conocimiento de las herramientas y la falta de experiencia en el campo.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Las amenazas cibernéticas continúan evolucionando y adaptándose a medida que la tecnología avanza, convirtiéndose en un riesgo constante: Los seres humanos son a menudo el eslabón más débil en la cadena de seguridad cibernética y esto se debe a la falta de conciencia, descuidos y la explotación de la ingeniería social por parte de ciberdelincuentes, es por ello que las compañías deben aportar una política de conciencia y constante capacitación para abordar este desafío por lo que es fundamental mejorar la capacitación en ciberseguridad entre los usuarios, Las organizaciones deben educar a su personal sobre prácticas seguras, cómo detectar posibles amenazas y cómo responder a estos incidentes. (Medina et al., 2022)

Contextualización

El desarrollo de un manual y el cumplimiento de políticas de seguridad informática apoyados por la alta dirección, garantizan que los empleados tengan una herramienta tangible que se vuelve primordial para el manejo de un entorno de colaboración interdisciplinaria (Angulo, 2023). La ciberseguridad no es solo responsabilidad de los departamentos de TI o de seguridad. Se necesita una colaboración interdisciplinaria en toda la organización para abordar los desafíos relacionados con el factor humano en la ciberseguridad. Esto incluye la participación de recursos humanos, departamentos legales y de cumplimiento, y la alta dirección.

La tecnología y automatización de la tecnología también puede desempeñar un papel importante en la mitigación de los riesgos relacionados con el factor humano. La implementación de herramientas de seguridad avanzadas, como sistemas de detección de amenazas y autenticación multifactor (MFA), puede ayudar a reducir el impacto de los errores humanos y la ingeniería social.

Conceptos fundamentales

Sistemas de información

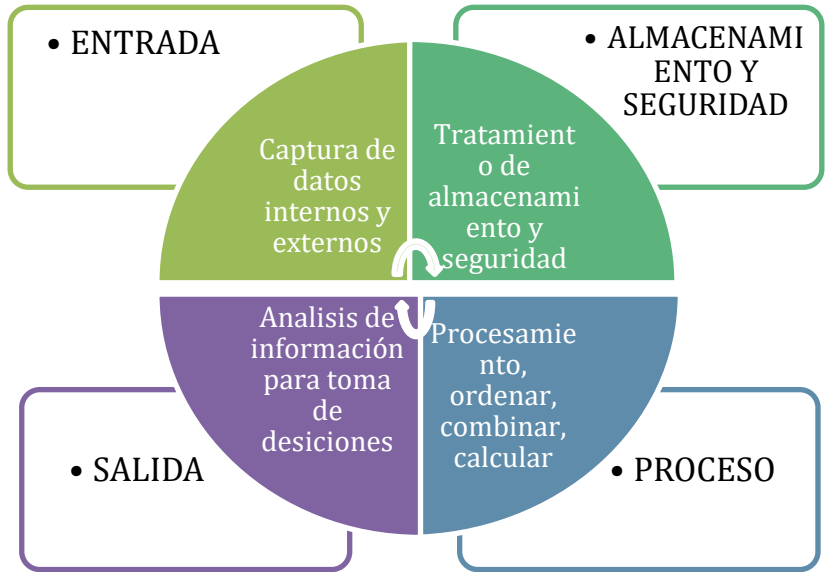
Según Sisti (2019) los sistemas de información específicamente provienen de la información, la cual se define como un recurso esencial para cualquier organización/negocio, ya que la toma de decisiones depende del análisis de los datos recopilados, también puede crear ventajas competitivas si se utiliza correctamente. Esto se logra mediante el proceso de retroalimentación generado en el sistema de información (p.9)

Los sistemas son definidos como un compendio de reglas, disposiivos y elementos que ordenados de forma correcta entre sí, contribuyen al logro de objetivos, nos permiten el

intercambio y la adquisición de conocimientos. Su ciclo comprende principalmente cuatro actividades; entrada, almacenamiento y seguridad, proceso y salida, que de acuerdo con Sisti (2019) son:

- **Entrada:** La adquisición del elemento principal del sistema de información, el dato en bruto, que puede ser internos o externos al negocio.
- **Almacenamiento y seguridad:** Tratamiento correcto de la información y su almacenamiento seguro.
- **Proceso:** Los datos comienzan a combinarse con otros elementos y adquieren significado mediante la contextualización en basado a las operaciones del negocio.
- **Salida:** Finalmente se generan reportes e información valiosa para los analistas, quienes deben tener la retroalimentación adecuada para evaluar, corregir y mejorar el proceso desde la entrada de datos.

Figura 1
Ciclo de la información.



Nota. Autoría propia. Basado en (Sisti, 2019).

Desde una perspectiva organizacional, los sistemas de información incluyen soluciones de seguridad y gestión basadas en tecnología que abordan problemas y desafíos en el entorno. Desglosa las tres dimensiones que componen los sistemas para que puedan operar de manera eficiente y crear valor (Sisti, 2019). Estas dimensiones son:

- **Organización:** comprende personal, estructura, procedimientos, cultura y políticas empresariales.
- **Administración:** planificar, asignar recursos financieros y humanos, desarrollar

estrategias para abordar los desafíos comerciales en el entorno y coordinar esfuerzos para lograr el éxito. Define la función principal del sistema.

- **Tecnología:** comprende, software, hardware, tecnología de redes, telecomunicaciones y almacenamiento de datos. Constituyen la infraestructura de tecnología y sistema de información.

Hoy en día, estos sistemas de información se ejecutan en plataformas digitales como sitios web, aplicaciones, la nube o servidores y lo que conlleva a permanecer expuestos a riesgos, vulnerabilidades y constantes amenazas por parte de ciberdelincuentes.

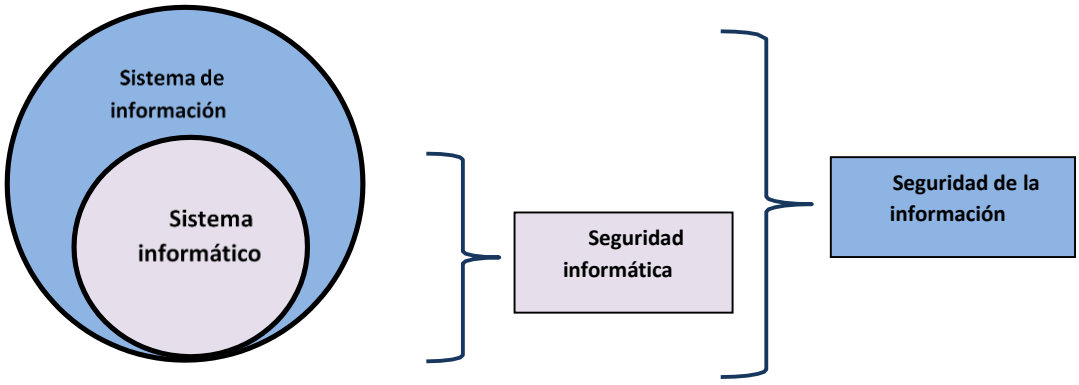
Seguridad informática

Según Morera (2022) "representa uno de los activos de mayor valor que posee toda empresa y es trascendental ya que se utiliza tanto en las tareas diarias como en la toma de decisiones estratégicas" (p.19).

Opera ante cualquier pérdida, daño o alteración dentro del sistema de información a fin de mitigar los problemas relacionados para el funcionamiento normal de las operaciones que puedan llegar a traducirse como pérdidas económicas. En definitiva, comprende las estrategias y herramientas que concentran la protección de los recursos informáticos.

Figura 2

Seguridad informática vs seguridad de la información



Nota. Esquematización del funcionamiento de la seguridad informática vs el de la seguridad de la información. Tomado de (Sisti, 2019).

Recursos del sistema de seguridad

Para Sisti (2019) "un sistema informático está conformado por el hardware, software, recursos humanos, datos e información" (p.20).

Según estas definiciones, hardware son los recursos físicos y que podemos palpar y

son necesarios para durante todo el ciclo que involucre sistemas de información, como teclados, ratón, escáner, dispositivos móviles, etc. El software, se trata de toda la parte lógica, lo que no podemos palpar, sin embargo, es visible a través del hardware, como programas, servicios web, aplicaciones, etc. Finalmente, los recursos humanos, son quienes dan uso y realizan acciones utilizando en conjunto el software y hardware, también formando parte de un sistema informático ya que actualmente la interacción humana con las TICS, funcionan a la par. El primer recurso de soporte técnico es una poderosa herramienta que puede potenciar las capacidades de las personas, pero para ello es necesario comprenderlo adecuadamente y someterlo a constante capacitación. Los activos de TI son fundamentales para el desempeño empresarial, por lo que deben protegerse adecuadamente contra cualquier amenaza que pueda afectarlos o dañarlos (Pérez, 2023).

Políticas de seguridad

Según UNIR (2022) la política de seguridad de la informática (PSI) "constituye un documento que establece los lineamientos y procedimientos para gestionar la seguridad de la informática". También ha sido definido como un compendio de reglas, procedimientos, normas y directrices que deben seguir todas las personas que utilizan la infraestructura de la empresa.

En criterios de la FECYT (2022) la PSI comprenden normas, directrices y ejes recogidos en un documento aprobado por la alta dirección de una empresa, en la que constan medidas y controles para que la organización pueda aplicar lineamientos inclinados a establecer confidencialidad, integridad y disponibilidad de la información.

La PSI debe ser dinámica, esto se traduce a que debe ajustarse y mejorarse continuamente, acorde a los cambios que se presentan en los ambientes que deben ser atendidos. El objetivo de una política de seguridad es garantizar que todos los miembros de una organización trabajen hacia un objetivo común a medida que evolucionan las amenazas a la seguridad informática y evoluciona el negocio. (CQR, 2020).

Factor humano

Estrada et (2022) "constituye una dimensión de las interacciones y características humanas en diferentes contextos, encierra características psicológicas, físicas y sociales que llegan a afectar la interacción humana con los equipos, sistemas, procesos, otras personas y equipos de trabajo" (p.13).

En criterios de De la Llave et (2022, p.56) El factor humano hace referencia a la vinculación entre el talento humano y los equipos tecnológicos o máquinas, que sumado a los

procedimientos y con los ambientes que los rodean comprenden un escenario multidimensional en donde convergen diversas variables internas y externa relacionadas a la persona.

Norma ISO/IEC 38500

La ISO/IEC 38500 responde a un estándar internacional para las buenas prácticas referentes a las Tecnologías de la Información (TI), en ella se enmarcan los principios, las definiciones y un modelo para ayudar a los órganos de gobierno a comprender la importancia de la Tecnología de la Información (TI) (ISO/IEC 38500, 2019).

Este estándar para las buenas prácticas de Gobernanza Corporativa de las Tecnologías de la Información (TI) están enfocadas en garantizar la elaboración y puesta en práctica de las políticas de gobernabilidad de una determinada empresa, a fin de diagnosticar los cambios organizativos y estructurales que se requieran en esta, para brindarle la capacidad de responder con rapidez, eficacia a los cambios demandantes del entorno en conjunto con varios requisitos para cumplir con los actos regulatorios de las actividades en las que participa y gestionar eficazmente los riesgos para asegurar la continuidad y sostenibilidad de las operaciones. (Global Trust Association, 2019).

La ISO/IEC 38500 se aplica a los procesos de gestión relativos a los servicios de información y comunicación IT de una organización, su función principal reside en atender desde normas técnicas el manejo de las TI dentro de la empresa (García, 2018). Para conseguirlo se basa en seis principios y tres procesos, dentro de ellos el factor humano, un elemento fundamental para atender en la propuesta de este proyecto.

La ISO/IEC 38500 se aplica en todo tipo de organizaciones facilitando la evaluación objetiva del gobierno de TI. Además, asegura el cumplimiento de la legislación vigente y permite una apropiada implementación y operación de los recursos de TI (García, 2018).

Norma ISO/IEC 27001

La norma ISO/IEC 27001 responde a un estándar internacional el cual determina requisitos para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI). Esta proporciona un marco de trabajo para los SGSI y su objetivo se sustenta en identificar los riesgos, definir estrategias para evitarlos e implementar salvaguardas (NQA, 2022).

La norma ISO/IEC 27001 también busca cumplir con los principios de confidencialidad, integridad y disponibilidad de la información; permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan (Global Trust Association, 2019).

La norma ISO/IEC 27001 se puede acoplar a cualquier tipo de negocio, contemplando a pequeñas, medianas y hasta grandes corporaciones, instituciones gubernamentales y sin fines de lucro. A cualquier sector, como finanzas, salud y servicios públicos. El proceso de implementación de la norma ISO/IEC 27001 se divide en cuatro fases: planificación, implementación, evaluación y mejora continua (NQA, 2022).

1.2. Proceso investigativo metodológico

El proceso metodológico de esta investigación se sostiene en un enfoque mixto, en primer lugar, cuantitativo el cual comprende en si un conjunto de estrategias investigativas que utiliza preguntas y encuestas para la recopilación de datos cuantificables (Hernández, 2014, p.7). La investigación cuantitativa generalmente parte de la pregunta de investigación, que deberá formularse en concordancia con la metodología que se pretende utilizar. Adicionalmente se aplicó el método cualitativo mediante una entrevista respondida por un colaborador de la empresa, con lo cual se pretende contextualizar de mejor manera el estado actual en gobernanza de TIC, la situación actual en el ámbito de seguridad informática y el alcance que se espera obtener con el presente estudio.

El estudio respalda el análisis estadístico de datos para obtener conclusiones de la investigación. El propósito del diseño es explorar la complejidad de los factores asociados al factor humano y las diferentes perspectivas y significados que tiene para la organización.

El enfoque para este proyecto se basa en la recopilación y el análisis de datos para responder a preguntas de investigación y evaluarlas, para ello se realizará una recolección de datos mediante entrevistas y encuestas, con lo que se realizará un adecuado análisis de la realidad de la empresa y mediante ello se definirá cuáles serán las acciones por tomar y apoyará la metodología de desarrollo del manual.

El tipo de investigación fue descriptivo que admitió el análisis de las características del fenómeno a fin de definir, clasificar, dividir o resumir. La investigación descriptiva es frecuentemente usada como un antecedente a los diseños de investigación cuantitativa, este método permitió sintetizar el diagnóstico de las políticas de seguridad informática y el factor humano para el conocimiento de los procesos administrativos y las vulnerabilidades a las que se enfrenta la organización.

El universo de estudio estuvo constituido por el gerente de la empresa WILPRO S.A que accedió a participar voluntariamente en este proyecto bajo consentimiento informado a fin de

facilitar la propuesta de estudio para la mejora de la seguridad informática, en conjunto con sus (5) colaboradores del sistema de información.

El proceso de análisis de los datos cuantitativos se realizó utilizando pruebas de significación, o análisis de varianza para determinar relaciones, tendencias y patrones en los datos, este método cuantitativo especialmente nos ayuda a medir y analizar datos de manera objetiva, para establecer patrones o tendencias en la población. En cuanto a los métodos de investigación bibliográfica, se pueden utilizar los siguientes métodos para recopilar y analizar información teórica y empírica:

- Lectura la cual es importante para adquirir conocimiento, analizar y determinar los aportes teóricos a ser utilizados.
- Mapas conceptuales y gráficos como visualizadores de procesos para una mayor comprensión conceptual y de flujo de procesos.
- El resumen con la finalidad de citar un escrito abreviado; para favorecer la comprensión, entender mejor el texto y redactar con exactitud y calidad.
- La encuesta comprende una técnica de gran utilidad en la investigación cuantitativa para recabar datos; está se delimita desde un cuestionario semiestructurado con preguntas cerradas y abiertas bajo la escala de Likert (Hernández, 2014)

En síntesis, para la recolección de datos fue mediante cuestionarios estructurados basados en políticas, procedimientos y responsabilidades relacionadas con el gobierno de seguridad informática bajo la norma ISO/IEC 27001 e ISO/IEC 38500, bajo la técnica de la encuesta web, para ello se empleó el software Online (Google Forms). Que admite capturar y analizar datos para crear tablas y gráficas con datos, las encuestas fueron aplicada directamente al personal de la empresa, lo que permitió la interpretación de resultados.

1.3. Análisis de resultados

En base a la aplicación de los métodos antes descrito se procedió a la recopilación y obtención de datos los que fueron sistematizados en las siguientes matrices y gráficas detalladas a continuación:

Pregunta 1: ¿La organización asigna responsabilidades relacionadas con el gobierno de seguridad informática?

Tabla 1

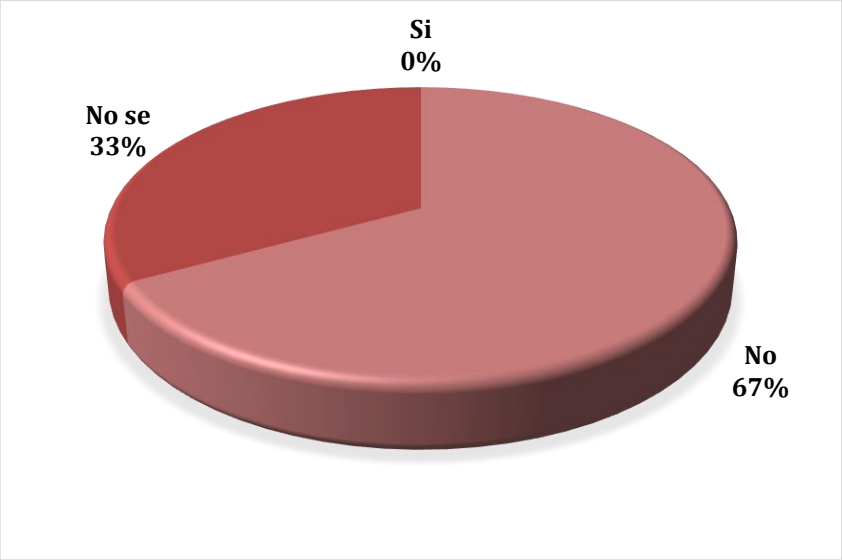
Asignación de responsabilidades

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	4	67%
No se	2	33%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 3

Asignación de responsabilidades



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En conformidad a la formulación sobre; ¿si la organización asigna responsabilidades relacionadas con el gobierno de seguridad informática? Se evidenció que: El 67% (n=4) establecieron, que no se asigna este tipo de responsabilidades sobre la protección y seguridad de la información (SI) manejada por la empresa; todo se ha manejado de forma empírica, cada uno conoce sus responsabilidades y funciones. Sólo un 33% (n=2) establecieron, que no tienen conocimiento, en las respuestas otorgadas, se confirmó que todas las responsabilidades se reconocen de acuerdo con el puesto y cargo del personal empíricamente.

Pregunta 2: ¿La organización asigna las responsabilidades del gobierno de seguridad informática en base a criterios propios y no de modelos establecidos?

Tabla 2

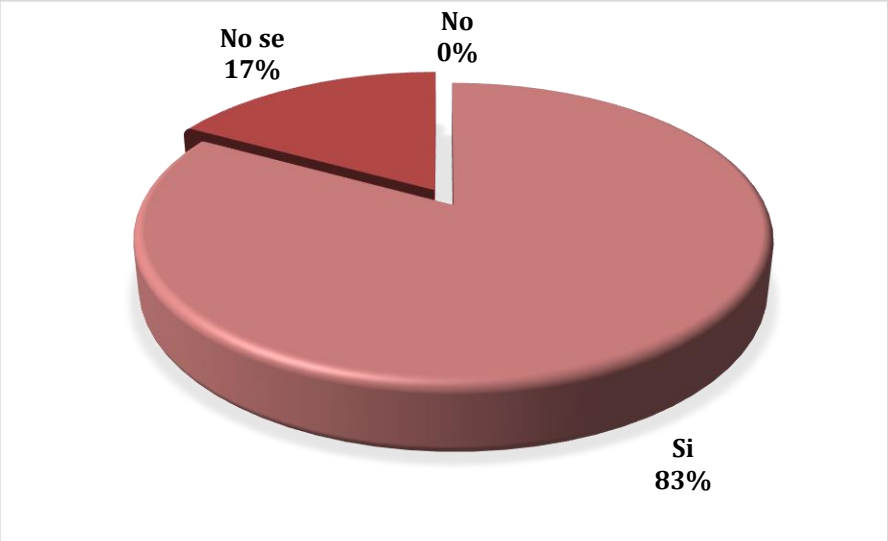
Asignación de responsabilidades (En base a criterios propios)

Opciones	Frecuencia	Porcentaje
Si	5	83%
No	0	0%
No se	1	17%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 4

Asignación de responsabilidades (En base a criterios propios)



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

Respecto a la a interrogante, se demostró que: El 83% (n=5) que, sí se asigna responsabilidades sobre criterios propios, muy básicos y no de modelos establecidos por la empresa; Por otro lado, sólo un 17% (n=1) establecieron, no tener conocimiento, sobre las respuestas indicadas; manifestaron que se reconocen las responsabilidades relacionadas con el puesto asignado del personal.

Pregunta 3: ¿El cuerpo directivo de la organización asignado para el manejo del gobierno de seguridad informática, tienen las competencias adecuadas para hacerlo?

Tabla 3

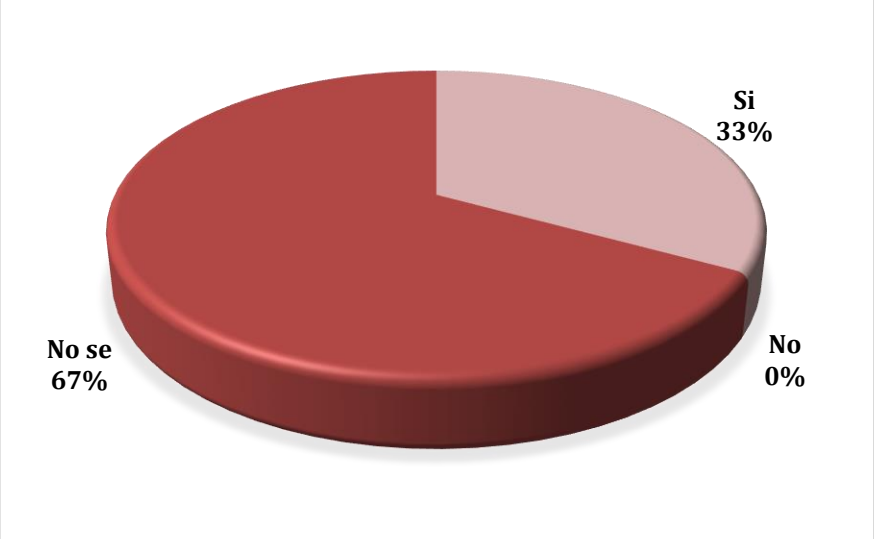
Competencias adecuadas del cuerpo directivo (Seguridad de la información)

Opciones	Frecuencia	Porcentaje
Si	2	33%
No	0	0%
No se	4	67%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 5

Competencias adecuadas del cuerpo directivo (Seguridad de la información)



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En relación con la formulación establecida, se reflejó que: El 67% (n=4) manifestaron, que desconocen estas competencias que ejercen el cuerpo directivo sobre el manejo de la SI, sobre la protección y de la información de la empresa, teniendo en cuenta que poseen competencias empíricas. Por otro lado, un 33% (n=2) (gerente y supervisor) indicaron que, si desempeñan las competencias adecuadas para el manejo de la SI, se constó en el reconocimiento de las competencias propicias de acuerdo con el cargo del personal.

Pregunta 4: ¿El cuerpo directivo encargado del gobierno de seguridad informática supervisan los diferentes niveles de gestión de seguridad informática?

Tabla 4

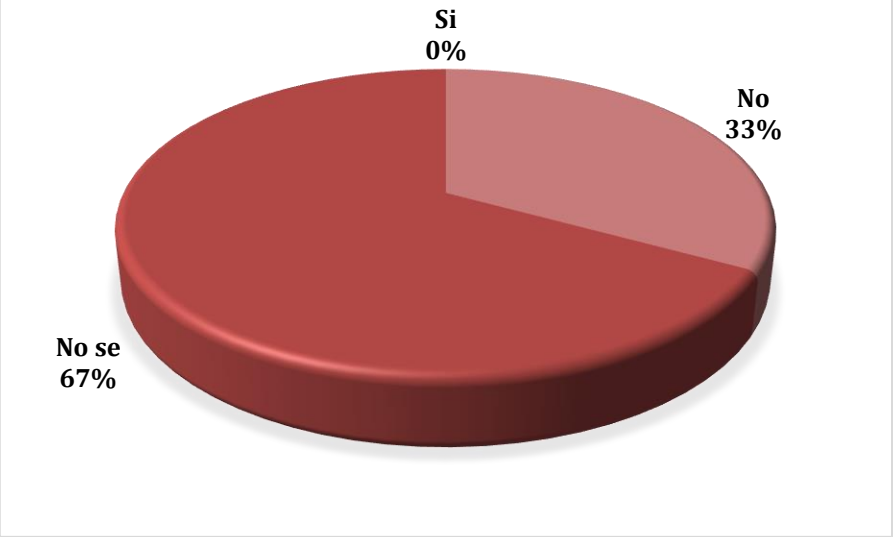
Supervisión de los niveles de gestión (Seguridad de la información)

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	2	33%
No se	4	67%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 6

Supervisión de los niveles de gestión (Seguridad de la información)



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En este sentido, e interpretando lo que indica la formulación anterior, se demostró que: El 67% (n=4) no tienen el conocimiento respectivo a cerca de la supervisión que efectúa sobre los distintos grados de gestión de la SI; lo que refleja, que no se lleva un control frecuente sobre la vigilancia e inspección de niveles de SI. Sólo un 33%(n=2) señaló que no conocen el empleo de supervisión en los niveles de la SI, lo cual evidencia falencias en el manejo de supervisión.

Pregunta 5: ¿Se realiza un seguimiento a los roles y responsabilidades asignadas a los colaboradores para garantizar que la ejecución de los procesos relacionados con la seguridad informática se realice de manera correcta a fin de evitar el error humano?

Tabla 5

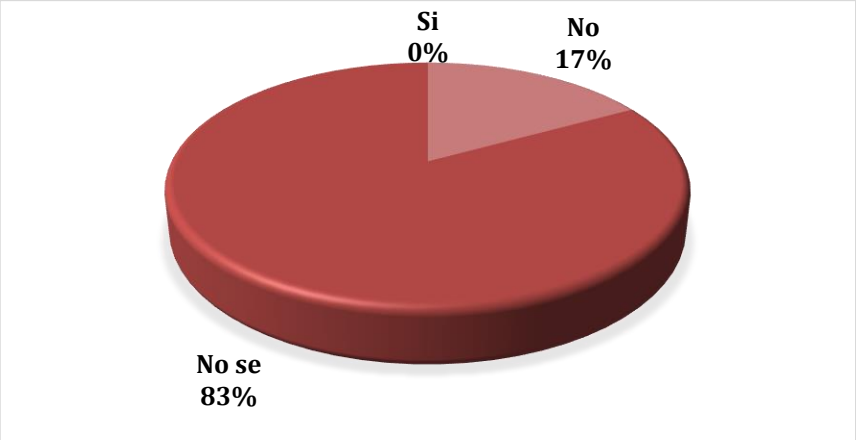
Seguimiento a los roles y responsabilidades asignadas

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	1	17%
No se	5	83%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 7

Seguimiento a los roles y responsabilidades asignadas



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En conformidad a la formulación anterior, se conoció que el 83% (n=5) no tiene conocimiento si se realiza este tipo de seguimiento. Por otra parte, un 17% (n=1), expresó que no se lleva a cabo el respectivo seguimiento. Esto permite evidenciar que los procesos relacionados a la seguridad de la información no están enmarcados en normativas y lineamientos para su protección, lo que puede incurrir en un error humano al no tener ninguna supervisión ni evaluación.

Pregunta 6: ¿Los colaboradores de la empresa atienden las responsabilidades básicas asignadas por el cuerpo directivo de la organización en materia de seguridad informática?

Tabla 6

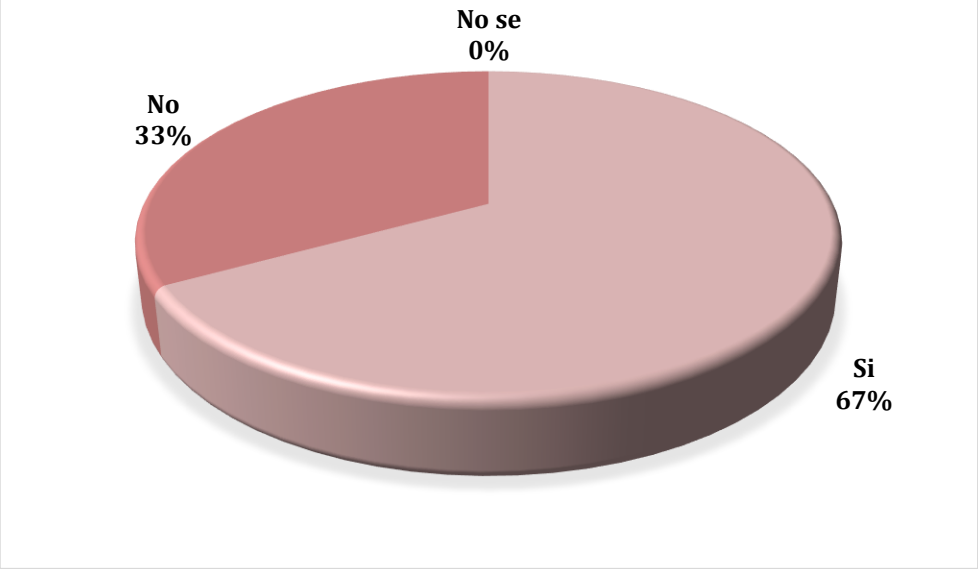
Comprensión de las responsabilidades por los colaboradores (Seguridad de la información)

Opciones	Frecuencia	Porcentaje
Si	4	67%
No	2	33%
No se	0	0%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 8

Comprensión de las responsabilidades por los colaboradores (Seguridad de la información)



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En cuanto a la interrogante planteada, el 67% (n=4) demostró, que atienden las responsabilidades básicas asignadas por el cuerpo directivo de la organización en materia de seguridad informática, lo que permite evidenciar que existe interés por cumplir funciones relacionadas al resguardo de la información de la empresa. Un 33% (n=2) manifestó, que no atiende este tipo de responsabilidades ya que sus funciones no se relacionan directamente con le seguridad informática.

Pregunta 7: ¿La organización dispone de un manejo de seguridad informática, aunque estas no se encuentren integrados en las políticas de Gobierno de seguridad de la Información?

Tabla 7

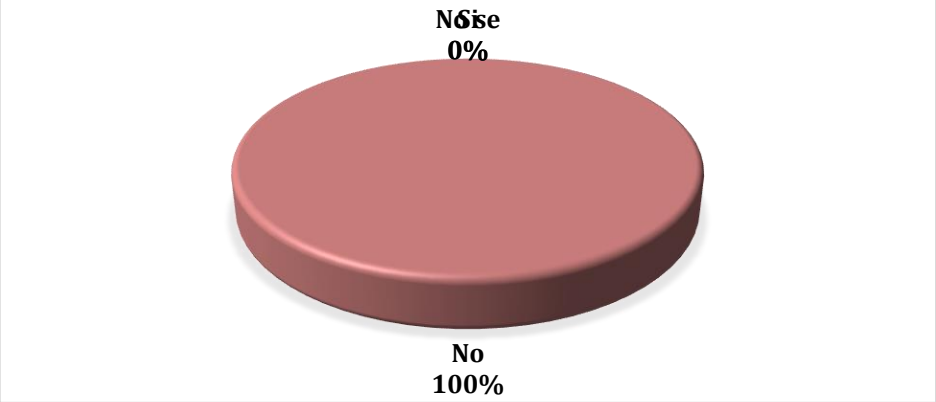
Manejo de seguridad de la información

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	6	100%
No se	0	0%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 9

Manejo de seguridad de la información



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

De acuerdo con la formulación, se evidenció que, el 100% (n=6) estableció que no se ejerce ningún manejo sobre la protección y seguridad de la información especialmente sensible y confidencial de la organización. En definitiva, se conoció que existe un manejo empírico, basado en la experiencia y en funciones de los colaboradores.

Pregunta 8: ¿Analiza el cuerpo directivo los riesgos asociados a la seguridad informática desde el punto de vista operativo y de cumplimiento normativo empresarial interno?

Tabla 8

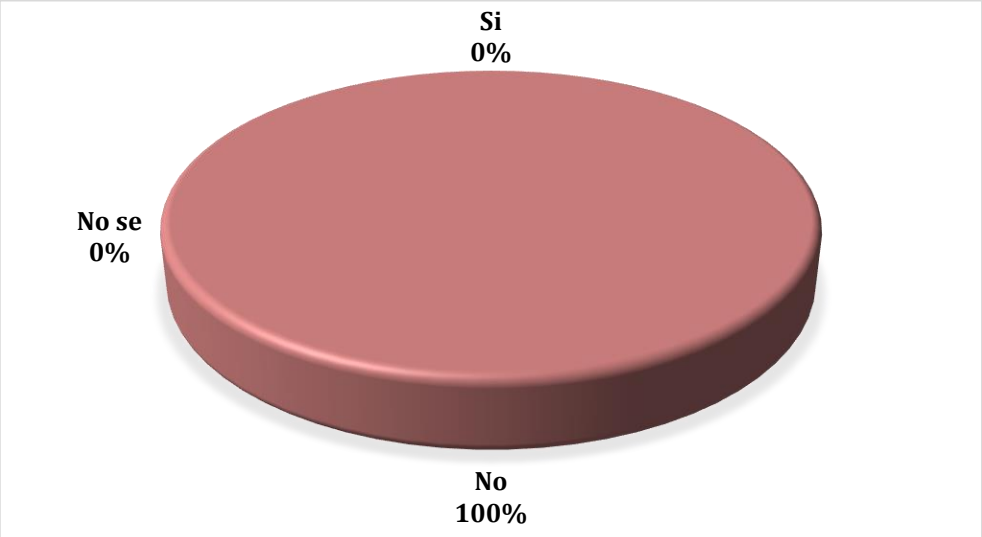
Análisis de los riesgos asociados a la seguridad por el cuerpo directivo

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	6	100%
No se	0	0%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 10

Análisis de los riesgos asociados a la seguridad por el cuerpo directivo



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

Respecto a la formulación anterior, el 100% (n=6) de los sujetos encuestados manifestó que no se emplea este tipo de análisis, el cual busca fortalecer la seguridad de la información, a fin de evitar los riesgos y amenazas que pueda presentar la organización y lo que esto implica para los colaboradores y usuarios de la empresa.

Pregunta 9: ¿El cuerpo directivo de la empresa diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad informática?

Tabla 9

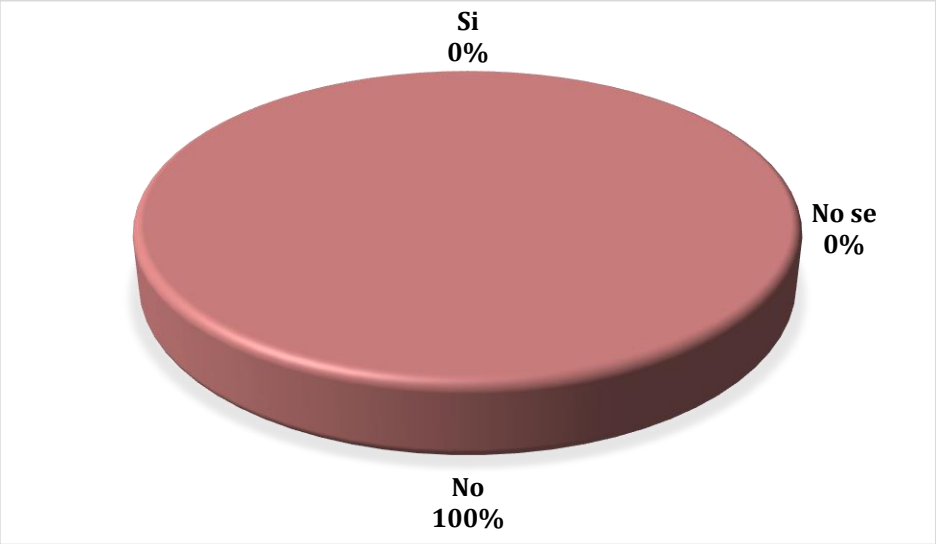
Diseños de procesos y procedimientos estratégicos

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	6	100%
No se	0	0%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 11

Diseños de procesos y procedimientos estratégicos



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En conformidad a esta formulación, el 100% (n=6) señaló que no se han diseñado estos procesos estratégicos relacionados con la seguridad informática, lo que genera vulnerabilidad ante ataques cibernéticos. Siendo esto una falencia en la que se debe considerar estrategias fundamentales y necesarias para el fortalecimiento y resguardo de la información y datos sensible, confidenciales de la organización.

Pregunta 10: ¿La organización realiza una planificación de la seguridad informática y seguimiento a pequeño, medio y largo plazo?

Tabla 10

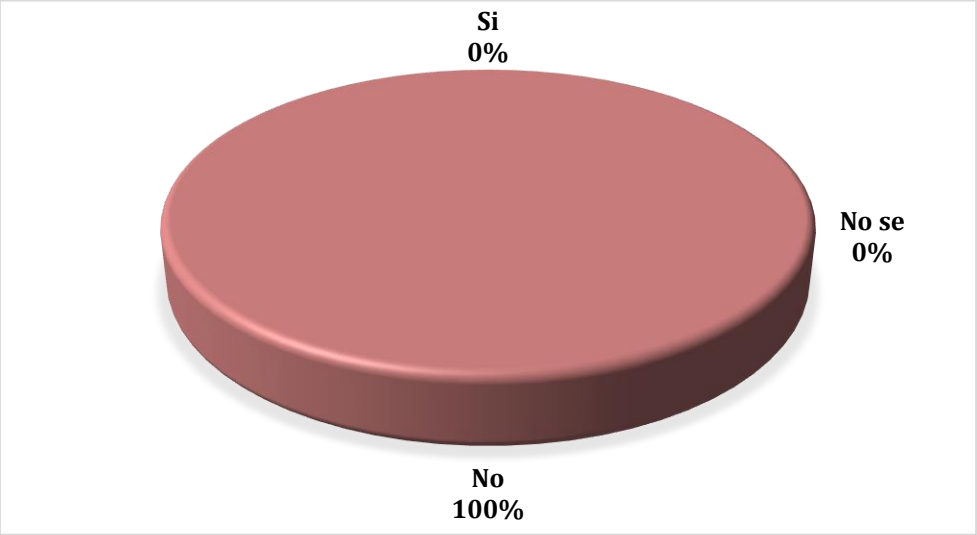
Planificación y seguimiento (Seguridad de la información)

Opciones	Frecuencia	Porcentaje
Si	0	0%
No	6	100%
No se	0	0%
Total	**6**	**100%**

Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Figura 12

Planificación y seguimiento (Seguridad de la información)



Nota. Datos extraídos de la encuesta aplicada al gerente y colaboradores de la empresa WILPRO S.A.

Análisis

En relación con la formulación anterior, se evidenció que el 100% (n=6) indicó que no se ha realizado una estructura planificada de la seguridad de la información y seguimiento a pequeño, medio y largo plazo que permita reforzar y resguardar los datos sensibles de la empresa.

Análisis general de la encuesta aplicada

En general se puede observar que la empresa no cuenta con controles, procesos y procedimientos estratégicos de acuerdo con la evidencia podemos concluir que el cuerpo directivo de la empresa no diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad informática, por lo que esto hace inminente la necesidad de diseñar un manual de políticas de seguridad informática que aborden debilidades humanas, basándose en los principios del anexo A.5 de las ISO/IEC 27001 en el cuál existen controles relacionados a políticas de seguridad de la información y orienta a la dirección para la gestión y revisión, así mismo las normas ISO/IEC 38500.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

Política de seguridad

La política de seguridad, según Arcos (2023) consiste en desarrollar un documento enmarcado en una serie de acciones y actuaciones apropiadas para salvaguardar la información de la organización, su objetivo principal reside en indicar el propósito del Sistema de Gestión de Seguridad informática y del documento en sí mismo.

Constituye un conjunto de normativas que se aplican y regulan las actividades del sistema y los recursos de comunicaciones que pertenecen a una organización, tales reglas o normativas, que admiten áreas como la seguridad física, personal, administrativa y de la red (Cortijo y Mullo, 2022).

Manual de políticas de seguridad informática

Según Morera (2022) menciona que el manual de políticas es un documento escrito o digitalizado que contienen los lineamientos de seguridad para que toda la información sea accesible para todos los funcionarios, dichos lineamientos se sostienen en las normativas que regulan todas las acciones.

El manual de seguridad de la información admite la implementación y mantenimiento de varios procesos para gestionar la información eficazmente, enfocada a mantener la confidencialidad, integridad y disponibilidad de los activos de información mientras se minimizan los riesgos de seguridad de la información. (Angulo, 2023).

Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información comprende un conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad (Tigse, 2020).

Principios de ISO/IEC 27001/ISO/IEC 38500.

En cuanto a los principios de la normativa ISO/IEC 27001 delimita todos los lineamientos y requisitos para la implementación, mantenimiento y mejora continua, basados en la confidencialidad, a fin de garantizar que solo los usuarios o entidades autorizados puedan acceder a la información (Sisti, 2019). Así mismo, se sostiene en la integridad, se refiere a la confiabilidad y exactitud de la información, finalmente está la disponibilidad, esto garantiza que el usuario acceda a la información que necesita en ese preciso momento. Dentro de este principio se ubican otros lineamientos que responden a la contextualización de la organización,

el alcance del SGSI, liderazgo, planificación, soporte, operación, evaluación de resultados y mejora, todo en pro a la identificación de los riesgos, definición de estrategias para evitarlos e implementar salvaguardas, estableciendo buenas prácticas para proteger los datos de una organización y generar mayor confianza entre los clientes, proveedores y empleados (Angulo, 2023).

En referencia a los principios de la ISO/IEC 38500, es definido como estándar internacional para el gobierno de las tecnologías de la información (TI). Estos están dirigidos para los directores de las organizaciones evalúen, dirijan y supervisen el uso de las TI, a fin de que se promueva el uso eficaz, eficiente y aceptable de las TI, se aseguren a los involucrados que pueden confiar en el gobierno corporativo de TI de la organización, se proporcionen guías a los directivos para el uso adecuado de las TI, se ayude a las organizaciones a comprender y satisfacer sus compromisos legales y obligaciones éticas en relación con el uso de las TI (Sisti, 2019)

El principio 6 de ISO/IEC 38500: La evaluación de factores humanos se basa en tres verbos, **Evaluar**: Los gerentes deben evaluar las actividades de TI para garantizar que el comportamiento humano sea reconocido y considerado apropiado. **Dirigir**: los gerentes deben garantizar que cualquier persona pueda identificar e informar los riesgos, oportunidades, problemas e inquietudes en cualquier momento. Estos riesgos deben gestionarse de acuerdo con las políticas y procedimientos publicados. **Controlar**: Los gerentes deben monitorear las prácticas laborales para garantizar que sean compatibles con el uso correcto de TI (Pérez, 2023).

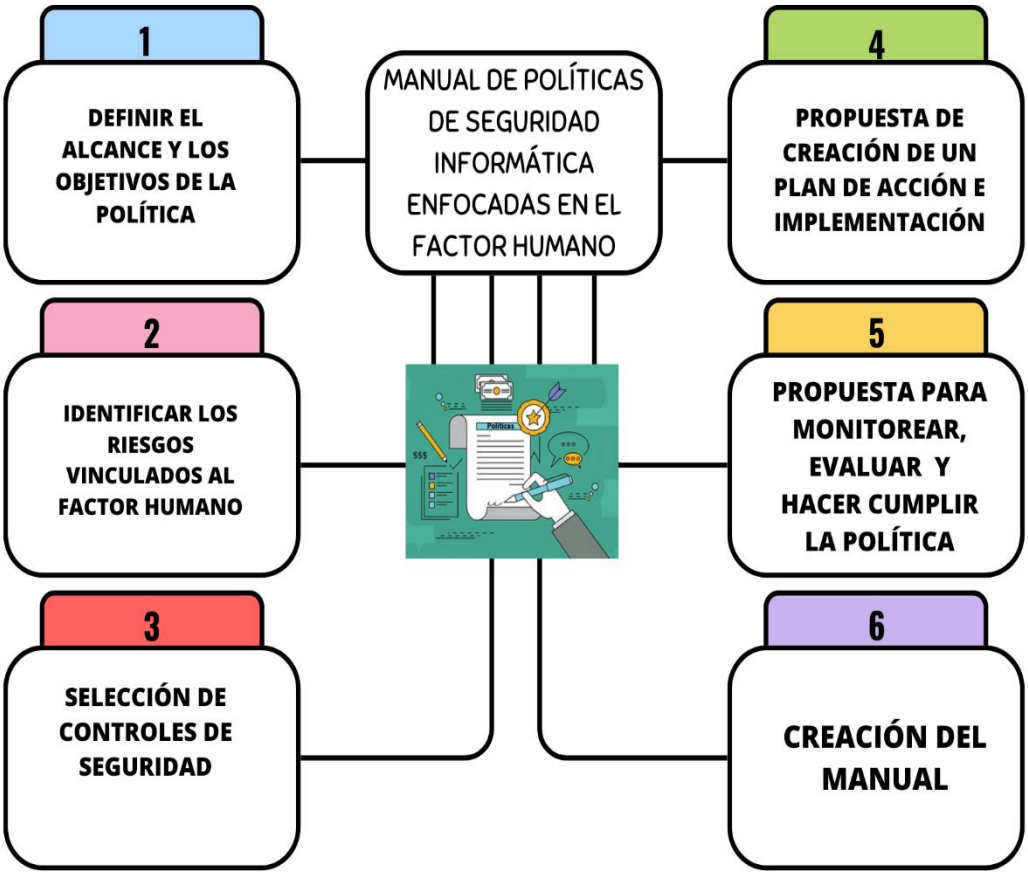
2.2. Descripción de la propuesta

La propuesta de estudio atiende la necesidad de establecer políticas de seguridad informática específicas que aborden debilidades humanas, basándose en los principios de ISO/IEC 27001 e ISO/IEC 38500 en las que se delimiten criterios e indicadores de evaluación, control y seguimiento, el cual será socializado con todos los colaboradores y cuerpo directivo de la empresa WILPRO S.A.

El objetivo del desarrollo del presente manual es establecer las políticas que integran el sistema de gestión de seguridad de la información SGSI para la empresa WILPRO S.A, el cual será socializado y adaptado a todas las áreas de la empresa y todo el personal. El desarrollo de estas políticas está orientadas y basadas en los controles y requisitos identificados en el estándar ISO/I27001 y la ISO/38500 a fin de implementar las buenas prácticas.

Figura 13

Organizador para elaboración de un manual de políticas de seguridad de la información



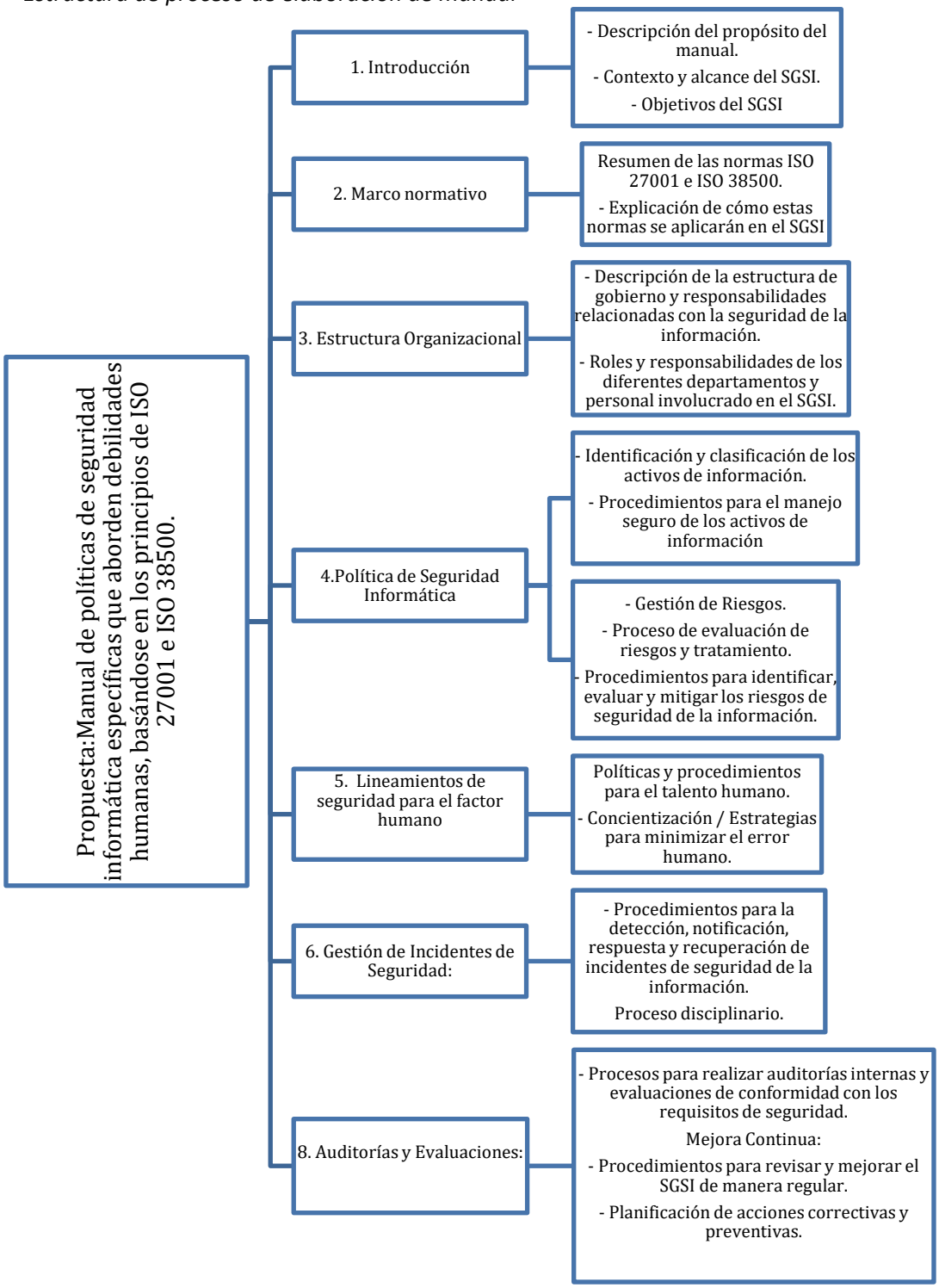
Nota. Autoría propia.

a. Estructura general

En la figura 13 se muestra el flujo de proceso de cómo se llevará a cabo la propuesta de un manual de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano, esta serie de pasos nos permite identificar el alcance y el desarrollo del manual como tal.

Tabla 11

Estructura de proceso de elaboración de manual



Nota. Autoría propia.

b. Explicación del aporte

El presente trabajo aporta una guía para la gestión de la seguridad informática, alineando las buenas prácticas sobre gobierno de tecnologías de la información provistas por ISO/IEC

38500, con los requerimientos técnicos y de gestión establecidos en la norma ISO/IEC 27001 de sistemas de gestión de seguridad de la información.

Asimismo, este manual permite complementar los controles tecnológicos y gerenciales tradicionales de un SGSI, con directrices específicas para fortalecer el factor humano, promoviendo conductas seguras, éticas y transparentes desde los altos directivos hasta todos los funcionarios.

De esta manera, el aporte radica en presentar una guía aplicable para implementar un sistema integral de seguridad de la información, involucrando no solo tecnologías y procesos, sino también concientizando a las personas sobre sus responsabilidades y la importancia de sus decisiones para proteger adecuadamente los activos informáticos.

Se propone que con la aplicación de este manual mejore sustancialmente la solidez de una estrategia de seguridad informática, al abordar de forma equilibrada aspectos de gobernabilidad, gestión administrativa, procesos operativos y comportamientos individuales.

c. Propuesta de creación de un plan de acción e implementación

La implementación exitosa requiere un enfoque integral que involucre la participación y el compromiso de todas las áreas de la organización, así como una gestión y monitoreo continuos para asegurar la efectividad de las medidas implementadas, es por ello por lo que se propone llevar a cabo los siguientes pasos:

1. Designar un líder del proyecto y conformar un equipo multidisciplinario que incluya representantes de diferentes áreas de la organización, como TICS, operaciones, recursos humanos, entre otros.
2. Definir roles y responsabilidades claras para cada miembro del equipo.
3. Desarrollar un cronograma detallado que incluya todas las tareas y actividades necesarias para la implementación del manual de seguridad.
4. Determinar los recursos humanos, financieros y tecnológicos requeridos para la implementación.
5. Crear un plan de comunicación efectivo para informar a todos los empleados sobre la implementación del manual de seguridad.
6. Utilizar diferentes canales de comunicación, como correos electrónicos, reuniones, carteles, etc.
7. Enfatizar la importancia y los beneficios de la seguridad informática para la organización.

8. Diseñar un programa de capacitación sobre las políticas, procedimientos y controles de seguridad establecidos en el manual.
9. Dividir la implementación en fases o áreas para facilitar la gestión y el seguimiento.

d. Propuesta para monitorear, evaluar y hacer cumplir la política.

Una propuesta sólida para monitorear, evaluar y hacer cumplir la política de seguridad informática es fundamental para garantizar la efectividad de las medidas de seguridad implementadas y mantener un alto nivel de protección para los activos de información y los sistemas de la organización.

1. Recopilar datos y métricas para medir la efectividad de las medidas implementadas.
2. Realizar ajustes y mejoras según sea necesario, basándose en los resultados del monitoreo.
3. Revisión y actualización periódica:
4. Programar revisiones periódicas del manual de seguridad para mantenerlo actualizado con los cambios en la tecnología, las amenazas y las mejores prácticas de la industria.
5. Involucrar al equipo de implementación y a los interesados clave en el proceso de revisión y actualización.
6. Recibir retroalimentación
7. Proceso de mejora continua

Para respaldar eficazmente el Sistema de Gestión de Seguridad de la Información (SGSI) de WILPRO S.A, se requerirá una variedad de documentación de referencia, formularios y otros materiales relacionados. A continuación, se detallan algunos de estos elementos:

Políticas de Seguridad de la Información: Documento que establece las políticas generales y específicas relacionadas con la seguridad de la información en la organización. Incluye políticas de acceso, uso aceptable, cifrado, manejo de incidentes, entre otras.

Formularios de Registro: Formularios diseñados para registrar información relevante durante la ejecución de procesos relacionados con la seguridad de la información. Esto puede incluir formularios de solicitud de acceso, formularios de informes de incidentes y formularios de evaluación de riesgos.

Matrices de Responsabilidades: Documentos que especifican las responsabilidades de cada individuo o departamento en relación con la seguridad de la información. Esto puede incluir

roles y responsabilidades en la gestión de accesos, la gestión de parches y la respuesta a incidentes.

Planes de Capacitación y Concientización: Documentos que detallan los programas de capacitación y concientización diseñados para educar al personal sobre las políticas y procedimientos de seguridad de la información. Incluye materiales de capacitación, calendarios de sesiones y evaluaciones de aprendizaje.

Documentación Técnica: Documentos técnicos relacionados con la configuración y operación de sistemas y herramientas de seguridad de la información. Incluye manuales de usuario, guías de configuración y documentación de API.

Registros de Auditoría y Monitoreo: Registros que documentan las actividades de auditoría y monitoreo realizadas para garantizar el cumplimiento de las políticas y procedimientos de seguridad de la información. Incluye registros de auditorías internas, registros de monitoreo de sistemas y registros de eventos de seguridad.

Estos son algunos ejemplos de la documentación y materiales relacionados que serán necesarios para respaldar eficazmente el SGSI de WILPRO S.A. Es importante mantener esta documentación actualizada y accesible para garantizar la efectividad del sistema y facilitar la gestión de la seguridad de la información en la organización.

e. Estrategias y/o técnicas

Para el desarrollo de este manual se consideraron varias técnicas como lo son; entrevista cualitativa director de TIC sobre el uso de normas ISO/IEC 27001 e ISO/IEC 38500 para mediante ello definir el alcance y objetivos de la misma, una matriz de riesgo para identificar activos de información con los riesgos potenciales y reales, se asignaran roles y responsabilidades, mediante la aplicación de la normas ISO/IEC 27001, gestión de capacitación, cambios en el personal y de controles de acceso, la realización de una tabla de declaración de aplicabilidad para conocer que normas se adaptan a la empresa, de esta forma y mediante los resultados obtenidos poder garantizar las mejores prácticas para conseguir los resultados deseados.

Análisis de amenazas

Para realizar esta evaluación con un enfoque metodológico adecuado se utilizará una matriz de riesgo, en primer lugar, se clasificará en cinco diferentes escenarios del impacto como se describe en la siguiente tabla:

Tabla 12

Clasificación de impacto

IMPACTO	IDENTIFICADOR
MUY ALTO	5
ALTO	4
MEDIO	3
MENOR	2
BAJO	1

Nota. Autoría propia.

Para cada amenaza se debe tipificar su probabilidad. La identificaremos con la frecuencia de ocurrencia. En el caso se utilizará 5 posibles valores, correspondientes a la frecuencia que se muestra en la siguiente tabla:

Tabla 13

Clasificación de probabilidad

PROBABILIDAD	IDENTIFICADOR
CIERTO	5
PROBABLE	4
POSIBLE	3
IMPROBABLE	2
RARO	1

Nota. Autoría propia.

Mediante la matriz de riesgo se podrá ponderar el impacto frente a la probabilidad de cada riesgo a la que se enfrenta la compañía, valorado en 4 grupos: Bajo, Medio, Alto y Grave, para su correcto tratamiento.

Tabla 14

Matriz de riesgo

RIESGO			IMPACTO				
			BAJA 1	MENOR 2	MEDIA 3	ALTA 4	MUY ALTA 5
PROBABILIDAD	CIERTO	5	MEDIO	ALTO	GRAVE	GRAVE	GRAVE
	PROBABLE	4	BAJO	MEDIO	ALTO	GRAVE	GRAVE
	POSIBLE	3	BAJO	MEDIO	MEDIO	ALTO	GRAVE
	IMPROBABLE	2	BAJO	BAJO	MEDIO	ALTO	ALTO
	RARO	1	BAJO	BAJO	BAJO	BAJO	MEDIO

Nota. Autoría propia.

Finalmente se deberá identificar los activos de mayor riesgo, determinando las amenazas a las que se expone la compañía, de tal manera que cuantifique la vulnerabilidad, midiendo la probabilidad de ocurrencia y el impacto al que se vería expuesta.

Tabla 15

Análisis Riesgo

N°	EVENTO	PROBABILIDAD	PROBABILIDAD NUMERICA	IMPACTO	IMPACTO NUMERICO	NIVEL DE RIESGO
1	Falta de documentación actualizada	INUSUAL	3	MEDIO	3	MEDIO
2	Daño no accidental de archivos	POSIBLE	3	ALTO	4	ALTO
3	Errores y omisiones en el ingreso de datos	FRECUENTE	5	MUY ALTO	5	MUY ALTO
4	Errores en el uso de archivos y programas	POSIBLE	3	ALTO	4	ALTO
5	Errores al abrir archivos de origen desconocido.	FRECUENTE	5	MUY ALTO	5	MUY ALTO
6	Errores involuntarios de empleados: Configuraciones equivocadas de seguridad, eliminación accidental de información, pérdida de equipos, entre otros.	PROBALBE	4	MUY ALTO	5	MUY ALTO
7	Acceso no autorizado a información sensible: Empleados que acceden a datos confidenciales sin fines legítimos por curiosidad o con intención de uso indebido.	RARO	1	MUY ALTO	5	MEDIO
8	Incumplimiento de políticas: No adoptar buenas prácticas como uso complejo de contraseñas, bloqueo de pantalla, manejo cuidadoso de información en espacios públicos.	POSIBLE	3	MENOR	2	MEDIO
9	Ingeniería social: Empleados vulnerables a técnicas de manipulación como phishing, pretexting, baiting para entregar información confidencial a terceros.	FRECUENTE	5	MUY ALTO	5	MUY ALTO
10	Uso indebido de recursos corporativos: Empleados que utilizan activos de TI para temas ilícitos, ilegales o para propósitos personales en horario laboral.	POSIBLE	3	MEDIO	3	MEDIO
11	Conexión de dispositivos no autorizados: Empleados que conectan a la red corporativa dispositivos personales sin protección adecuada, exponiendo información sensible de la empresa.	FRECUENTE	5	ALTO	4	MUY ALTO
12	Compartir cuentas y contraseñas entre usuarios facilita pérdida de control y dificulta la rendición de cuentas ante incidentes.	FRECUENTE	5	MUY ALTO	5	MUY ALTO
13	Colaboradores sancionados o despedidos que conservan acceso a sistemas o la habilidad para sabotear operaciones.	INUSUAL	2	MUY ALTO	5	ALTO

N°	EVENTO	PROBABILIDAD	PROBABILIDAD NUMERICA	IMPACTO	IMPACTO NUMERICO	NIVEL DE RIESGO
14	El uso de medios de almacenamiento personales sin restricciones puede introducir malware a la red corporativa.	FRECUENTE	5	MUY ALTO	5	MUY ALTO
15	Suplantación de identidad de ejecutivos para convencer a empleados de realizar transferencias no autorizadas.	FRECUENTE	5	MUY ALTO	5	MUY ALTO
16	Brechas de seguridad que no son reportadas por vergüenza, temor a consecuencias o falta de canales apropiados.	FRECUENTE	5	MEDIO	3	MUY ALTO
17	Personal susceptible para ser reclutado por organizaciones criminales para extraer información sensible.	INUSUAL	2	MUY ALTO	5	ALTO
18	Empleados descontentos que filtran información confidencial o propiedad intelectual a la competencia.	INUSUAL	2	MUY ALTO	5	ALTO
19	Conflicto de intereses de colaboradores en el manejo de información que puede afectar objetividad o ética empresarial.	RARO	1	MUY ALTO	5	MEDIO
20	Agotamiento, estrés y problemas personales: Empleados con productividad reducida o distraídos, propensos a cometer errores de seguridad o con intenciones de perjudicar a la empresa.	FRECUENTE	5	MUY ALTO	5	MUY ALTO

Nota. Autoría propia.

Declaración de aplicabilidad de controles de seguridad ISO/IEC 27001

Estos controles se han evaluado en referencia al estado actual habiéndose clasificados según la siguiente tabla:

Tabla 16

Descripción estatus tabla declaración de aplicabilidad ISO/IEC 27001

ESTATUS	SIGNIFICADO
? Desconocido	No ha sido revisado todavía
Inexistente	Ausencia completa de la política, procedimiento, control, etc.
Inicial	El desarrollo ha comenzado y requerirá un trabajo significativo para satisfacer las necesidades
Limitado	Progresando, pero no completado
Definido	El desarrollo está casi completo, faltan detalles y/o no está implementado
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y comenzó a operar
Optimizado	El requisito está plenamente desarrollado

Nota. Controles Normas ISO/IEC 27001:2022.

Para el caso de la Empresa WILPRO S.A. se han seleccionado de los 30 de los 93 controles del Anexo A, los cuales nos brindan la posibilidad de analizar el estado actual para la implementación de esos controles.

Tabla 17

Tabla declaración de aplicabilidad controles ISO/IEC 27001

Sección	Control de seguridad de la información	Estatus	Observaciones
A5	**Controles organizacionales**		
A.5.1	Políticas para la seguridad de la información	Inexistente	
A.5.2	Roles y responsabilidades en la seguridad de la información	Limitado	Los roles los asume el jefe de área de TIC sin embargo la seguridad se valida a discreción de cada uno de los empleados
A.5.3	Segregación de tareas	Limitado	No está totalmente definido
A.5.4	Responsabilidades de gestión	Limitado	No está totalmente definido
A.5.5	Contacto con las autoridades	? Desconocido	
A.5.7	Inteligencia de amenazas	Inicial	Existe una base de datos con información de amenazas frecuentes
A.5.12	Clasificación de la información	Inicial	No está totalmente detallado, sin embargo, se encuentra en proceso de clasificación
A.5.15	Control de Acceso	Inicial	Se encuentran creados roles, sin embargo, no se encuentran definidos los responsables
A.5.16	Gestión de la identidad	? Desconocido	
A.5.17	Información de autenticación	Inexistente	
A.5.18	Derechos de acceso	Inexistente	
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Inexistente	
A.5.26	Respuesta a los incidentes de seguridad de la información	Definido	El personal de TIC toma acción inmediatamente ante los incidentes reportados
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Limitado	Se encuentran generando su propia política de Seguridad y validado los requisitos de la LOPDP
A.5.35	Revisión independiente de la seguridad de la información	Inexistente	
A.5.36	Cumplimiento con las políticas, reglas y normas de la seguridad de la información	Inexistente	

A.5.37	Procedimientos operacionales documentados	Inicial	Se encuentra en proceso
A6	**Controles personales**		
A.6.1	Revisión de antecedentes	Inexistente	
A.6.2	Términos y condiciones de empleo	Limitado	definidos bajo el contrato laboral
A.6.3	Concientización, educación y entrenamiento en seguridad de la información	Inexistente	
A.6.4	Proceso disciplinario	Limitado	No existe clasificación
A.6.5	Responsabilidades luego de la finalización o cambio de empleo	Inexistente	
A.6.6	Acuerdos de confidencialidad o no revelación	Definido	Existe un acuerdo de confidencialidad firmado a la par con el contrato de trabajo
A.6.7	Trabajo remoto	Inexistente	
A.6.8	Reportes de eventos de seguridad de la información	Limitado	los reportes se los hace de manera personal y no un sistema de control
A7	**Controles físicos**		
A.7.7	Escritorio y pantalla limpios	Inexistente	
A.7.10	Medios de almacenamiento	Inexistente	
A8	**Controles tecnológicos**		
A.8.3	Restricción de acceso a la información	Inexistente	
A.8.12	Prevención de filtración de datos	Inexistente	
A.8.19	Instalación de software en sistemas operacionales	Inexistente	

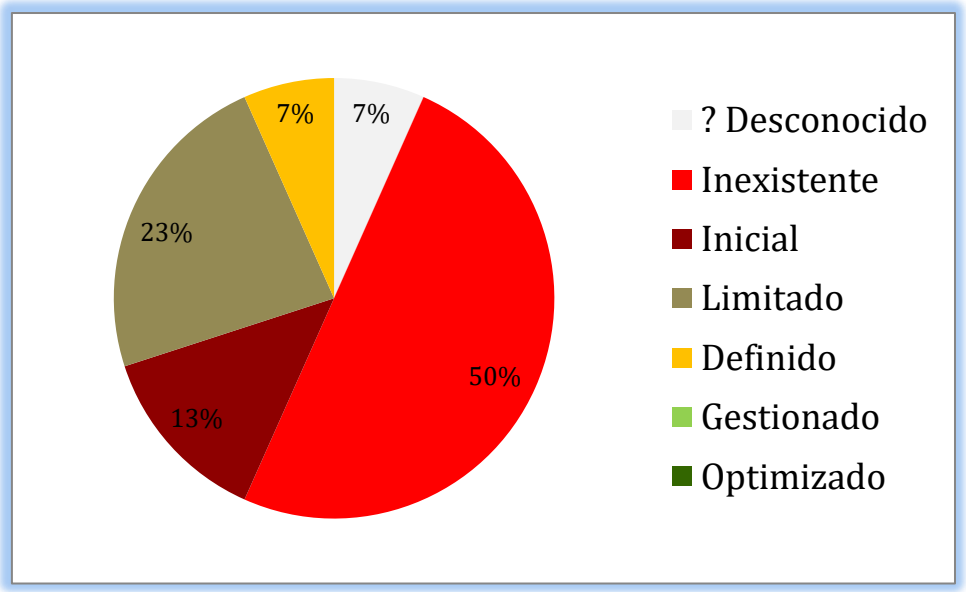
Nota. Autoría propia. Basado Controles Normas ISO/IEC 27001:2022.

Análisis

Al realizar el análisis de los resultados se puede evidenciar que el cincuenta por ciento de los controles verificados se encuentran en estado inexistente, es decir se encueran desatendidos, no existe documentación al respecto, el veinte y tres por ciento se encuentra en estado limitado, lo que nos indica que han iniciado un proceso de verificación, pero no se completado, y finalmente un trece por ciento se encuentra en estado inicial , lo que significa que han encontrado un punto de control pero no se ha desarrollado una política.

Figura 14

Estatus controles Wilpro



Nota. Autoría propia.

2.3. Validación de la propuesta

Se ha realizado la validación de la propuesta mediante el criterio de 3 especialistas los cuales se puedes verificar en el ANEXO 3, quienes han presentado sus criterios, comentarios y recomendaciones, donde se obtuvo un 95.23% de aprobación, según se puede visualizar en la Tabla 19 de Resultados de la validación.

Para la elección de especialistas se ha considerado un perfil acorde a encuentran los siguientes criterios: Formación académica relacionada con el tema investigativo, experiencia académica y/o laboral orientada a la informática y motivación para participar.

La siguiente tabla presenta información detallada de los actores seleccionados para la validación del modelo.

Tabla 18

Descripción de perfil de validadores

Nombres y Apellidos	Años de experiencia	Titulación Académica	Cargo
Byron Giovanny Guamushig	10 años	Magister en Gerencia de Sistemas y Tecnología Empresarial	Analista de la Dirección de Infraestructura, Seguridad y Soporte de T.I. del MREMH
Ivonne Dayana Sandoval	13 años	Magister en Gerencia de Sistemas y Tecnologías de la Información	Subgerente de Tecnologías de la Información y Comunicación CENACE
Edison Richard Condor	12 años	Ingeniero en Sistemas de Información	Analista de la Dirección de Infraestructura, Seguridad y Soporte de T.I. del MREMH

Nota. Autoría propia.

Los objetivos perseguidos mediante la validación son los siguientes:

- Validar la metodología de trabajo aplicada en el desarrollo de la investigación.
- Aprobar los resultados, conclusiones y recomendaciones obtenidas.
- Redefinir (si es necesario) el enfoque de los elementos desarrollados en la propuesta, considerando la experiencia de los especialistas.
- Constatar las posibilidades potenciales de aplicación del Plan de negocios propuesto.

Se han establecido los niveles de importancia y representatividad en la cual el valor máximo es de 5 puntos (Totalmente de acuerdo) que será otorgado según el desempeño adecuado del criterio; y un valor mínimo de un 1 punto (Totalmente en desacuerdo) en el caso de observarse un cumplimiento insuficiente.

Tabla 19

Resultados de la validación

Indicador	Experto 1	Experto 2	Experto 3	Total	Porcentaje
Impacto	5	5	5	15	100%
Aplicabilidad	4	4	5	13	86.66%
Conceptualización	5	4	5	14	93.33%
Actualidad	5	5	5	15	100%
Calidad Técnica	4	5	4	13	86.66%
Factibilidad	5	5	5	15	100,00%
Pertinencia	5	5	5	15	100,00%
Total	33	33	34	100	95.23%

*Nota***.** Autoría propia.

2.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 20

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Estudio al marco de referencia ISO/IEC 27001	Marco de referencia para buenas prácticas de un sistema de GSI (NQA, 2022).	Metodología bibliográfica.	Revisión de la norma vigente.	Permite una visión integral y define conceptos en Seguridad Informática.	Investigación bibliográfica.
Estudio al marco de referencia ISO/IEC 38500	Marco de referencia para gobernar las TI al interior de las organizaciones (ISO/IEC 38500, 2019).	Metodología bibliográfica.	Revisión de la norma vigente	Fomenta principios para las organizaciones en la gestión adecuada del gobierno de TI	Investigación bibliográfica.
Definir el alcance y los objetivos de la política.	Definición según el contexto de la empresa para establecer el alcance y los objetivos.	Metodología de investigación mixta.	Fuentes bibliográficas y entrevistas.	Define el alcance y los objetivos de una política de manera fundamentada y realista.	Entrevistas y encuestas.
Identificar los riesgos vinculados al factor humano.	Análisis de impacto y probabilidades.	Experimental, Entrevistas.	Elaboración matriz de riesgo.	Describe los riesgos a los que está expuesta la empresa y pondera el impacto.	Investigación y Observación.

Selección de controles de seguridad.	Análisis de controles ISO/IEC 27001 (NQA, 2022).	Experimental.	Elaboración de matriz (Declaración de aplicabilidad).	Describe el estado actual de cada control según marco de referencia Anexo ISO/IEC 27001.	Investigación y Observación.
Creación de un plan de acción e implementación.	Gobernanza de las TI al interior de las organizaciones (ISO/IEC 38500, 2019).	Metodología bibliográfica, Experimental	Propuesta de creación de un plan de acción e implementación	Se desarrolló una propuesta que permiten implementar el manual.	Investigación y Observación.
Monitorear, evaluar y hacer cumplir la política.	Evaluación y mejora continua mediante controles ISO/IEC 27001 (NQA, 2022).	Metodología bibliográfica,	Propuesta de creación de un plan de evaluación y mejora continua.	Se desarrolló una propuesta que permiten realizar el seguimiento y control del cumplimiento del manual.	Investigación y propuesta de plan de acción.
Creación del manual.	Creación de políticas de seguridad alineadas al factor humano.	Análisis de necesidades, Revisión por expertos.	Fuentes bibliográficas y entrevistas.	Sustento para la creación de un manual estructurado y alineado con las necesidades de los usuarios.	Investigación, entrevistas y validación de expertos.
Encuesta y entrevista a empleados.	Proceso de investigación mixta.	Encuestas y entrevistas.	Entrevistas a director TIC y encuestas a gerente y colaboradores.	Se desarrolla entrevistas y encuestas con el fin de conocer la situación actual de la empresa y cuáles son las vías por tomar.	Investigación y propuesta de plan de acción.

*Nota***.** Autoría propia.

CONCLUSIONES

En el entorno de la empresa Wilpro S.A., donde la información y la tecnología desempeñan un papel crucial, es fundamental contar con un manual de políticas de uso adecuado de las tecnologías de la información que sirva como guía, provea capacitación y concientización para educar a los empleados sobre los riesgos y las mejores prácticas para mitigar fallas de ciberseguridad, Esto fomenta una cultura de seguridad sólida en toda la organización, donde cada individuo comprenda su papel y responsabilidad en la protección de la información y los activos tecnológicos.

Se ha comprendido y definido los conceptos teóricos y las normas internacionales relacionadas de la seguridad Informática y la gobernanza de TI, las cuales son primordiales para una empresa que ha enfocado sus esfuerzos en mantener una cultura de seguridad, ayudando al objetivo general de desarrollar e implementar estrategias adecuadas para mitigar los riesgos asociados al factor humano en el manejo de la información.

De acuerdo con el diagnóstico del estado situacional actual de la empresa, enfocado en las brechas de seguridad relacionadas con el factor humano, se pudo comprobar que no existe un procedimiento adecuado y documentado que funcione como referencia para los empleados de la empresa Wilpro S.A. lo cual es un paso crítico para identificar las áreas de mejora que permitan mitigar estos riesgos y fortalecer la seguridad en toda la organización.

Este manual de políticas es una herramienta fundamental para fortalecer la cultura de seguridad de la organización y promover un comportamiento responsable y consciente de los empleados al interactuar con los recursos tecnológicos y la información confidencial. Al abordar directamente las debilidades humanas, se reducirá significativamente el riesgo de incidentes de seguridad causados por errores, negligencia o acciones maliciosas.

La valoración de la efectividad de las políticas de seguridad informática por parte de especialistas externos e independientes es un paso que brinda confianza, credibilidad y una perspectiva experta para garantizar que las políticas sean sólidas, efectivas y adaptadas a las necesidades específicas de la organización, aumentando así las posibilidades de éxito en la implementación y mitigación de los riesgos.

En conclusión, el diseño de un manual de políticas de seguridad informática específicas para abordar debilidades humanas, basado en los principios de ISO/IEC 38500 e ISO/IEC 27001, permitirá a la organización contar con un marco sólido y alineado con las mejores prácticas para mitigar los riesgos asociados al factor humano en la seguridad de la información.

RECOMENDACIONES

Se recomienda desarrollar un procedimiento sobre el uso y tratamiento de información, adicionalmente no han preparado reglamentación referente a la LOPDP, se debe asignar un procedimiento interno donde el departamento de TI asuma las responsabilidades del manejo de datos e implementar más controles adicionales a los 30 estudiados de las normas ISO/IEC 27001.

Se recomienda establecer un programa de gestión del conocimiento dentro de la empresa, que permita capturar, organizar y compartir de manera efectiva el conocimiento adquirido sobre seguridad informática y gobernanza de TI. Esto puede incluir la creación de repositorios de conocimiento, bases de datos de mejores prácticas, grupos de discusión y sesiones de intercambio de conocimientos.

Para fortalecer la cultura de seguridad y promover un comportamiento responsable de los empleados al interactuar con recursos tecnológicos e información, se recomienda complementar el manual de políticas con un programa integral de concientización y capacitación continua, estas acciones, junto con el manual de políticas, abordarán las debilidades humanas, reduciendo significativamente el riesgo causado por errores, negligencia o acciones maliciosas, y fomentando una cultura de seguridad sólida en toda la organización.

Se recomienda mantenerse al tanto de los cambios en el entorno tecnológico, las amenazas emergentes, las regulaciones, mejores prácticas y realizar los ajustes necesarios en las políticas y procedimientos para abordar estos cambios. Un proceso de revisión continua, respaldado por una estructura de gobernanza sólida, permitirá a la organización adaptar proactivamente sus controles de seguridad y mantener un alto nivel de protección para sus activos de información.

BIBLIOGRAFÍA

Angulo, W. (2023). *PROPUESTA DE ESTRATEGIA PARA EVITAR LA FUGA DE INFORMACIÓN EN EMPRESAS CONSTRUCTORAS UTILIZANDO DETECCIÓN POR COMPORTAMIENTO (UEBA) CASO DE ESTUDIO: SCMI INC (USA)*. https://repositorio.uisrael.edu.ec/bitstream/47000/3611/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-001.pdf

Arcos, M. (2023). *Análisis de brechas para la protección de datos personales en base a LOPD: Caso Mobilvendor*. https://repositorio.uisrael.edu.ec/bitstream/47000/3544/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-002.pdf

Cortijo, R., y Mullo, H. (2022). *SISTEMA DE CONTROL Y MONITOREO DE PARÁMETROS ELÉCTRICOS DE LA SUBESTACIÓN DE TRANSFORMACIÓN NOVACERO MEDIANTE LabVIEW.* http://repositorio.uisrael.edu.ec/handle/47000/3329

CQR. (2020). *POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN*. https://scj.gov.co/sites/default/files/planeacion/Poli%CC%81tica%20de%20Seguridad%20de%20la%20Informacio%CC%81n%20V.5-23122020.pdf

De la Llave, M., Donají, D., y Canal, E. (2022). *Efecto de la gestión del factor humano en la flexibilidad y la efectividad organizacionales en PYMEs turísticas mexicanas*. https://erevistas.uacj.mx/ojs/index.php/estudiosregionales/issue/view/735

DeloitteEcuador. (2023). *Seguridad de la información (SGSI)*. DeloitteEcuador: https://www2.deloitte.com/ec/es/pages/technology-media-and-telecommunications/articles/presentacion-de-resultados-encuesta-estado-actual-de-la-ciberseg.html

Estrada, S., Zuccarello, R., Chirinos, E., y Córdova, G. (2022). *Factor Humano y Cambio Organizacional*. http://fer.uniremington.edu.co/ojs/index.php/AMR/article/view/577/614

FECYT. (2022). *Política de Seguridad de la Información*. https://www.fecyt.es/sites/default/files/info/attachments/2022/02/politica_de_seguridad_de_la_informacion.pdf

García, M. (2018). *ISO/IEC 38500*. https://codingornot.com/gobierno-de-ti-que-es-la-isoiec-38500-y-para-que-sirve

Global Trust Association. (2019). *Objetivos Principales de la Norma ISO 38500 en la Organización*. https://globaltrustassociation.org/es/objetivos-principales-de-la-norma-iso-38500-en-la-organizacion/#:~:text=El%20objetivo%20de%20la%20norma,ante%20los%20cambios%20del%20entorno

GlobalSuite. (2023). *¿Qué es la norma ISO 27001 y para qué sirve?* https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Ibarra, O., y Cordero, M. (2022). *Políticas de seguridad de la información basadas en normas internacionales para garantizar controles ante amenazas y vulnerabilidades en el*

departamento de tecnología de la cooperativa de ahorro y crédito San Francisco LTDA. https://repositorio.uta.edu.ec/handle/123456789/34814

IRONTEC. (2022). *Política de Seguridad de la Información*. https://www.irontec.com/politica-de-seguridad-de-la-informacion-irontec-2022.pdf

ISO/IEC 38500. (2019). *Fundamentos del Gobierno de TI basados en ISO/IEC 38500*. https://www.researchgate.net/publication/254864701_Fundamentos_del_Gobierno_de_TI_basados_en_ISOIEC_38500

Medina, P., Chango, M., Corella, M., y Guizado, D. (2022). *Transformación digital en las empresas: una revisión conceptual*. https://dialnet.unirioja.es/descarga/articulo/8808726.pdf

Morera, M. (2022). *Los Sistemas de Información Gerencial y su evolución hacia la Cuarta Revolución*. https://www.researchgate.net/publication/363162743_Los_Sistemas_de_Informacion_Gerencial_y_su_evolucion_hacia_la_Cuarta_Revolucion

NQA. (2020). *ISO 27001:2013 - GUÍA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Pérez, F. (2023). *INFLUENCIA DE LA GESTIÓN Y COMPORTAMIENTO DE USUARIOS EN EL CONTROL DE LA*. https://repositorio.uisrael.edu.ec/bitstream/47000/3559/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2023-008.pdf

Sisti, M. (2019). *SEGURIDAD INFORMÁTICA: LA PROTECCIÓN DE LA INFORMACIÓN EN UNA EMPRESA VITIVINÍCOLA DE MENDOZA*. https://bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Tigse, J. (2020). *PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN EN LA EMPRESA PLASTICAUCHO INDUSTRIAL S.A.* https://repositorio.uta.edu.ec/bitstream/123456789/30696/1/Tesis_t1663si.PDF

UNIR. (2022). *Claves de las políticas de seguridad informática*. https://mexico.unir.net/ingenieria/noticias/politicas-seguridad-informatica/

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

Datos

Nombre: _____

Cargo: _____

Pregunta 1: ¿La organización asigna responsabilidades relacionadas con el gobierno de seguridad de la información?

Pregunta 2: ¿La organización asigna las responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos?

Pregunta 3: ¿El cuerpo directivo de la organización asignado para el manejo del gobierno de seguridad de la información tienen las competencias adecuadas para hacerlo?

Pregunta 4: ¿El cuerpo directivo encargado del gobierno de seguridad de la información supervisan los diferentes niveles de gestión de seguridad de la información?

Pregunta 5: ¿Se realiza un seguimiento a los roles y responsabilidades asignadas a los colaboradores para garantizar que la ejecución de los procesos relacionados con la seguridad de la información se realice de manera correcta a fin de evitar el error humano?

Pregunta 6: ¿Los colaboradores de la empresa atienden las responsabilidades básicas asignadas por el cuerpo directivo de la organización en materia de seguridad de la información?

Pregunta 7: ¿La organización dispone de un manejo de seguridad de la información, aunque estas no se encuentren integrados en las políticas de Gobierno de seguridad de la Información?

Pregunta 8: ¿Analiza el cuerpo directivo los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo empresarial interno?

Pregunta 9: ¿El cuerpo directivo de la empresa diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información?

Pregunta 10: ¿La organización realiza una planificación de la seguridad de la información y seguimiento a pequeño, medio y largo plazo?

ANEXO 2

FORMATO ENTREVISTA RESPONDIDO POR UN COLABORADOR

Datos

Nombre: _____

Cargo: _____

Pregunta 1: ¿La organización asigna responsabilidades relacionadas con el gobierno de seguridad de la información?

Respuesta: No, la organización muy poco asigna responsabilidades relacionadas con el gobierno de seguridad de la información.

Pregunta 2: ¿La organización asigna las responsabilidades del gobierno de seguridad de la información en base a criterios propios y no de modelos establecidos?

Respuesta: No, las responsabilidades del gobierno de seguridad de la información se asignan en base a criterios propios y también a modelos establecidos.

Pregunta 3: ¿El cuerpo directivo de la organización asignado para el manejo del gobierno de seguridad de la información tienen las competencias adecuadas para hacerlo?

Respuesta: Muy pocas, el cuerpo directivo de la organización asignado para el manejo del gobierno de seguridad de la información tiene las competencias adecuadas para hacerlo.

Pregunta 4: ¿El cuerpo directivo encargado del gobierno de seguridad de la información supervisan los diferentes niveles de gestión de seguridad de la información?

Respuesta: No, el cuerpo directivo encargado del gobierno de seguridad de la información muy poco supervisa los diferentes niveles de gestión de seguridad de la información.

Pregunta 5: ¿Se realiza un seguimiento a los roles y responsabilidades asignadas a los colaboradores para garantizar que la ejecución de los procesos relacionados con la seguridad de la información se realice de manera correcta a fin de evitar el error humano?

Respuesta: No, no se realiza un seguimiento a los roles y responsabilidades asignadas a los colaboradores para garantizar que la ejecución de los procesos relacionados con la seguridad de la información se realice de manera correcta a fin de evitar el error humano.

Pregunta 6: ¿Los colaboradores de la empresa atienden las responsabilidades básicas asignadas por el cuerpo directivo de la organización en materia de seguridad de la información?

Respuesta: No, no los colaboradores de la empresa atienden las responsabilidades básicas asignadas por el cuerpo directivo de la organización en materia de seguridad de la información.

Pregunta 7: ¿La organización dispone de un manejo de seguridad de la información, aunque estas no se encuentren integrados en las políticas de Gobierno de seguridad de la Información?

Respuesta: No, la organización no dispone de un manejo de seguridad de la información integrado en las políticas de Gobierno de seguridad de la Información.

Pregunta 8: ¿Analiza el cuerpo directivo los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo empresarial interno?

Respuesta: No, el cuerpo directivo muy poco analiza los riesgos asociados a la seguridad de la información desde el punto de vista operativo y de cumplimiento normativo empresarial interno.

Pregunta 9: ¿El cuerpo directivo de la empresa diseña procesos, políticas y procedimientos estratégicos relacionadas con la seguridad de la información?

Respuesta: No, el cuerpo directivo de la empresa no diseña procesos, políticas y procedimientos estratégicos relacionados con la seguridad de la información.

Pregunta 10: ¿La organización realiza una planificación de la seguridad de la información y seguimiento a pequeño, medio y largo plazo?

Respuesta: No, la organización no realiza una planificación de la seguridad de la información y seguimiento a corto, medio y largo plazo.

Pregunta 11 ¿Conoce acerca de normas internacionales para la seguridad informática?

Respuesta: Si, somos conscientes que debemos cumplir reglamentos de seguridad de la información, también apegados a la LOPDP y otras asociadas a normas internacionales y marcos de buenas prácticas como ITIL y normas ISO.

Pregunta 12 ¿Han aplicado de alguna norma internacional para la seguridad informática?

Respuesta: No, lamentablemente no tenemos el conocimiento suficiente

Pregunta 13. ¿Se ha capacitado al personal de la empresa en alguna norma o estándar internacional para el manejo de la seguridad informática?

Respuesta: Cada uno tienen nociones básicas de normas y buenas prácticas.

Pregunta 14. ¿Considera que la elaboración y ejecución de un manual de políticas de seguridad informática puede ayudar a la empresa a protegerse de ataques y robos de información?

Respuesta: Ayudaría que haya un apoyo por parte de Administración, para que todo el personal se inmiscuya y se comprometa con las normas de seguridad

Pregunta 15. ¿Considera que las políticas de seguridad de la información son relevantes para el progreso?

Respuesta: Si, marcan un camino para un correcto proceso

ANEXO 3
VALIDACIÓN DE PROFESIONALES
VALIDACIÓN PROFESIONAL # 1

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de políticas de seguridad informática mediante la aplicación de norma ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: SANDOVAL ENRIQUEZ IVONNE DAYANA

Título obtenido
Magister en Gerencia de Sistemas y Tecnologías de la Información
Cédula de Identidad
1718535626
E- mail
dsandoval@cenace.gob.ec
Institución de Trabajo
OPERADOR NACIONAL DE ELECTRICIDAD - CENACE
Cargo
Subgerente de Tecnologías de la Información y Comunicación
Años de experiencia en el área
13 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de políticas de seguridad informática mediante la aplicación de norma ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A.

Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	***X***				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		***X***			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	***X***				
Total		***25***	***8***			

Observaciones: El documento se alinea a las políticas de estado y a la transformación digital que es parte del Plan de gobierno que atañe tanto a entidades públicas como privadas, en este sentido el documento apalanca y aporta de manera significativa a WILPRO S.A para resguardar sus activos de información.

Recomendaciones

Implementar el Manual, y las políticas indicadas ya que se enmarca en estándares y marcos de referencias internacionales, efectuar los controles y seguimiento a cada proceso implementado para conseguir un nivel de madurez adecuado en mediano plazo.

Lugar, fecha de validación: Quito, 7 de marzo del 2024

Firmado electrónicamente por:
IVONNE DAYANA
SANDOVAL ENRIQUEZ

Firma del especialista

VALIDACION DE PROFESIONALES
VALIDACIÓN PROFESIONAL # **2**

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de un manual de políticas de seguridad informática mediante la aplicación de norma ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: BYRON GIOVANNY GUAMUSHIG LASLUISA

Título obtenido
Magister en Gerencia de Sistemas y Tecnología Empresarial
Cédula de Identidad
1718048224
E- mail
Giovanny.guamushig@gmail.com
Institución de Trabajo
Ministerio de Relaciones Exteriores y Movilidad Humana
Cargo
Analista de la Dirección de Infraestructura, Seguridad y Soporte de T.I.
Años de experiencia en el área
10 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de un manual de políticas de seguridad informática mediante la aplicación de norma ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*		***X***			
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***X***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total		*25*	*8*			

Observaciones: La propuesta destaca la importancia de un enfoque integral que combine la comprensión teórica, el diagnóstico y el diseño para mitigar los riesgos asociados al factor humano en la seguridad informática de la empresa. Esta perspectiva holística es fundamental para abordar eficazmente este tipo de riesgos, ya que considera tanto los aspectos técnicos como los humanos de la seguridad.

Se resalta la organización clara y concisa del manual, con secciones y subsecciones claramente definidas. Esta estructura facilita la navegación y la búsqueda de información específica, lo que convierte al manual en una herramienta útil y accesible para los usuarios.

Lugar, fecha de validación: Quito D.M. 07 de marzo de 2024

Firmado electrónicamente por:
BYRON GIOVANNY
GUAMUSHIG LASLUISA

_____

Firma del especialista

VALIDACION DE PROFESIONALES
VALIDACIÓN PROFESIONAL # **3**

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: **Propuesta de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A.**

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: EDISON RICHARD CONDOR LICERO

Título obtenido
Ingeniero en Sistemas de Información
Cédula de Identidad
1720138963
E- mail
econdor@cancilleria.gob.ec
Institución de Trabajo
Ministerio de Relaciones Exteriores y Movilidad Humana
Cargo
Analista
Años de experiencia en el área
12 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de políticas de seguridad informática mediante la aplicación de normas ISO/IEC 38500 e ISO/IEC 27001 alineadas al componente humano para la empresa WILPRO S. A.

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	***X***				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*		***X***			
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total		*30*	*4*			

Observaciones: El lenguaje utilizado en el manual es claro, conciso y fácil de entender, evitando tecnicismos innecesarios o jerga compleja, lo que lo hace accesible para todo tipo de usuarios, es evidente que el manual se mantiene actualizado y refleja información vigente, lo que lo convierte en una herramienta de referencia confiable y valiosa.

Recomendaciones

Es recomendable que los responsables de la implementación y capacitación realicen talleres interactivos con los empleados, para un primer acercamiento amigable a las políticas planteadas.

Lugar, fecha de validación: Quito, 8 de marzo del 2024

Firmado electrónicamente por:
EDISON RICHARD
CONDOR LICERO

Firma del especialista

WILPRO

MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL PERSONAL DE LA EMPRESA WILPRO S.A.

Contenido

1 INTRODUCCIÓN

El propósito de este manual es establecer un conjunto de políticas y procedimientos claros y detallados relacionados con la seguridad de la información en WILPRO S.A, con el objetivo de proteger los activos de información de la organización y garantizar la confidencialidad, integridad y disponibilidad de los datos. Este manual está diseñado para proporcionar orientación y directrices a todos los miembros de la organización sobre cómo manejar, procesar y proteger la información de manera segura. Adicionalmente, el manual tiene como propósito promover una cultura de seguridad de la información dentro de la organización, donde todos los empleados entiendan la importancia de su papel en la protección de la información y estén comprometidos con las prácticas y políticas de seguridad establecidas. Al tener políticas claras y procedimientos bien definidos, se busca minimizar los riesgos de seguridad de la información y proteger la reputación y la integridad de la empresa frente a posibles amenazas y vulnerabilidades, finalmente proporcionar un marco integral para la gestión de la seguridad de la información en WILPRO S.A, con el fin de proteger los activos de información, garantizar el cumplimiento de las regulaciones y normativas pertinentes, y mantener la confianza y la satisfacción de los clientes y partes interesadas.

Misión y Visión de la empresa

Velamos por la seguridad de nuestros clientes y de toda la sociedad, brindamos asesoría y calidad en general en un servicio integral de seguridad privada, contribuyendo así a reducir los mayores casos de inseguridad registrados en el país.

Ser reconocida por nuestros clientes como la empresa de seguridad más confiable y eficiente del mercado ecuatoriano, mantener un compromiso inquebrantable con la seguridad y el orden.

Objetivos del manual

Definir los lineamientos, políticas generales y específicas que deben cumplir todos los empleados de la empresa WILPRO S.A, contratistas o terceros que cuenten con acceso a la información, frente a amenazas internas o externas, acciones deliberadas o accidentales, para garantizar y preservar la confidencialidad, integridad y disponibilidad de los activos de la información.

Alcance y aplicabilidad

Este documento aplica a todos los niveles, tales como empleados, directores y terceros (como proveedores y contratistas), usuarios internos y externos que accedan o utilicen cualquier medio de información independientemente de su ubicación, medio o formato.

Definir roles y responsabilidades para la implementación, monitoreo y mejora del SGSI.

Definiciones y terminología clave

- **ISO/IEC 27001**: Estándar técnico diseñado para proporcionar un modelo para establecer, implementar, operar, monitorear, auditar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI).

- **ISO/IEC 38500:** Es un estándar internacional para el Gobierno de TI
- **Cliente**: La entidad o persona que recibe productos y/o servicios.
- **Efectividad**: Grado en el que se llevan a cabo las actividades planificadas y se logran los resultados planificados.
- **Eficiencia**: relación entre los resultados alcanzados y los recursos utilizados.
- **Mejora continua**: Toma de acciones continuas para mejorar la capacidad de cumplir con los requisitos y optimizar el rendimiento.
- **Acuerdo de Confidencialidad**: Un documento el área de talento humano que declara su voluntad de mantener la confidencialidad de la información
- **Autenticación de dos factores**: El sistema de autenticación utiliza al menos dos factores de verificación básicos: algo que alguien sabe (contraseña, PIN, número de perfil, nombre de familiar, etc.) que tiene la persona. (credenciales, deslizamiento, token, etc.) o algo sobre esa persona (reconocimiento facial, voz, iris, retina, etc.). De esa manera, si uno de los factores se ve comprometido, todavía hay otro factor que brinda seguridad.
- **Ciberseguridad**: Es el proceso de proteger los activos de información evitando amenazas a la información que se procesa, almacena y/o transmite a través de sistemas de información interconectados.
- **Confidencialidad**: La propiedad que dicta que la información no puede ser proporcionada ni divulgada a personas, entidades o procesos no autorizados, y solo el personal autorizado puede acceder a esa información.
- **Accesibilidad**: Solo los usuarios autorizados pueden acceder a información y atributos de activos relacionados cuando sea necesario.
- **Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseados o inesperados que pueden comprometer la confidencialidad, integridad y/o disponibilidad de la información
- **Legalidad**: Se refiere al cumplimiento por parte de la empresa de leyes, reglamentos, normas o reglamentos.
- **Oficial de seguridad de la información**: Persona que supervisa el cumplimiento de esta política y brinda asesoramiento a los empleados sobre cuestiones de seguridad de la información.
- **Medios de almacenamiento extraíbles**: Los dispositivos de almacenamiento extraíbles son dispositivos de almacenamiento que son independientes de la computadora y pueden transportarse libremente.
- **Perfil de Usuario**: Usuarios con necesidades de información similares y las mismas autorizaciones a recursos informáticos o sistemas de información. Se les conceden derechos de acceso en función de las funciones que desempeñan.
- **Riesgo**: La combinación de la probabilidad de un evento y sus consecuencias o consecuencias.
- **Seguridad de la información**: protección de la confidencialidad, integridad y disponibilidad de la información.
- **Malware**: Se refiere a diversos software o programas con código malicioso e intrusivo diseñados para ingresar a computadoras o redes para dañar o robar recursos informáticos, o sistemas de información.

2 MARCO NORMATIVO

Normas ISO/IEC 27001 e ISO/IEC 38500

La norma ISO 27001 establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) dentro de una organización. Su objetivo principal es garantizar la protección de la información mediante la identificación de riesgos, la definición de estrategias para mitigarlos y la implementación de salvaguardas adecuadas. Esta norma se aplica a organizaciones de cualquier tamaño, sector o industria, y busca asegurar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de los requisitos legales y regulaciones relacionadas con la seguridad de la información.

Por otro lado, la norma ISO 38500 establece las directrices y principios para el gobierno de las tecnologías de la información (TI) en una organización. Su objetivo es ayudar a los directivos y líderes empresariales a comprender la importancia estratégica de las TI y a tomar decisiones informadas sobre su uso y gestión. Esta norma se basa en seis principios fundamentales, incluyendo el liderazgo, la responsabilidad, la estrategia, la adquisición, el rendimiento y la conformidad. ISO 38500 se aplica a todos los tipos de organizaciones, independientemente de su tamaño o industria, y busca promover el uso efectivo, eficiente y aceptable de las TI en la empresa.

La aplicación conjunta de las normas ISO 27001 e ISO 38500 en el SGSI permitirá establecer un marco integral de seguridad de la información y gobernanza de las TI en la organización, asegurando la protección de los activos de información y el uso estratégico de la tecnología para impulsar el éxito empresarial.

Enfoque en factor humano

Incrementar el conocimiento de los requisitos técnicos de la norma de seguridad de la información ISO/IEC 27001 que requieren la creación, implementación y mejora continua de sistemas de gestión de seguridad de la información y ISO 38500 que provee un marco para gobernar las TI al interior de las organizaciones, todo esto para que el personal de la empresa cuente con una herramienta de acción referente a la seguridad informática y sus funciones.

3 ESTRUCTURA ORGANIZACIONAL

Descripción de la estructura de gobierno y responsabilidades relacionadas con la seguridad de la información.

Junta Directiva:

La Junta Directiva de WILPRO S.A es responsable de establecer la visión estratégica de la empresa, incluyendo las políticas y objetivos relacionados con la seguridad de la información, Se encarga de aprobar el presupuesto y los recursos necesarios para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo.

Comité de Seguridad de la Información (CSI)

El CSI está compuesto por representantes de la alta dirección, los responsables de TI, seguridad y cumplimiento, y otros expertos relevantes.

Su función es supervisar y dirigir las iniciativas de seguridad de la información, incluyendo la implementación y el mantenimiento del SGSI.

Oficial de Seguridad de la Información (OSI)

El OSI es el responsable designado para liderar y coordinar todas las actividades relacionadas con la seguridad de la información en WILPRO S.A.

Se encarga de desarrollar e implementar políticas, procedimientos y controles de seguridad, así como de promover la conciencia y la capacitación en seguridad de la información.

Departamentos y Empleados

Todos los departamentos y empleados de WILPRO S.A tienen responsabilidades específicas en relación con la seguridad de la información.

Esto incluye cumplir con las políticas y procedimientos de seguridad establecidos, proteger los activos de información y reportar cualquier incidente o vulnerabilidad de seguridad.

La estructura de gobierno y las responsabilidades relacionadas con la seguridad de la información están diseñadas para garantizar que WILPRO S.A cuente con un enfoque integral y colaborativo para proteger sus activos de información y mitigar los riesgos de seguridad.

4 POLÍTICA DE SEGURIDAD INFORMÁTICA

La empresa WILPRO S.A. define los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad, siendo estos catalogados mediante el manal de clasificación de la información, y establecidos según la siguiente tabla:

Nivel de confidencialidad	***Etiquetado*** ***(DE SER NECESARIO)***	***Criterios de clasificación***	***Restricción de acceso***
Pública	(sin etiquetar)	Hacer pública la información no puede dañar a la organización de ninguna forma	Disponible para todo el público
Uso interno	USO INTERNO	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la organización	La información está disponible para todos los empleados y terceros seleccionados
Restringida	RESTRINGIDA	El acceso no autorizado a la información podría dañar considerablemente el negocio y/o la reputación de la organización	La información está disponible solamente para un grupo específico de empleados y de terceros autorizados
Confidencial	CONFIDENCIAL	El acceso no autorizado a la información podría dañar de forma catastrófica (irreparable) el negocio y/o la reputación de la organización	La información está disponible solamente para personas de la organización

Los empleados, contratistas o terceros deben aplicar la clasificación de la información, el inventario de activos de información y lineamientos para la administración de los archivos.

Cada propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información.

Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

Política de control de acceso

Todos los usuarios deben tener un identificador único (ID de usuario) para uso personal y se debe seleccionar una técnica de autenticación adecuada para garantizar la identidad del usuario. Este control se aplica a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de redes y administradores de bases de datos etc.)

El Proceso de Administración de Tecnologías e Información debe controlar el acceso mediante el enfoque basado en roles, aplicando los siguientes principios:

- **Lo que necesita conocer:** solamente se concede acceso a la información que la persona necesita para la realización de sus tareas (diferentes tareas/roles significan diferentes cosas que se necesita saber y, en consecuencia, diferentes perfiles de acceso).
- **Lo que necesita usar:** solamente se concede acceso a las instalaciones de procesamiento de información (equipos de TI, aplicaciones, procedimientos,) que la persona necesita para la realización de su tarea/trabajo/rol.

Para los usuarios que requieran contar con servicios especiales de mensajería instantánea, páginas de encuentro o descargas, deben ser autorizados por el jefe inmediato, justificando la necesidad del acceso

Las conexiones remotas a los recursos de la plataforma tecnológica; deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

Política de contraseñas

Los usuarios y contraseñas son de uso personal e intransferible, cualquier utilización indebida y/o irregularidad debe ser responsabilidad del colaborador. Como medida de seguridad los usuarios deben crear y administrar sus contraseñas siguiendo las siguientes normas para la creación y el uso:

- Las contraseñas se consideran como información confidencial y deben ser protegidas como tal.
- La contraseña debe tener al menos ocho (8) caracteres, donde se tengan letras en mayúscula, minúscula y números o caracteres especiales.
- Las contraseñas deben cambiarse mínimo cada 60 días y no se pueden repetir las ultimas 10 contraseñas.
- Si se digita más de 3 veces la contraseña de forma inválida, la cuenta del usuario debe ser bloqueada.
- La contraseña no debe incluir un nombre o palabra en algún lenguaje común (español, inglés, etc. evitando que éstas sean vulnerables a los ataques de diccionarios.) u otra

información pública como números de tarjeta de crédito, nombres de calles y números telefónicos. Una contraseña debe incluir información que solo sea conocida por el usuario.

- No utilizar contraseñas por defecto, éstas se deben cambiar una vez se adquieran componentes tecnológicos nuevos o sistemas de información que perfectamente las puedan incluir.
- No es permitido compartir usuarios, contraseñas y cualquier mecanismo de autenticación asignado.
- En los casos que se sospeche del compromiso de una contraseña en un posible incidente de seguridad, ésta debe ser cambiada inmediatamente por el administrador de la aplicación y debe reportarse al Oficial de Seguridad de la Información.
- Los usuarios deben tener presente no incluir las claves en ningún proceso de registro automatizado; por ejemplo, almacenado en una macro o sistema de información.

Política de pantalla limpia

Todos los colaboradores del WILPRO deben conservar su pantalla del escritorio libre de información confidencial, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

- Los computadores deben cargar por defecto el fondo de pantalla de la empresa WILPRO S.A. éste no debe ser modificado y debe permanecer activo.
- Los empleados y contratistas deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplique el comando de bloqueo oprimiendo simultáneamente las teclas Windows + L), a su vez, la Oficina de Tecnología e Información debe implementar mecanismos para cierres de sesión automáticos no superior a cinco minutos.
- Los usuarios son responsables y asumen las consecuencias por la pérdida de información que este bajo su custodia.
- Se prohíbe el almacenamiento de información personal en los computadores de la empresa. El escritorio lógico (del computador) debe estar libre de información restringida o confidencial.

Política de dispositivos móviles

- Los dispositivos móviles corporativos (teléfonos inteligentes, tablet, portátiles), son herramientas de trabajo que se deben utilizar únicamente para el desarrollo de actividades relacionadas con los procesos de la empresa.
- Con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles la Oficina de Tecnología e Información debe controlar la conexión de dispositivos móviles tales como Smartphone, tablets y computadores personales de los contratistas a la red corporativa, a excepción de los dispositivos que sean propiedad de la empresa.

Política de correo electrónico

- El correo electrónico personal no debe utilizarse para ningún proceso de la Entidad.
- El usuario de correo electrónico debe ser igual al usuario de red, y contar con single on (mismo usuario, misma contraseña en los dos (2) servicios.
- Los empleados, contratista o terceros, deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que provienen de correos electrónicos desconocidos.

- Los empleados tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los empleados.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la empresa y cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la empresa.
- Está prohibido el envío de o intercambio de mensajes con contenido que atente contra la integridad de las personas o clientes, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que atente con la integridad de las personas.
- Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo con los niveles de clasificación teniendo en cuenta el tipo de información que se pretende compartir.
- Es responsabilidad de cada usuario asegurar los destinarios a los cuales va dirigida una comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.
- El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen empresarial.
- Está prohibido la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor

Política de navegación web

- Hacer uso adecuado del servicio de internet de acuerdo con las actividades que se desarrollan.
- Se bloquea y prohíbe el acceso a sitios de apuestas, pornografía, descargas ilegales, etc. que impliquen riesgos legales o de seguridad.
- Sólo se permite descargar programas aprobados por TI o que provengan de fuentes confiables para evitar malware.
- Se sugiere no guardar contraseñas ni formularios de autocompletar en los navegadores web.
- El acceso a la red wifi para visitantes se realiza a través de la red definida para el fin y con uso de la clave establecida que será suministrada por área de TIC.
- Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso

5 LINEAMIENTOS DE SEGURIDAD PARA EL FACTOR HUMANO

Seguridad de Recursos Humanos

- Talento Humano deberá desarrollar un procedimiento de selección de acuerdo con las normas vigentes para tal efecto.
- Previo a la contratación, talento humano elaborará una lista de verificación que contiene los aspectos necesarios para revisar la experiencia de las personas empleadas para la prestación de servicios de acuerdo con las disposiciones reglamentarias vigentes.

- Talento Humano debe establecer los mecanismos o controles necesarios para proteger la confidencialidad y privacidad de la información contenida en el historial laboral y los documentos contractuales.
- Cada empleado y/o contratista deberá firmar un documento o cláusula que establezca un acuerdo de confidencialidad y no divulgación de la información de WILPRO S.A. los cuales deben registrarse en el historial laboral del empleado.

Concientización / Estrategias para minimizar el error humano.

- Recibir las capacitaciones o sensibilizaciones sobre Seguridad informática, de tal forma que tenga conocimiento respecto a las Políticas.
- Participar en las distintas capacitaciones y/o jornadas de sensibilización lideradas por el área de TICS

Gestión de derechos de acceso privilegiado

- Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso; acciones de esta naturaleza se consideran violatorias de las políticas de la Entidad.
- La información de gestión del área deber ser almacenada por los usuarios en carpetas compartidas del área y la información de gestión del usuario en el almacenamiento virtual de One Drive corporativo de Office 365.
- Se realizará una verificación trimestral para validar el correcto uso de los repositorios de información definidos.

Alta y baja de usuarios

Para la alta y baja de usuarios se procederá bajo las siguientes condiciones

- El acceso a los sistemas será suspendido para todo empleado o colaborador que se encuentre en licencia, permisos, vacaciones, entre otras novedades; si por necesidad del negocio se requiere mantener habilitado, únicamente para cargos a nivel de jefatura, para los demás cargos si existen funciones que se deban reasignar para dar continuidad durante dichas novedades, los jefes o delegados deben realizar las solicitudes de acceso necesarias a los colaboradores que ejecutaran las actividades, una vez cumplido el plazo se debe solicitar retiro de los permisos, además;
- Los usuarios creados que no hayan sido utilizados en un período mayor o igual a 3 meses serán inhabilitados por los administradores, así mismo, si éstas no han sido utilizadas en un periodo igual o mayor a 6 meses debe ser eliminadas
- El acceso a los sistemas será suspendido al fin del vínculo laboral o contrato.
- Cuando el responsable de la información lo solicite.
- Los derechos de acceso de un usuario se reasignarán únicamente por cambio de cargo o traslado de área, dentro de la empresa.

6 GESTIÓN DE INCIDENTES DE SEGURIDAD.

Se proporcionará capacitación regular a los empleados sobre cómo reconocer y responder a incidentes de seguridad de la información. Se enfatizará la importancia de reportar incidentes de manera oportuna y de seguir los procedimientos establecidos.

Estos procedimientos garantizarán una respuesta efectiva y organizada ante cualquier incidente de seguridad de la información, minimizando el impacto en WILPRO S.A y protegiendo la confidencialidad, integridad y disponibilidad de los datos de la organización.

Proceso de notificación y gestión de incidentes

- Es responsabilidad del empleado, contratista o personal provisto por terceros, informar de los incidentes de seguridad informática a la Oficina de Tecnología.
- Es responsabilidad del usuario reportar un correo electrónico cuando crea que es de dudosa procedencia a la Oficina de Tecnología, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad
- Los empleados, contratista o terceros del Ministerio que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a la Oficina de Tecnología, con el fin de ejercer los controles correspondientes.

Proceso disciplinario

La Política de Seguridad de la información, pretende instituir y afianzar la cultura informática segura en los empleados, y personal externo de la empresa:

- El incumplimiento de esta política está sujeto a las sanciones disciplinarias, fiscales y penales que se deriven de la conducta del implicado, incluso cuando se encuentre en situaciones administrativas como permisos, licencias, vacaciones, suspensiones en ejercicio del empleo o en comisión.
- Toda actividad informática (escaneos de seguridad, ataques de autenticación o de denegación de servicio, etc.) no autorizada que afecte tanto las redes empresariales como los sistemas de información, están prohibidas dando lugar a los procesos disciplinarios y/o legales correspondientes.
- El empleado o contratista que por negligencia no reporte a tiempo un incidente de seguridad o que aproveche deficiencias de seguridad y haga mal uso de la información, será investigado para establecer las sanciones disciplinarias.
- Cualquier intento de interferencia, obstrucción o de disuadir a quien reporta una posible violación de seguridad, está prohibido y será motivo de una acción disciplinaria.

7 AUDITORÍAS Y EVALUACIONES:

Las auditorías y evaluaciones son herramientas que permiten verificar el cumplimiento del manual, identificar áreas de mejora, evaluar la eficacia y eficiencia de los procesos:

Para asegurar la efectividad y conformidad del Sistema de Gestión de Seguridad de la Información (SGSI) de WILPRO S.A, se implementarán los siguientes procesos para realizar auditorías internas y evaluaciones de conformidad:

- Se establecerá un plan anual de auditorías internas que defina el alcance, los objetivos y los criterios de evaluación de cada auditoría. Este plan será revisado y aprobado por la dirección de la organización.
- Se designará un equipo de auditores internos capacitados y competentes en seguridad de la información para llevar a cabo las auditorías. Estos auditores deben ser independientes de las áreas que están siendo auditadas y deben poseer el conocimiento necesario para evaluar los controles de seguridad.
- Durante las auditorías internas, se evaluará la conformidad del SGSI con los requisitos establecidos en la norma ISO 27001 y otros estándares pertinentes. Se identificarán las no conformidades y se registrarán para su posterior seguimiento y corrección.

Acciones Correctivas y Preventivas:

- Se establecerán procedimientos para abordar las no conformidades identificadas durante las auditorías internas. Se asignarán responsabilidades para corregir las

deficiencias encontradas y se implementarán acciones correctivas y preventivas para evitar su recurrencia.

- Se realizará un seguimiento continuo de las acciones correctivas y preventivas para verificar su efectividad y cumplimiento. Además, se llevará a cabo una revisión periódica del SGSI para garantizar su mejora continua y su alineación con los objetivos estratégicos de la organización.
- Estos procesos asegurarán que las auditorías internas sean realizadas de manera sistemática y efectiva, permitiendo a WILPRO S.A identificar oportunidades de mejora y mantener la conformidad con los requisitos de seguridad de la información.

Mejora Continua:

- Se establecerán mecanismos para recopilar retroalimentación de todas las partes interesadas, incluidos empleados, clientes, proveedores y socios comerciales, sobre la eficacia del SGSI y las áreas de mejora.
- Se analizarán los resultados de las auditorías internas, evaluaciones de riesgos, incidentes de seguridad y otros procesos de monitoreo para identificar tendencias, áreas de debilidad y oportunidades de mejora.

Establecimiento de Objetivos de Mejora:

- Basándose en los hallazgos y análisis, se establecerán objetivos específicos y medibles para mejorar el desempeño del SGSI. Estos objetivos deben estar alineados con los objetivos estratégicos de la organización.

Implementación de Mejoras:

- Se llevarán a cabo las acciones planificadas para mejorar el SGSI. Esto puede implicar cambios en los procesos operativos, actualizaciones de tecnología, asignación de recursos adicionales y otras iniciativas.
- Seguimiento y Evaluación:
- Se realizará un seguimiento continuo del progreso hacia el logro de los objetivos de mejora. Se evaluará la efectividad de las acciones implementadas y se realizarán ajustes según sea necesario.
- Revisión por la Dirección:
- Se llevará a cabo una revisión periódica por parte de la dirección de la organización para evaluar el desempeño del SGSI y la efectividad de las medidas de mejora implementadas. Se tomarán decisiones informadas sobre los próximos pasos a seguir.
- Se fomentará una cultura organizacional que promueva la mejora continua en todos los niveles de la organización. Se alentará la participación del personal en la identificación de oportunidades de mejora y en la implementación de soluciones.
- Es importante adaptar la estructura del manual a las necesidades y características específicas de la organización, asegurándose de cumplir con los requisitos de las normas ISO 27001 e ISO 38500.

Responsabilidades del empleado para la gestión de políticas de Seguridad Informática

- Conocer y cumplir la política.
- Ser responsable del manejo de la información clasificada y reservada, para que ésta sea protegida con las medidas de seguridad necesarias.
- Realizar notificación y retroalimentación para futuros procesos de mejora continua.

Responsabilidades para la gestión de políticas de la Alta Dirección

- Cumplimiento con requisitos legales y contractuales
- Privacidad y Protección de Información de Datos Personal, será responsable del tratamiento de los Datos Personales, tal y como se define en la LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES, respeta la privacidad de terceros que le suministren sus datos personales a través de los diferentes puntos de recolección y captura de información. Por lo tanto, WILPRO. S.A. implementará los controles necesarios para su protección y en ningún momento divulgará esta información a terceras partes a menos que cuente con la autorización formal de los mismos o en los casos en que la Ley lo permita.
- Cumplir y obedecer con los acuerdos de licenciamiento de software y las leyes de derechos de autor.
- Compromiso y apoyo en el diseño e implementación de políticas que garanticen la mitigación de riesgos de Seguridad informática.
- Revisión y aprobación de las presentes Políticas de Seguridad informática.
- Incentivar la cultura de Seguridad.
- Aprobar la divulgación de esta política a todos los empleados de la empresa
- Establecer los recursos para implementar y mantener las iniciativas de seguridad informática
- Validar el correcto cumplimiento de las presentes Políticas de Seguridad de la Información.
- Facilitar los espacios y tiempos para la capacitación de los trabajadores en materia de seguridad, para participar en las actividades respectivas.

VERSIÓN	ELABORADO POR	REVISADO Y APROBADO POR
1.0	**NOMBRE:** MAURICIO BAZÁN **ESTUDIANTE UNIVERSIDAD ISRAEL** Fecha: 06 de marzo de 2024	**NOMBRE:** WILLIAM PROAÑO **GERENTE WILPRO S.A.** Fecha: 06 de marzo de 2024