FACULTAD DE POSTGRADO
TRABAJO FINAL DE GRADUACIÓN

DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN NORMA ISO 27001:2022 EN EMPRESA SAN SERVICES S. de R. L.

SUSTENTADO POR:

ALEXANDER ENOC BONO RIVERA
LUIS ANTONIO TINOCO RIOS

PREVIA INVESTIDURA AL TÍTULO DE

MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

SAN PEDRO SULA, CORTÉS, HONDURAS, C.A.

AGOSTO, 2024

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTORA

ROSALPINA RODRÍGUEZ

VICERRECTOR ACADÉMICO NACIONAL

JAVIER ABRAHAM SALGADO LEZAMA

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANA NACIONAL DE POSTGRADO

ANA DEL CARMEN RETTALLY VARGAS

DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN NORMA ISO 27001:2022 EN EMPRESA SAN SERVICES S. de R. L.

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE

MÁSTER EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ASESOR METODOLÓGICO

JORGE RAÚL MARADIAGA CHIRINOS

MIEMBROS DE LA TERNA:

MSc. KEVIN FÚNEZ
MSc. RIGOBERTO RODRÍGUEZ
PhD. FREDIS MEDINA

FACULTAD DE POSTGRADO

DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN NORMA ISO 27001:2022 EN EMPRESA SAN SERVICES S. de R. L.

ALEXANDER ENOC BONO RIVERA
LUIS ANTONIO TINOCO RIOS

Resumen

San Services S. de R.L. brinda diferentes servicios que manejan información sensible de sus clientes, proveedores y colaboradores, la cual es susceptible a amenazas como ciberataques, interrupciones de servicios, vulnerabilidades, entre otras. El siguiente trabajo tiene como propósito presentar un análisis y proponer un diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el estándar internacional ISO 27001:2022 para salvaguardar la integridad, confidencialidad y disponibilidad de la información de San Services S. de R.L. Los resultados de la investigación se obtuvieron mediante fuentes de información como encuestas y entrevistas a personas claves tomados del área de TI para realizar un análisis de brechas y determinar el estado actual de la empresa en cuanto a la seguridad de la información con respecto a los requisitos de la norma ISO 27001 así como la identificación, análisis y evaluación de las amenazas utilizando herramientas como matriz de riegos y uso de metodología MAGERIT y se elaboró el documento que determina el alcance y límites del SGSI dentro de San Services S. de R.L. La investigación se desarrolló bajo una metodología de investigación con un enfoque mixto y con un alcance exploratorio descriptivo. San Services presentó al final un nivel de cumplimiento aceptable frente a la implementación de un SGSI y también se definieron los riegos clave con su respectiva serie de acciones para contrarrestarlos. Finalmente se desarrolló un estudio de aplicabilidad con un plan de implementación del SGSI mediante el seguimiento de varias fases.

Palabras claves: (Control de acceso a datos, Ciberseguridad, ISO 27001, Riesgos, Seguridad de la Información)

GRADUATE SCHOOL

DESIGN OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) BASED ON ISO 27001:2022 STANDARD AT SAN SERVICES S. de R. L.

ALEXANDER ENOC BONO RIVERA
LUIS ANTONIO TINOCO RIOS

Abstract

San Services S. de R.L. offers different services that deal with sensible information from its customers, suppliers and collaborators, and it's susceptible to threats like cyber-attacks, denial of service, vulnerabilities, among other. The following research has as its purpose to present an analysis and propose a design of an Information Security Management System (ISMS) based on the ISO 27001:2022 standard to safeguard the integrity, confidentiality and availability of the information of San Services S. de R.L. The results of this research were obtained through information sources like surveys and interviews done to key people inside the IT area in order to do a breach analysis and determine the current status of the company in regards of information security with regard of the requisites of the ISO 27001 as well as the identification, analysis and assessment of the threat making use of tools like risk matrix and the MAGERIT methodology and a document was created that determines the range and limits of the ISMS inside San Services S. de R.L. The research was developed following a mixed focus with a descriptive explorative range. San Services showcased a fulfillment level that was acceptable against the implementation of an ISMS and the key threats were identified along with their corresponding counter actions. Finally, an applicability study was done with an implementation plan of the ISMS divided into several phases.

Keywords: (Data access control, Cybersecurity, Information Security, ISO 27001, Risks)

DEDICATORIA

Dedico este trabajo primeramente a Dios por darme las fuerzas necesarias para lograr culminar este nivel educativo. A mis papás y hermanos por todo el apoyo brindado durante todo este proceso académico. A mi amada hija Camila Sofía quien fue mi motivación principal para cada esfuerzo en la realización de este trabajo, para que todas mis metas alcanzadas le sean como huellas a seguir.

Atte. Luis Antonio Tinoco Rios

Dedico este trabajo a Jehová por proveer todos los recursos que se necesitaron para lograr cumplir con los deberes y llegar al final de todo este recorrido académico. A mis padres por el apoyo brindado durante todo este proceso académico, así como a todas aquellas personas con las que recorrí este camino y con quienes fue un gusto poder haber trabajado para llegar a la meta.

Atte. Alexander Enoc Bono Rivera

AGRADECIMIENTO

Quiero agradecer a la institución donde laboro Banco Promerica por darme la oportunidad de poder cursar esta maestría. A la Lic. Tania Molina por creer en mí y darme siempre todo su apoyo en cada etapa de este proceso. A nuestro asesor de tesis Jorge Maradiaga por toda su ayuda y experiencia brindada para la realización de esta tesis. A mi amada esposa Carolina Muñoz por no soltarme de la mano en todo este camino, este trabajo también es su logro.

Atte. Luis Antonio Tinoco Rios

Agradezco a Jehová por habernos permitido llegar al final de este proceso educativo, permitiéndonos conseguir todo lo que ocupábamos para lograr finalizar con éxito. A mis padres por el apoyo y motivación que me brindan para empeñarme en mis estudios. A nuestro asesor de tesis, Jorge Maradiaga por toda la ayuda y experiencia brindada para la realización de esta tesis y a mis amistades que estuvieron allí brindando su granito de arena para la realización de esta tesis.

Atte. Alexander Enoc Bono Rivera

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I – PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCIÓN

Desde sus inicios, la humanidad siempre ha valorado mucho el acceso a la información fidedigna, la cual presta una utilidad al que la posee. Muchas de las grandes guerras se ganaron gracias a información recabada acerca de los movimientos enemigos, lo que permitió tomar acciones que permitieran vencer al oponente con el menor esfuerzo. Esta misma filosofía ha sido aplicada por las organizaciones modernas, las cuales logran conseguir información mediante diversas fuentes, y las almacenan para hacer uso de esta con el objetivo de mejorar sus servicios o procesos internos. Si bien, hoy en día esta información no es necesariamente utilizada para ganar una guerra, muchas empresas enfrentan nuevos retos modernos de los cuales deben protegerse. Algunos de estos retos son el espionaje industrial, leyes y regulaciones gubernamentales, ataques cibernéticos, errores humanos, fallas de infraestructura e incluso, desastres naturales catastróficos.

Debido a todas estas amenazas, las organizaciones modernas de todos los ámbitos se ven en la necesidad de crear reglas y políticas que permitan gestionar sus activos digitales, sin que esto entorpezca sus operaciones. Sin embargo, muchas lo hacen sin apoyarse en un estándar internacional, lo cual provoca que ciertas implementaciones no sean tan robustas o no estén lo suficientemente modernizadas para hacer frente a las ultimas amenazas que surgen. Sumado a esto, muchas organizaciones no consideran que puedan ser blanco de un ataque, ya que consideran que los datos que ellos poseen no son críticos o que no son una organización de alto perfil que pueda ser llamativa para los ciber-delincuentes.

La presente investigación busca presentar un diseño de sistema de gestión de seguridad de la información bajo los estándares de la norma ISO 27001:2022. Este diseño busca fortalecer la gestión y el manejo de la información dentro de la empresa San Services S. de R.L., con el objetivo de asegurar que se sigan estándares modernos que permitan proteger la información de la organización y evitar que ocurran incidentes que puedan provocar fuga o daños.

En el capítulo I, se explican los antecedentes del problema, se define cual es la dificultad dentro de la organización, se define la pregunta general y las preguntas específicas, así como el objetivo general y objetivos específicos. Asimismo, se plantea la justificación del porqué de esta investigación.

En el capítulo II, se plantean los conceptos básicos relacionados con esta investigación, las herramientas que se utilizaran, el marco legal existente bajo el que la organización trabaja, las metodologías que son la base para esta investigación como el entorno bajo el que la organización opera.

En el capítulo III, se explica el enfoque, alcance, el diseño de la investigación, así como su población, muestra y la técnica de muestreo utilizada. Además de esto, se explican las técnicas, instrumentos, procedimientos, las fuentes de información primaria y secundarias, así como el plan de análisis de datos y la matriz de congruencia utilizada en esta investigación.

En el capítulo IV, se exponen los resultados de la investigación y el análisis de estos. Se muestran los riesgos identificados dentro de la organización, así como la recolección de información de esta que permita determinar el nivel de cumplimiento de los requisitos administrativos y de los controles técnicos que exige la norma ISO 27001:2022.

En el capítulo V, se exponen las conclusiones y recomendaciones alcanzadas luego de la realización del levantamiento de datos dentro de la organización y el análisis de estos.

En el capítulo VI, se expone la propuesta final que se alcanzó mediante la realización de este trabajo de investigación.

1.2 ANTECEDENTES DEL PROBLEMA

Las preocupaciones de los seres humanos por la seguridad no empezaron en las décadas recientes. Desde que empezó a existir comunicación entre un pueblo con otro, siempre ha existido una preocupación por garantizar que el mensaje que se recibía o se enviaba era legítimo. En ese entonces, los reyes o líderes enviaban sus mensajes junto con algún objeto de valor, lo cual diera legitimidad al mismo, con el fin de que nadie pudiera cambiarlo o interceptarlo con facilidad. Con el paso del tiempo, dicha validación cambio al uso de un sello que estaba en el anillo real que el rey usaba en su mano derecha, lo cual daba a los edictos y mensajes un peso sumamente importante, el cual implicaba la muerte para todo aquel quien no lo cumpliera.

Y esto se mantuvo por mucho tiempo de esta forma, con ciertas variantes de la misma idea desarrollada en diversos reinos e imperios a través de la historia, hasta hace unos siglos. En 1684, se da lo que fue uno de los primeros incidentes de interceptación de mensajes entre naciones, lo cual abrió la puerta a una nueva forma de descubrir los planes de aliados y enemigos por igual. En

enero de 1684, la república francesa y la republica holandesa estaban al borde de la guerra. Los franceses lanzaron un ataque a ciertos territorios de la república holandesa. Esto provoco que el comandante de la armada, Stadholder William III, empezara a solicitar apoyo económico para lograr levantarse en armas contra Francia y defender sus territorios. Mientras tanto, el embajador de Francia de la época, Count D'Avaux, se reunió con la alcaldía de Ámsterdam, para evitar que estos proveyeran ayuda económica al comandante. Estas negociaciones eran una muestra clara de interferencia en los asuntos internos de la república, por lo que Stadholder decidió evidenciar las acciones del conde mediante espías que siguieron los mensajeros del Conde en un momento en donde seguramente estaban moviendo mensajes de las negociaciones entre ambas partes. Para evitar un problema de inmunidades políticas, el mensajero del Conde fue interceptado luego de que cruzara la frontera. La carta cayó en manos del Stadholder, y a pesar de que esta estaba codificada, logro demostrar la traición y descubrió los beneficios de interceptar correos, práctica que llevo a cabo durante su reinado en Inglaterra muchos años más tarde. Esta práctica se esparciría a muchas naciones durante el siglo XVIII, en donde se volvió común el uso de descifradores, lingüistas y mercenarios para interceptar y descifrar estos mensajes. De estos elementos tan básicos, se puede extraer el concepto clave de lo que es seguridad de la información:

> La protección de la información y el sistema que lo contiene en contra de accesos no autorizados, modificaciones ya sea durante el almacenamiento, procesamiento o tránsito, y en contra de denegación del servicio a los usuarios autorizados. La seguridad de la información incluye todas las medidas necesarias para detectar, documentar y defenderse de esas amenazas (Leeuw, 2007)

Con el paso del tiempo, a pesar de que el objetivo ha sido el mismo, las acciones tomadas para llevarlo a cabo han cambiado. Durante las dos guerras mundiales que sucedieron en el siglo pasado, los mensajes encriptados jugaron un papel importante en la comunicación de movimientos militares, y cada nación se esforzaba en interceptar mensajes enemigos para descifrarlos, y en como fortalecer su propia encriptación para protegerse en caso de que interceptaran sus mensajes. Esto llevo a muchas naciones a crear sus primeras agencias de inteligencia, las cuales luego de la guerra, se encontraron con los primeros problemas de protección de la información, esta vez dentro de sus propias filas. Surgió la necesidad de establecer una forma de trabajo con políticas y reglas que permitieran manejar proyectos con información sensible dentro de las agencias, sin que esta información pasara por todas las manos de los miembros de esta. Estos primeros pasos empezaron

en los años 60. Se hicieron estudios con los cuales se dieron recomendaciones acerca de cómo encriptar y manejar la información clasificada, así como un modelo de seguridad que clasificaba la información de acuerdo con su nivel de secretividad. Este modelo de seguridad (conocido como Bell-LaPadula) funcionó durante el tiempo en que todos los archivos eran manejados de forma física, sin ningún almacenamiento digital que permitiera enviarlos a través de una red de datos. Una de las debilidades de la época con este modelo, era que no tomaba en cuenta casos en donde algún activo tuviera múltiples niveles de requisitos de seguridad, como podría ser el caso de una base de datos relacional, ni tampoco tomaba en cuenta políticas de seguridad comercial. (Leeuw, 2007)

Al mismo tiempo que empezaban a surgir las primeras redes de comunicaciones por Internet para uso militar, en paralelo, los primeros pasos para el manejo y validación de la integridad de la información se estaban dando. Con la llegada de la IBM 360 en 1964, se da un gran paso en la forma de manejar información de transacciones bancarias. La información paso de manejarse en tarjetas perforadas y cintas magnéticas, a memoria digital, la cual podría ser auditada y validada mediante software escrito para la IBM 360. El almacenamiento en disco y la entrada de datos por internet permitieron el acceso a los datos desde cualquier oficina, lo cual obligo a los encargados de IT y sus auditores a definir procedimientos que permitieran validar el formato de los datos y la entrada de estos.

Gracias al auge del internet y las telecomunicaciones, el flujo de información y generación de datos ha aumentado en gran manera en los últimos años. Hoy en día, las personas utilizan las redes sociales para compartir intereses, mensajes, campañas o expresar sus opiniones, compartiendo con otras personas, grupos u organizaciones. Esta nueva manera de compartir datos y de comunicarse ha transformado la forma de operar no solo de las personas y las organizaciones, sino también de gobiernos y organismos internacionales, los cuales ahora pueden involucrarse más fácilmente en eventos de índole global.

Pero esta revolución trajo consigo nuevos riesgos en todas las naciones alrededor del mundo. En naciones como Nigeria (Robitiki, Ayo, 2015), se han hecho estudios para identificar aquellas infraestructuras de suma importancia nacional, entre las cuales se mencionó sistemas de comunicaciones, manufactura, sistemas bancarios, sistemas de controles de seguridad en entidades gubernamentales, sistemas con importancia militar, entre otros. Tanto naciones como

organizaciones dedicadas a crimines informáticos son parte de los actores que pueden provocar daños, ya sea buscando un fin económico o un fin político. En ciertas naciones, se han introducido leyes con el objetivo de garantizar la seguridad nacional de sus infraestructuras digitales, crear planes de recuperación en caso de incidentes y legislar castigos contra aquellos que busquen atacar de manera digital a la nación y sus ciudadanos. Dichas legislaciones se empezaron a discutir a inicios del siglo XXI, luego del auge de las comunicaciones por internet, y luego de que se suscitaran ataques de virus informáticos a nivel global.

Debido a este aceleramiento en la forma de procesar, gestionar y manejar datos, las organizaciones que tienen varias décadas de existencia se vieron obligados a cambiar sus procesos de manejo de la información, dejando atrás los viejos métodos físicos (como libros y archiveros) para pasar a almacenar toda su información de manera digital. Esto trajo consigo tanto beneficios, como retos y una nueva serie de amenazas a las cuales se enfrentarían. Dichas amenazas van desde ataques de malware, a ataques de ransomware o phishing, todas con el objetivo de robar la preciosa información de la organización. Sumado a esto, el desarrollo de la Internet y su alcance dentro de un mundo globalizado significa que los ataques y riesgos son en una escala global, y no solamente regional o local como pudiera haber ocurrido en el pasado.

Dado a que las legislaciones para castigar estos crímenes y a los intereses compartidos de salvaguardar la información entre las entidades gubernamentales y el sector privado, surgen de esta forma diversos marcos de trabajo orientados a dar lineamientos básicos sobre cómo hacer frente a estas amenazas de seguridad, con el objetivo principal de salvaguardar la información. El NIST (National Institute of Standards and Technology) surgió como una entidad gubernamental del departamento de comercio de los Estados Unidos de América que tiene como objetivo el definir estándares para su uso dentro del territorio estadounidense, a fin de evitar que organizaciones clave queden expuestas a ataques por enemigos extranjeros. La mayoría de sus publicaciones están disponibles sin costo alguno y proveen un detallado proceso sobre los elementos y primeros pasos que una organización puede tomar para escudarse ante las amenazas. Sus informes proveen liderazgo en cuanto a los estándares, pruebas, métodos y datos de referencia que puedan ser de utilidad a la población en general para hacer un uso efectivo, poco costoso y con privacidad de cualquier información, tanto en sistemas federales como externos. (NIST, 2017)

Tomando todo esto en cuenta, surge dentro de las organizaciones la necesidad de

implementar un Sistema de Gestión de Seguridad de la Información que les permita gestionar todos estos riesgos de una forma que permita el acceso rápido a la información, pero sin que esta se vea comprometida, o alterada de alguna forma, y siguiendo lineamientos modernos que puedan ser actualizados con el paso del tiempo para que los procesos no queden obsoletos.

1.3 DEFINICIÓN DEL PROBLEMA

La organización San Services gestiona todos los datos recabados de los clientes que visitan los resorts y sitios webs de los resorts inclusivos en el Caribe de Unique Vacations Ltd. Dicha información se encuentra repartida entre diversas bases de datos, distribuida a través de diferentes nodos de servidores que datan de hace más de una década. Esta información va desde datos superfluos como preferencias de comida hasta información privada de datos de contacto de los clientes, datos de transacciones de pagos e incluso información confidencial de los huéspedes y sus visitas a los distintos resorts. Esto también incluye información que aparece en los diversos sitios webs, los cuales sirven para presentar a los clientes los diversos resorts y sus atractivos.

Con tanta información distribuida entre diversos lugares y plataformas, es difícil de determinar si dicha información está a salvo de cualquier ataque, si está siendo manejada de la mejor manera posible, y si esta tiene pocas probabilidades de filtrarse o sufrir modificaciones. Si bien, no ha habido recientemente incidentes con la gestión de datos de lado de TI, esto no significa que no se puedan presentar, y lo ideal sería evaluar en qué situación de riesgo están, para lograr tomar las medidas de mitigación necesarias con el fin de reducir los niveles de riesgo y mejorar la seguridad de la información que poseen.

1.4 PREGUNTAS DE INVESTIGACIÓN

1.4.1 PREGUNTA GENERAL

¿Cómo se puede diseñar un Sistema de Gestión de Seguridad de la Información eficaz y conforme con la norma ISO 27001:2022 en la empresa San Services S. de R.L.?

1.4.2 PREGUNTAS ESPECÍFICAS

¿Cuál es la situación actual de San Services S. de R.L. en cuanto a la infraestructura de TI y sus sistemas de manejo de datos ante posibles vulnerabilidades y puntos de riesgos?

¿Qué riesgos de seguridad de la información son más críticos para San Services S. de R. L., y cómo deberían ser abordados en el diseño del SGSI?

¿Cuáles son los principales riesgos asociados a los activos críticos de San Services S. de R. L., y qué salvaguardas recomienda fortalecer la metodología MAGERIT para mitigar estos riesgos?

¿Cómo se puede elaborar un documento que defina claramente el alcance del SGSI, delimitando sus objetivos para asegurar la claridad y el enfoque en la gestión de la seguridad de la información en San Services S. de R. L.?

1.5 OBJETIVOS DEL PROYECTO

1.5.1 OBJETIVO GENERAL

Proponer el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para salvaguardar la integridad, confidencialidad y disponibilidad de la información de los procesos más críticos de San Services S. de R.L. basados en la norma ISO 27001:2022.

1.5.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual del manejo de la seguridad de la información en la empresa según norma ISO 27001:2022.
- Realizar un análisis de riesgos de seguridad de la información específicos para San Services S. de R. L. y desarrollar estrategias para mitigar los riesgos identificados.
- Evaluar los principales riesgos asociados a los activos críticos de San Services S. de R. L. mediante la metodología MAGERIT, tomando en cuenta la recomendación de salvaguardas para mitigar dichos riesgos.
- Elaborar un documento con el alcance del SGSI que delimite los objetivos de este y permita claridad y enfoque en la gestión de la seguridad de la información dentro de San Services S. de R. L.

1.6 JUSTIFICACIÓN

En la era digital actual es muy necesario contar con mecanismos de ciberseguridad que ayuden salvaguardar el activo más valioso para cualquier organización como lo es la información, un SGSI que esté basado en la norma internacional ISO 27001:2022 es un elemento fundamental que permite poder implementar procedimientos y controles de seguridad para minimizar los riesgos de la seguridad de la información ante una infinidad de amenazas que atentan contra la

continuidad del negocio, además de eso, se robustece la reputación de la organización y la confianza del cliente así como de las partes interesadas, haciendo la organización más rentable y ofreciendo una ventaja competitiva en el mercado. Así mismo se fortalece el cumplimiento normativo y regulatorio relacionado con la seguridad de la información ya que la norma ISO 27001:2022 es muy reconocida internacionalmente como un estándar de referencia de la seguridad de la información.

La empresa San Services S. de R.L. en la naturaleza de su negocio brinda diferentes servicios que manejan información confidencial y sensible de sus clientes, proveedores y colaboradores, esa información es susceptible a perdida ante amenazas como ciberataques, interrupciones de servicios, vulnerabilidades en los sistemas y plataformas de trabajo, entre otras. Por lo cual el identificar, evaluar y tratar riegos de la seguridad de la información de manera sistemática por medio del diseño inicial de un SGSI permitirá a la organización poder proteger sus datos de manera adecuada permitiendo la toma de decisiones de manera oportuna.

CAPÍTULO II – MARCO TEÓRICO

2.1 MACROENTORNO

2.1.1 FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS

Según Ladino et al. (2018) la norma ISO 27001 como eje central de la guía de un SGSI es certificable, es decir las empresas que buscan contrarrestar las amenazas que puedan comprometer su información, pueden emprender a través de planes de acción que conlleven lineamientos oficiales, responsables y toda la documentación que garantice que el SGSI sea aplicado, estas pueden optar por un certificado internacional ISO 27001 a través de una entidad certificadora acreditada la cual se realiza en un proceso que conlleva varias fases. La certificación no solo ayuda a las empresas a mejorar la seguridad de su información, sino que también cumplen con una normativa legal relacionado con la protección de los datos y la seguridad de la información traduciéndose en un compromiso serio por parte de las empresas hacia los clientes, socios, empleados y proveedores, lo cual genera confianza y conduce al aumento de la rentabilidad.

Para (Villamizar, 2023) como parte de las recomendaciones al momento del diseño del SGSI lo primero y más transcendental es que se debe de contar con el compromiso de la alta dirección de la empresa, se debe de hacerles saber cuáles son las consecuencias económicas de no contar con un SGSI, seguidamente realizar un estudio de identificación de los activos más críticos de la empresa que tienen relación con la información, sobre todo reconocer que cada empresa tiene un ambiente de control, apetito de riesgo y riesgos de seguridad de la información particulares. Así como fomentar una cultura de seguridad, definición y tratamiento de los riesgos que permita la mejora y sostenibilidad de un SGSI.

Como afirman las últimas estadísticas en la International Organization for Standarization (ISO) el top 10 con la mayor cantidad de certificados ISO 27001 está liderado por los países asiáticos China y Japón seguido por el Reino Unido.

Tabla 1. Top 10 países con certificaciones ISO 27001

Ranking	País	Certificados
1	China	26301
2	Japón	6987
3	Reino Unido	6084

4	India	2969
5	Italia	2424
6	Estados Unidos	1980
7	Países Bajos	1741
8	Alemania	1582
9	España	1561
10	Israel	1467

Fuente: (Organización Internacional de Normalización, 2022)

2.1.2 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES A NIVEL MUNDIAL

El análisis de amenazas y vulnerabilidades a nivel mundial revela una serie de desafíos interconectados que afectan a diversas áreas y regiones del planeta. Estos incluyen riesgos, por mencionar algunos, como la ciberseguridad, el cambio climático, pandemias, seguridad alimentaria, desigualdad social, seguridad energética, desastres naturales, conflictos internacionales y terrorismo, así como el impacto de tecnologías emergentes. Estas amenazas requieren respuestas globales y coordinadas para mitigar sus efectos y promover la seguridad y estabilidad a escala mundial.

Según un informe de (ECIIA, 2021) el cual presenta los temas clave y los riesgos más importantes para los auditores internos de Europa en 2022, destaca la importancia de la ciberseguridad como un riesgo crítico debido al aumento de amenazas digitales y al incremento del trabajo remoto. Otros temas incluyen la gestión de riesgos relacionados con la sostenibilidad y el cambio climático, así como los desafíos derivados de la transformación digital y la adopción de nuevas tecnologías. También se abordan riesgos emergentes como la integridad de los datos, la privacidad y la ética en el uso de la inteligencia artificial y la automatización. El informe subraya la necesidad de que los auditores internos estén preparados para abordar estos riesgos y proporcionar una evaluación eficaz y proactiva de los controles y procesos dentro de las organizaciones.

Gráfico 1. Ranking de riesgos asociados a las organizaciones.
Fuente: (ECIIA, 2021).

Siendo el riesgo de ciberseguridad y protección de los datos el más prominente, según un informe de (Harán, 2023) se revela que las empresas en América Latina en 2023 enfrentan una creciente amenaza cibernética, con un aumento significativo en ataques dirigidos y ataques de ransomware. Los ciberdelincuentes están aprovechando vulnerabilidades en sistemas obsoletos y técnicas de ingeniería social para comprometer redes corporativas. Además, se observa un incremento en la sofisticación de los ataques, incluyendo la utilización de herramientas de hacking avanzadas y el despliegue de campañas de phishing cada vez más dirigidas. también aborda la importancia de la adopción de medidas proactivas de seguridad, como la implementación de soluciones de seguridad avanzadas y la mejora de la gestión de parches y actualizaciones de software. Se destaca la necesidad de contar con políticas de seguridad robustas y estrategias de respuesta a incidentes bien definidas para mitigar los riesgos y minimizar el impacto de posibles ataques.

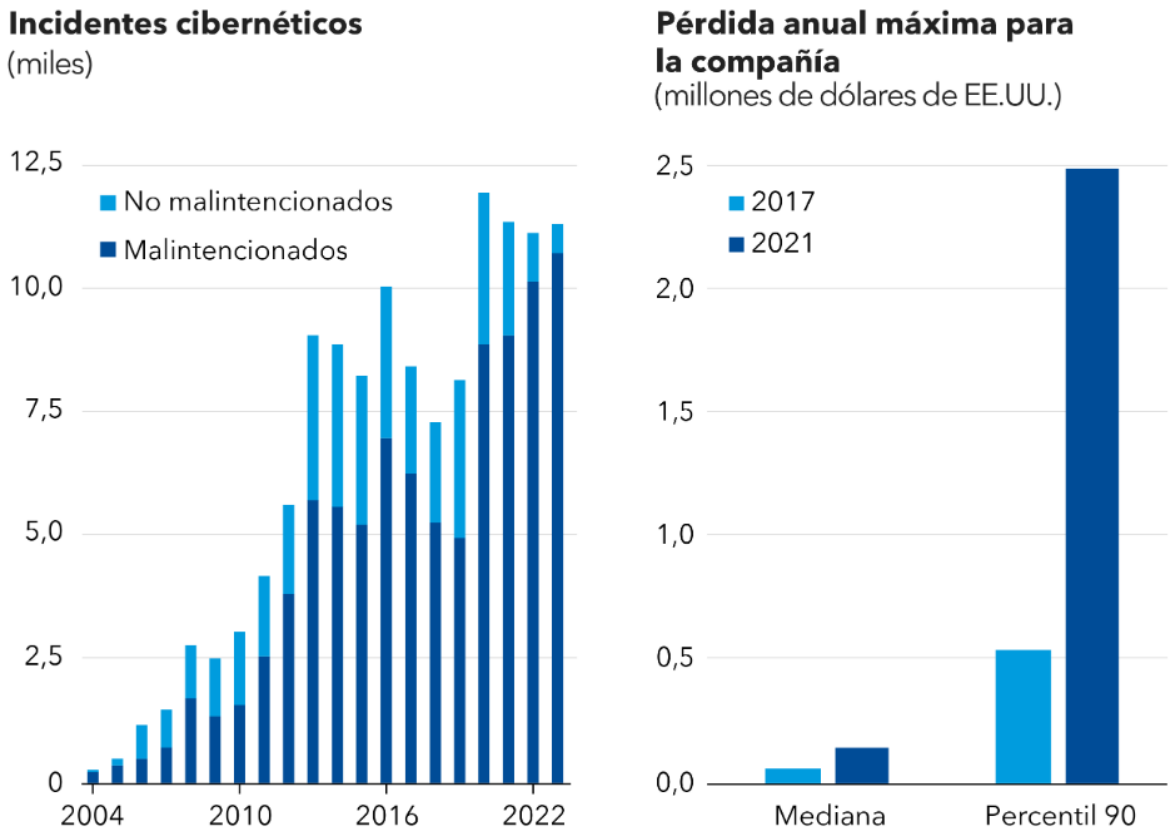

Gráfico 2. Crecimiento de incidentes cibernéticos clasificados según criterio y pérdida anual máximas para las compañías en un año.
Fuente: (Natalucci et al., 2024).

Como se puede observar en la Gráfica 2, en un informe elaborado por el Fondo Monetario Internacional (FMI) realizado en abril del 2024, demuestra que los ataques cibernéticos van en aumento en cierta parte por el ascenso de la digitalización tomando como punto de inflexión la pandemia de 2020 en el cual los ciberataques se multiplicaron por más de dos, esto obviamente repercute en las pérdidas que acarrean los problemas de financiamiento en las empresas sin mencionar las perdidas indirectas como el perjuicio reputacional y los elevados costos destinados para la mejora de la seguridad.

2.1.3 APLICACIÓN DE SGSI EN EL SECTOR EMPRESARIAL BASADO EN ISO 27001

Rodríguez (2017), llevo a cabo una investigación sobre el diseño de un SGSI basado en ISO 27001 para una empresa de laboratorios servicios farmacéuticos, en la ciudad de Bogotá Colombia. Por la naturaleza de sus servicios, la empresa maneja información confidencial, la cual

necesitaba de un nivel adecuado de seguridad y el establecimiento de procedimientos definidos que garanticen la confidencialidad. Certificados de análisis microbiológicos, procedimientos críticos, formulas maestras y certificados de análisis para la preparación de medicamento son algunas de los datos más críticos que necesitan máxima seguridad. Para el desarrollo del diseño del SGSI, se apoyaron en la metodología MAGERIT y para el tratamiento de los riesgos tomaron como herramienta EAR/PILAR, la cual es parte de la metodología anteriormente mencionada en su tercera versión. Seguidamente, como parte del proceso que dicta la norma, es la identificación y valoración de los activos de la empresa, la identificación de los riesgos y sus respectivas salvaguardas, creación de políticas, terminando con los resultados y discusiones de las actividades con los diferentes métodos como entrevistas, documentación física y electrónica y asesorías.

Solano (2020), en su trabajo propuso plantear un prototipo de la seguridad de la información en base a la norma ISO 27001 en una empresa que brinda servicios tercerizados en Heredia, Costa Rica, en la cual busca mejorar los niveles de seguridad de la información, ya que la empresa no cuenta con políticas, procedimientos o controles que minimicen los riesgos. El estudio que se llevó a cabo fue un enfoque cualitativo con tipo de investigación exploratorio. El SGSI fue diseñado por la metodología PHVA o Deming, así como el desarrollo de las políticas y procedimientos. El instrumento que se llevó a cabo como una de las fuentes de información fueron las encuestas.

Cortes Malagón, J. & Pulido Espinosa J. (2023), finalizaron un informe sobre el diseño de un SGSI puntualmente sobre procesos críticos de una empresa dedicada al desarrollo de proyectos y soluciones integrales para los sectores de hidrocarburos, energía e infraestructura con sede en Venezuela. El SGSI fue diseñado tomando como referencia la norma ISO 27001 en su versión más actual 2022, y su origen surge a raíz de la falta de controles que permitan una correcta gestión de los riesgos, políticas y estrategias de seguridad de la información. Se obtuvieron resultados de la evaluación en base a los controles del anexo (A) del ISO 27001 y se concluye que la empresa cumple únicamente con el 36% lo cual evidencia la necesidad de robustecer el SGSI.

2.1.4 ANÁLISIS DE RIESGOS EN UN SGSI UTILIZANDO METODOLOGÍAS COMPLEMENTARIAS INTERNACIONALES

La norma ISO 27001 establece un proceso sistemático para identificar, analizar y evaluar los riesgos de seguridad de la información. Este proceso se basa en la identificación de activos de

información, la evaluación de amenazas y vulnerabilidades, así como la determinación del impacto potencial de los riesgos. Sin embargo, ISO 27001 no proporciona una guía detallada para la cuantificación de riesgos o la priorización de medidas de control. Es aquí donde las metodologías complementarias pueden ser útiles. Según Alemán Novoa, H. & Rodríguez Barrera, C. (2015) en el campo de la seguridad informática, las metodologías de análisis de riesgos son una disciplina fundamental que se desarrolla a través de los Sistemas de Gestión de Seguridad Informática (SGSI) en las organizaciones. Estas metodologías llevan a cabo evaluaciones exhaustivas de vulnerabilidades utilizando una variedad de modelos y procesos, con el objetivo de proponer formas más seguras de proteger la información y los recursos de TI. Algunos de los propósitos de estas metodologías incluyen la planificación para reducir riesgos, la prevención de incidentes, la identificación y visualización de debilidades en los sistemas, y proporcionar apoyo en la toma de decisiones para la seguridad de la información.

En el ámbito de la seguridad de la información, se destacan varias metodologías de análisis de riesgos, como Octave, MAGERIT, Mehari, NIST SP 800:30, Coras, Cramm y Ebios.

MAGERIT, por ejemplo, ofrece un método para cuantificar el riesgo utilizando un enfoque basado en factores como la probabilidad de ocurrencia del evento y la severidad del impacto. OCTAVE, por otro lado, proporciona un marco para la evaluación de riesgos centrado en los activos de información y los procesos de negocio. MEHARI, finalmente, ofrece una metodología para la identificación y análisis de amenazas.

Al combinar ISO 27001 con estas metodologías complementarias, las organizaciones pueden obtener una comprensión más completa de sus riesgos de seguridad de la información y tomar decisiones más informadas sobre la implementación de controles y medidas de seguridad adecuadas.

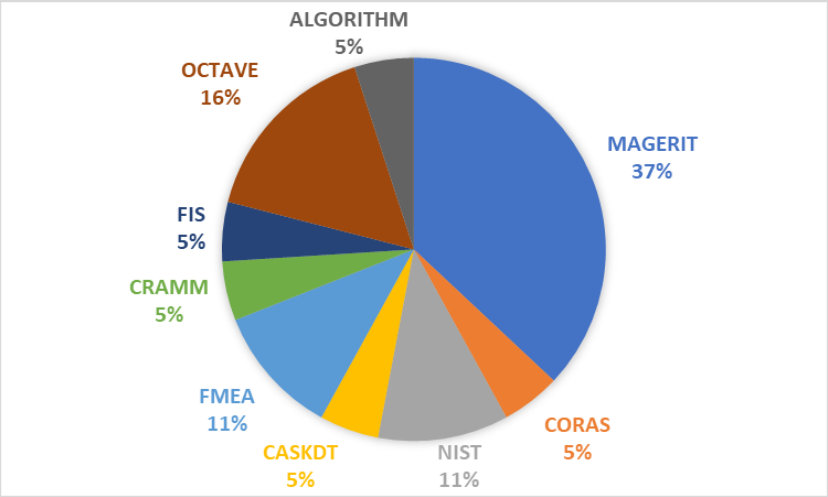

Gráfico 3. Principales metodologías para el análisis de riego informático.
Fuente: (López Rimari, R. P.,2020).

López Rimari, R. P. (2020) realizó una investigación en la cual determina cuales son las metodologías para el análisis de riesgos que son más usadas en base a una búsqueda en librerías digitales indexadas como IEE Xplore, Science Direct, Springer Link y Google Scholar, teniendo como criterios de inclusión todos los artículos de investigación que contengan estudios, análisis o metodologías de riesgo de seguridad de la información, incluyendo revistas científicas y conferencias entre el año 2014 y 2020. La tabulación de 1,269 resultados obtenidos se muestra en la Gráfica 3, en la cual se observa claramente la metodología MAGERIT con el 37% como la más usada.

2.2 MICROENTORNO

2.2.1 ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS HONDUREÑAS

En Honduras, la ISO 27001 ha empezado a ganar peso en la última década, sobre todo en las empresas u organizaciones hondureñas que prestan servicios de índole digital a sus clientes o que hacen uso de sistemas digitales para el almacenamiento de la información de sus colaboradores y clientes. Algunas de estas empresas u organizaciones se han certificado con éxito en este ámbito, aplicando la norma con el objetivo de proteger los activos de información que manejan en sus procesos internos, mientras que otras, han decidido desarrollar su propio sistema de gestión de seguridad de los datos de una forma que cumpla con las amenazas más inminentes que puedan enfrentar, sin que esto signifique que realmente cubran todas las posibles amenazas o que se

apeguen a algún estándar en específico.

Dentro de algunas de las empresas que podemos mencionar que se han certificado con el ISO 27001, en sus diferentes versiones, encontramos:

- Instituto de Previsión Militar: El IPM (Instituto de Previsión Militar) se certificó a través de ICONTEC con el certificado ISO 27001:2013 en 2022. El alcance del certificado fue para Seguridad de la información con el fin de brindar servicios de seguridad social a través de las plataformas tecnológicas a cada uno de sus afiliados. (Instituto de Previcion Militar, 2022)
- Confianza SA-FGR: Confianza – Sociedad Administradora de Fondos de Garantía Recíproca obtuvo su certificado en ISO 27001:2013 en 2021, lo cual les permite cumplir legalmente con la confidencialidad, integridad y disponibilidad continuada de la información. Se certificaron a través de ICONTEC, y la razón por la cual se certificaron, es de acuerdo con su gerente general Francisco Fortín, debido a que muchos de sus procesos corren exclusivamente por medios electrónicos, por lo que es necesario establecer mecanismos de seguridad que permitan protegerlo. (Confianza SA-FGR, 2021)
- SUMITEC: La empresa SUMITEC, quien brinda soporte de personal técnico, productos, repuestos y suministros a diversos clientes a nivel nacional, se certificó en diciembre de 2018 con la ISO 27001, para sus servicios de soporte y gestión tecnológica, así como para mejorar sus procesos de seguridad de la información. (Costa, LinkedIn, 2019) (Costa, 2019)
- IMPACT MOBILE: La empresa IMPACT MOBILE se certificó con ISO 27001:2013 con la ayuda de Intedya (International Dynamic Advisors), consiguiendo sus certificados a través de la entidad certificadora STAREGISTER. Como proveedor de plataformas de Mobile Marketing, y con el fin de asegurar la confidencialidad e integridad de los datos y de la información, IMPACT MOBILE alcanzo la certificación de Sistemas de Gestión de la Seguridad de la Información ISO 27001:2013. (Intedya, 2024)

Estas 4 empresas, son un pequeño ejemplo reciente de organizaciones que están empezando a tomar conciencia de las utilidades que les puede brindar la ISO 27001, así como su aplicabilidad para cada uno de los servicios que proveen a sus clientes. Existen otras empresas a nivel nacional

que tienen desarrollado un sistema de gestión de seguridad de la información, pero al no estar certificado, es difícil determinar si dicho sistema esta modernizado para enfrentar las amenazas actuales o si dicho sistema está realmente diseñado de la manera correcta, permitiéndole ser flexible ante las necesidades futuras de la organización.

2.2.2 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES EN HONDURAS

En Honduras, si bien no estamos exentos de tener que hacer frente a las amenazas que enfrentan cada uno de los demás países a nivel mundial, hay algunas que prevalecen más que otras en nuestra nación. Los retos son muchos y las organizaciones deben de enfrentarse no solo a actores mal intencionados nacionales, sino también a los internacionales, quienes ven naciones como la nuestra como campo libre con blancos fáciles de atacar. Sumado a esto, la falta de un trabajo colaborativo entre el gobierno y la empresa privada para alcanzar objetivos en común, hacen que sea más difícil de alcanzar metas que sean para el bien común de la sociedad hondureña.

De acuerdo con un artículo publicado en la revista Innovare (Centeno, 2017), el gobierno de Honduras no posee una política nacional de seguridad cibernética, ni un equipo de respuesta a incidentes, por lo cual tiene una capacidad limitada para lograr abordar las amenazas de ciberseguridad existentes. Si bien se está al tanto de la existencia de dichas amenazas y se asiste a foros internacionales para lograr obtener la información necesaria para la planificación de planes estratégicos para la gestión de crisis e incorporar programas digitales en la Comisión Nacional de Telecomunicaciones (CONATEL) para manejar una agenda digital de estado. La implementación de normas internacionales con el fin de proteger los activos nacionales que involucren infraestructura digital de nivel crítico. Nuestra nación carece de un marco legislativo para la seguridad de las TIC, y la dirección nacional de información criminal de la Policía Nacional, quien es el ente responsable de investigar los delitos cibernéticos, carece de un laboratorio forense digital y de estadísticas nacionales de incidentes de delincuencia cibernética.

Han existido intentos de promulgar leyes respecto a la privacidad y protección de datos, pero muchas de estas leyes han quedado engavetadas, sin que haya interés político por retomarlas. La baja penetración de Internet en muchos sitios del país, más la inseguridad pública, la mala gestión de los servicios en línea que las entidades estatales proveen y el desconocimiento de las amenazas cibernéticas existentes también son otra piedra en el camino de muchas organizaciones y empresas que están tomando la vía digital para ofrecer muchos de sus servicios, como lo hacen

ahora muchos bancos y empresas de servicios a domicilio. El sector privado prácticamente está obligado a adoptar marcos de trabajo extranjeros que les permita evolucionar y estar a la vanguardia con respecto a las amenazas que pueden tener que enfrentar, mas no todos pueden financiarse los gastos relacionados a los costos de certificación y educación, los cuales son ofrecidos por diversas instituciones regionales y nacionales.

2.3 TEORÍAS DE SUSTENTO

2.3.1 LA CUARTA REVOLUCIÓN INDUSTRIAL.

En la era de la Cuarta Revolución Industrial, los Sistemas de Gestión de Seguridad de la Información (SGSI) deben evolucionar para enfrentar los nuevos desafíos de seguridad derivados de la digitalización y la interconectividad. Tal como lo asegura Moya (2023) La Cuarta Revolución Industrial ha transformado radicalmente la forma en que las organizaciones gestionan la ciberseguridad. En este nuevo entorno, la ciberseguridad no se considera solo una necesidad, sino un elemento fundamental para garantizar la sostenibilidad y la resiliencia en un mundo cada vez más digitalizado.

Bajo ese contexto Rodríguez Parra, C. F., (2010). señala que “La Seguridad de la Información es el proceso de proteger la información de la perdida, de la alteración no autorizada y de divulgación inapropiada.”

Los propósitos de la Seguridad de la Información son, por consiguiente, preservar la confidencialidad, integridad y disponibilidad de los datos. La confidencialidad se enfoca en mantener la información protegida contra el acceso no autorizado. La integridad garantiza que la información permanezca íntegra y sin alteraciones. Finalmente, la disponibilidad se refiere a asegurar que la información y los sistemas de comunicación estén accesibles para los usuarios de manera oportuna.

Además de los principios fundamentales de confidencialidad, integridad y disponibilidad, existen otros principios adicionales que guían el programa de seguridad de la información, centrados en la integridad y autenticidad de los datos.

Uno de estos principios es el "no repudio", que se refiere a la incapacidad de negar la recepción o envío de un mensaje o transacción. Implica que ninguna de las partes puede negar su participación en una comunicación. Por ejemplo, el uso de firmas digitales en correos electrónicos

garantiza que un remitente no pueda negar haber enviado un mensaje y que el destinatario no pueda afirmar que el mensaje recibido fue alterado.

El principio de "autenticidad" se relaciona con la verificación de la identidad de los usuarios y la confiabilidad de la fuente de la información. Asegura que los usuarios sean auténticos y que la información provenga de fuentes confiables, promoviendo la recepción de mensajes válidos y genuinos.

Finalmente, la "rendición de cuentas" se refiere a la capacidad de rastrear acciones hasta la organización o entidad responsable. Este principio es esencial para identificar y resolver fallas, detectar problemas y garantizar la responsabilidad en el uso de la información y los sistemas.

Figura 1. Los principios fundamentales y adiciones de la seguridad de la información.
Fuente: (Ordoñez, W., 19 de Julio de 2023).

La interconectividad y la dependencia de las tecnologías digitales han incrementado significativamente la superficie de ataque, exponiendo a las organizaciones a un panorama de amenazas cibernéticas más complejo y sofisticado., Para ello, es fundamental integrar tecnologías de vanguardia como la inteligencia artificial (IA), el Internet de las Cosas (IoT), la computación en la nube y blockchain. Estas herramientas permiten optimizar la protección de activos de información críticos, mejorar la eficiencia operativa y escalar las medidas de seguridad. Sin

embargo, también introducen nuevos retos, como la gestión de la seguridad de datos en entornos dinámicos y distribuidos.

Más allá de la integración tecnológica, un SGSI moderno debe centrarse en la implementación de estrategias proactivas de gestión de riesgos para hacer frente a las amenazas cibernéticas en constante evolución. Esto implica la adopción de análisis predictivo y técnicas de inteligencia artificial, permitiendo anticipar y mitigar riesgos potenciales antes de que se materialicen. La capacidad de adaptación y respuesta rápida se vuelve crítica en la Cuarta Revolución Industrial, donde las amenazas cibernéticas son cada vez más sofisticadas y dinámicas lo que hace más complejo la gestión de los riesgos.

2.3.2 GESTIÓN DE RIESGOS

La gestión de riesgos es el conjunto de elementos de control que permiten encausar los objetivos institucionales al identificar oportunidades para un mejor cumplimiento de su función, o aumentar la confianza y satisfacción de las partes interesadas (Guerrero et al.,2020)

La gestión de riesgos desempeña un papel fundamental en las organizaciones, ya que contribuye a la orientación hacia procesos efectivos, la optimización de recursos y la reducción de costos. Además, refleja una cultura organizacional centrada en establecer un sólido control interno.

En este contexto se determina que es prácticamente imposible que las organizaciones eviten todos los riesgos y que no siempre las repercusiones deben de ser malas, por lo cual es crucial evaluar el riesgo potencial junto con las oportunidades que podría tener, definiendo así el riesgo aceptable. La gestión del riesgo se puede llevar oportunamente mediante el proceso que describe la Figura 2.

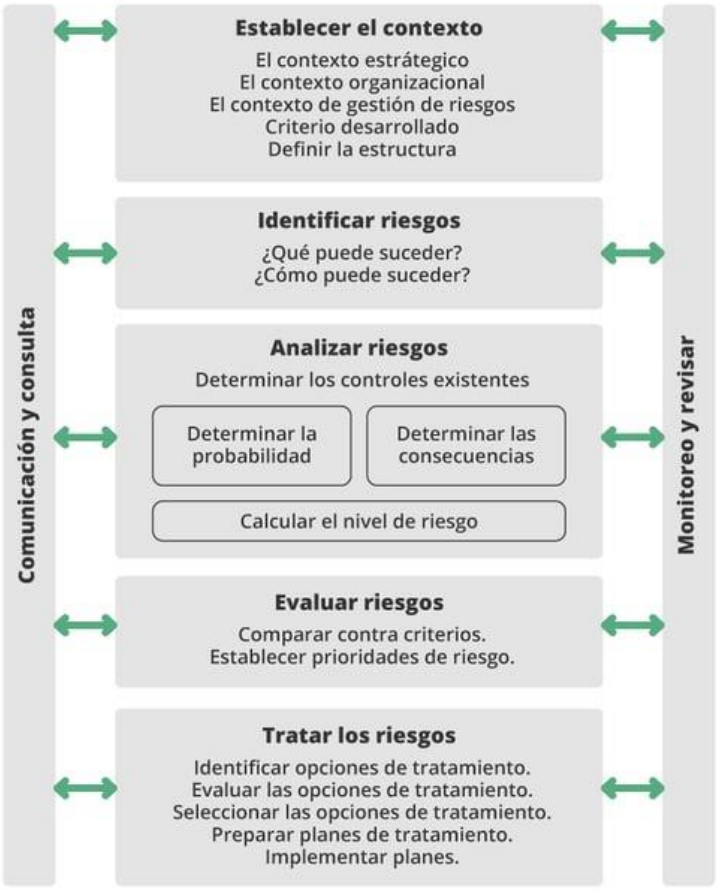

Figura 2. Proceso de gestión de riesgos.
Fuente: (piranirisk,2024).

Es esencial que este proceso esté debidamente documentado y sea lo más sistemático posible para garantizar la consistencia en los resultados, independientemente de quién realice el análisis. Otro punto crítico es la comparación de los resultados obtenidos en diferentes análisis a lo largo del tiempo, lo cual permite evaluar si las acciones implementadas están realmente mejorando la seguridad de la información en la organización.

2.3.3 ISO

La International Organization for Standardization (ISO), según su sitio web oficial ISO (2024) reúne a expertos globales para acordar las mejores prácticas en una variedad de áreas, desde la fabricación de productos hasta la gestión de procesos. Como una de las organizaciones internacionales no gubernamentales más antiguas, ISO ha facilitado el comercio y la cooperación

entre personas y empresas en todo el mundo. Los estándares internacionales publicados por ISO tienen como objetivo hacer la vida más sencilla, segura y mejor.

Tal como lo ratifica Global Standards. (2024), ISO fue fundada en Londres en 1946, 65 delegados de 25 países se reunieron para discutir el futuro de la Normalización Internacional. En 1947, ISO nace oficialmente con 67 comités técnicos. Su origen se remonta a la necesidad de unificar estándares internacionales tras la Segunda Guerra Mundial, facilitando el comercio y la cooperación internacional. El nombre "ISO" proviene del griego "isos", que significa "igual", reflejando su misión de estandarizar procedimientos y productos a nivel mundial sin importar países o lenguajes. Desde su fundación, ISO ha crecido exponencialmente, publicando más de 24,000 estándares que abarcan una amplia gama de industrias, desde tecnología y seguridad alimentaria hasta salud y gestión ambiental.

A lo largo de su historia, ISO ha evolucionado para adaptarse a los cambios tecnológicos y las necesidades globales. En las últimas décadas, ha incorporado normas relacionadas con la digitalización, ciberseguridad y sostenibilidad, reflejando las prioridades emergentes de la sociedad moderna. Su proceso de desarrollo de estándares es inclusivo y colaborativo, involucrando a expertos de diferentes países y sectores. Esta evolución constante asegura que los estándares ISO sigan siendo relevantes y útiles, facilitando la innovación y el comercio global, y promoviendo prácticas seguras y eficientes en todo el mundo.

En 1950, ISO, estaba en sus primeros años de operación tras su fundación en 1947. Durante este período inicial, la organización se centró en establecer su estructura y procedimientos para la creación de estándares internacionales. En estos años formativos, ISO trabajó principalmente en áreas industriales y técnicas, con el objetivo de mejorar la eficiencia y la compatibilidad en la manufactura y el comercio global. Se iniciaron comités técnicos que se encargaban de desarrollar normas en diferentes sectores, como ingeniería mecánica, productos químicos y textiles.

El enfoque de ISO en 1950 era fomentar la cooperación internacional para superar las barreras comerciales y tecnológicas que existían tras la Segunda Guerra Mundial. Aunque el número de estándares publicados en este período era relativamente pequeño comparado con el presente, los primeros estándares de ISO sentaron las bases para la normalización global, permitiendo una mayor interoperabilidad y calidad en productos y servicios. Este trabajo inicial fue crucial para establecer la reputación y la credibilidad de ISO como una autoridad en la creación

de estándares que facilitan el comercio y la innovación a nivel mundial.

2.3.3.1 ISO 27000

Presentación, G. S. B. (2023) establece que las normas ISO 27000 son un conjunto de estándares desarrollados por la ISO que proporcionan un marco para la Gestión de la Seguridad de la Información, aplicable a todo tipo de organizaciones. Estos estándares tienen como objetivo optimizar la gestión de riesgos y garantizar la confidencialidad, integridad y disponibilidad de la información para las partes autorizadas, limitando su acceso a personas no autorizadas. Además, incluyen las mejores prácticas para el desarrollo, implementación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI).

La norma ISO 27000 fue inicialmente publicada el 1 de mayo de 2009 y ha sido revisada en varias ediciones posteriores: una segunda edición el 1 de diciembre de 2012, una tercera edición el 14 de enero de 2014 y una cuarta edición en febrero de 2016. Este estándar proporciona una visión general de las normas que conforman la serie ISO 27000, detallando el alcance y el propósito de cada una de ellas. También incluye todas las definiciones utilizadas en la serie ISO 27000 y subraya la importancia de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI), ofreciendo una introducción detallada a estos sistemas.

La familia ISO 27000 incluye varias normas relacionadas, las cuales mencionaremos las más importantes:

- ISO 27001: Define los requisitos para establecer, implementar, mantener y mejorar un SGSI dentro de una organización. Proporciona un marco para gestionar los riesgos de seguridad de la información de manera sistemática y efectiva.
- ISO 27002: Anteriormente conocida como ISO 17799, esta norma ofrece directrices detalladas sobre controles de seguridad de la información. Describe un conjunto de controles y buenas prácticas que pueden ser implementados para mejorar la seguridad de la información.
- ISO 27005: Se centra en la gestión de riesgos de seguridad de la información. Proporciona pautas sobre cómo llevar a cabo la evaluación y tratamiento de riesgos relacionados con la seguridad de la información.
- ISO 27003: Ofrece orientación específica sobre la implementación de un SGSI,

detallando los procesos, actividades y consideraciones necesarias para llevar a cabo esta implementación de manera efectiva.

- ISO 27004: Se enfoca en la medición y evaluación del desempeño del SGSI. Proporciona directrices sobre cómo establecer indicadores clave de rendimiento (KPIs) y métricas para evaluar la eficacia y eficiencia del sistema de gestión.
- ISO 27006: Especifica los requisitos para organismos de certificación que realizan auditorías y certificación de conformidad con ISO 27001.

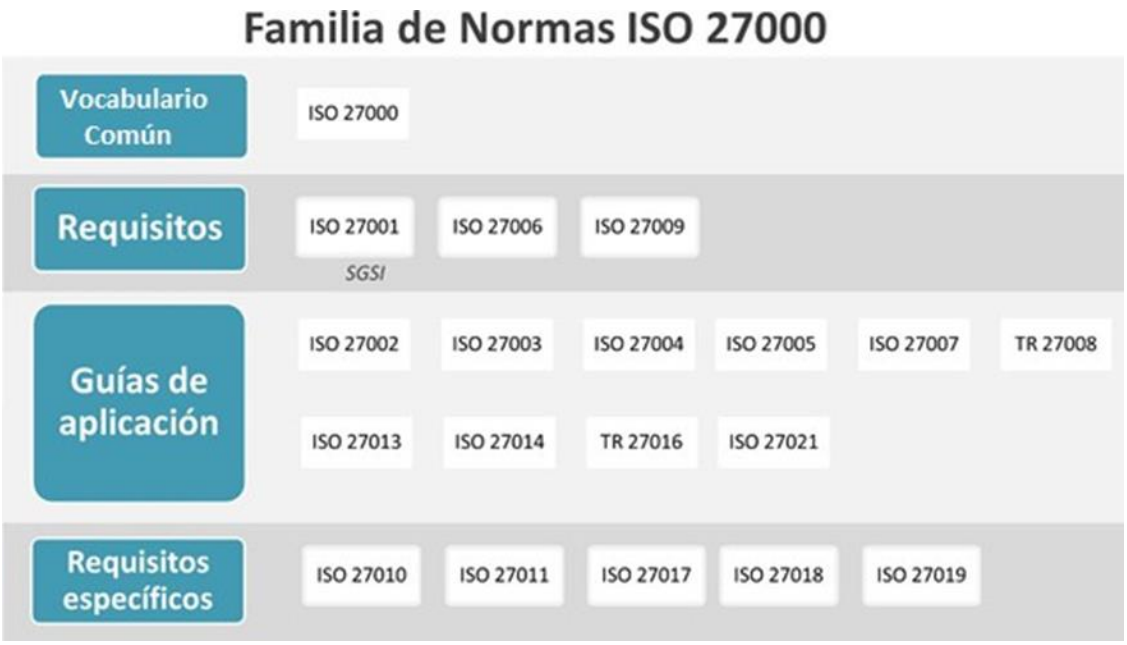

Figura 3. Familia de normas ISO 27000.
Fuente: (Referencias normativas ISO 27000, mayo 2024).

2.3.4 SGSI

La definición de un SGSI según Gómez Fernández, L. & Fernández Rivero, P. P. (2018) "Es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización". Y que para su implementación implica establecer procesos formales y definir claramente las responsabilidades, apoyadas en políticas, planes y procedimientos que deben documentarse como información oficial dentro de la organización.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) es crucial por varias razones, primeramente, ayuda a proteger la información de la organización contra posibles amenazas, riesgos y ataques, asegurando el cumplimiento de las leyes y regulaciones relacionadas con la privacidad y protección de datos, así como con los estándares internacionales de seguridad. Además, contribuye a garantizar la continuidad del negocio, dado que la información es fundamental para la operación organizativa. El SGSI también fortalece la imagen y la reputación de la organización, demostrando su compromiso con la protección de la información, y finalmente, ayuda a reducir los costos asociados con incidentes de seguridad.

Figura 4. SGSI relaciones entre los componentes del riesgo.
Fuente: (Kwo-Jean et al, 2004).

Un SGSI busca identificar los riesgos y amenazas de seguridad, analizar su impacto y probabilidad, y luego implementar medidas de seguridad efectivas para mitigar estos riesgos. Al establecer controles de seguridad apropiados, el SGSI tiene como objetivo reducir al mínimo la probabilidad de interrupciones en las operaciones comerciales o pérdidas financieras debido al extravío o compromiso de información crítica.

El marco teórico de un SGSI incluye elementos como normas y estándares internacionales. Por ejemplo, la norma ISO 27001 proporciona un marco reconocido para la implementación

efectiva de un SGSI.

Figura 5. Elementos importantes de un SGSI.
Fuente: (Sistema de Gestión de Seguridad de la Información (SGSI), 2023).

2.4 METODOLOGÍAS

2.4.1 ISO 27001

La ISO/IEC 27001 es la norma más reconocida globalmente para sistemas de Gestión de la Seguridad de la Información (SGSI), estableciendo los requisitos que debe cumplir dicho sistema.

Esta norma brinda a empresas de cualquier tamaño y sector directrices para establecer, implementar, mantener y mejorar de forma continua un sistema de gestión de la seguridad de la información, también fomenta un enfoque completo de la seguridad de la información que incluye aspectos como las personas, las políticas y la tecnología. Un sistema de gestión de la seguridad de la información implementado según esta norma es una herramienta esencial para la administración de riesgos, la resiliencia cibernética y la eficiencia operativa.

2.4.2 ANTECEDENTES DE ISO 27001

2.4.2.1 HISTORIA DE LA NORMA ISO 27001

Según la línea de tiempo trazada por Palomino (2022), en 1990 se introduce el primer estándar relacionado con la seguridad, conocido como BS 7799 (British Standard). Posteriormente, la ISO adopta este estándar y lo publica como ISO 17799 en el año 2000. Más tarde, en 2005, se renombra como ISO/IEC 27002 como parte de la familia ISO 27000. En 2013, se lleva a cabo una segunda revisión para actualizarlo según las necesidades actuales, y la tercera revisión, publicada en febrero de 2022, es la versión vigente.

En 1998, se publica un estándar que incorpora la seguridad dentro de un ciclo de mejora continua. Este estándar es adoptado por la ISO y publicado como ISO/IEC 27001 en el año 2005. En 2013, se realiza una segunda revisión de este estándar, que continúa siendo la versión vigente hasta el momento.

Es fundamental destacar que, al publicar la norma en 2013, se abordó la problemática entonces existente sobre la seguridad de la información, reconociendo que las circunstancias y desafíos en 2013 eran muy diferentes a los de 2022.

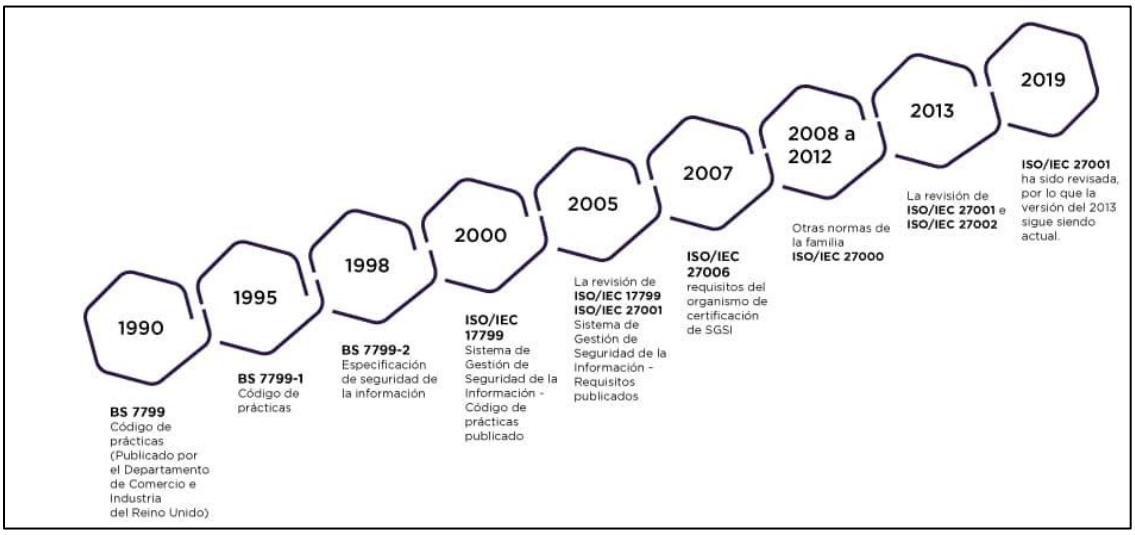

Figura 6. Fechas importantes en el desarrollo de familia ISO 27000.
Fuente: Palomino (2022).

2.4.2.2 ISO 27001 VERSIÓN 2022

Durante la pandemia de COVID hasta la actualidad, se observó un profundo impacto cultural, económico y tecnológico. Las empresas adoptaron el teletrabajo, la educación a distancia y herramientas colaborativas en línea, aumentando el acceso a Internet a través de dispositivos móviles. Este período también ha presenciado un cambio en los centros de datos hacia la nube,

junto con un aumento en los ciberataques a nivel global y la aparición de nuevas amenazas como el ransomware. Además, se introdujo nueva normativa de protección de datos, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea en 2016, que ha marcado un hito en la protección de la privacidad. Estos desarrollos tecnológicos han generado una cantidad masiva de datos provenientes de dispositivos conectados a Internet, reflejando las nuevas necesidades y expectativas de múltiples partes interesadas que deben abordarse en la nueva versión de la norma.

La nueva versión de ISO 27001, publicada en 2022, presenta cambios significativos, especialmente en el anexo A que ahora incluye todos los controles del sistema de gestión alineados con la norma ISO/IEC 27002 también actualizada en febrero de 2022. Los cambios más notables en ISO 27002 incluyen la incorporación de un total de 93 controles de seguridad de la información, una nueva estructura que reduce los dominios de 14 a solo 4, modificaciones en los controles que incluyen nuevos y fusionados, así como la introducción de nuevos conceptos y atributos asociados a cada control. Además, el cambio de nombre de la norma tiene un impacto significativo al pasar de "Código de prácticas para los controles de seguridad de la información" a "Código de prácticas para los controles de seguridad de la información, ciberseguridad y protección de la privacidad", lo que implica que además de trabajar en seguridad de la información, se requiere ahora abordar la ciberseguridad y la protección de la privacidad, ampliando así el alcance y las exigencias de esta normativa.

2.4.3 APLICACIÓN ISO 27001

Tal como lo hemos descrito hablar de ISO 27001 es hablar de un SGSI, ya que ISO 27001 establece los requisitos básicos para un SGSI como tal, por lo tanto, según la norma existe una paso a paso para implementar disco SGSI:

1. **Establecer la política de seguridad:** implica definir los objetivos, el marco general, los requisitos legales y los criterios de evaluación de riesgos. También se debe establecer una metodología aprobada por la dirección o la junta directiva.
2. **Determinar el alcance del Sistema de Gestión de Seguridad de la Información (SGSI):** conlleva en comprender qué se logrará al implementar el plan en la organización, incluyendo la identificación de activos, tecnologías y sus descripciones.

3. **Identificar riesgos:** implica reconocer las posibles amenazas para la compañía, identificar a los responsables, las vulnerabilidades y evaluar el impacto en caso de violación de la confidencialidad, integridad y disponibilidad de los activos de información.
4. **Analizar y evaluar los riesgos:** determina evaluar el impacto potencial de los riesgos, la probabilidad de ocurrencia y cómo afectarían a los controles existentes. También implica decidir si los riesgos pueden aceptarse o si necesitan ser mitigados.
5. **Aplicar un tratamiento de riesgos:** conlleva implementar controles adecuados, clasificar los niveles de riesgo y evitar o transferir los riesgos a terceros cuando sea posible.
6. **Declarar la aplicabilidad:** establecer los objetivos de control y seleccionar los controles que se implementarán en el SGSI.
7. **Realizar la gestión del SGSI** incluye definir cómo se tratarán los riesgos, aplicar los controles identificados, definir responsabilidades, implementar controles, establecer métricas, generar conciencia en la organización y fomentar una cultura de seguridad.
8. **Monitorear el SGSI** implica realizar revisiones periódicas para verificar el cumplimiento con la norma ISO 27001, evaluar la efectividad del sistema y planificar mejoras continúas basadas en los resultados de las revisiones.

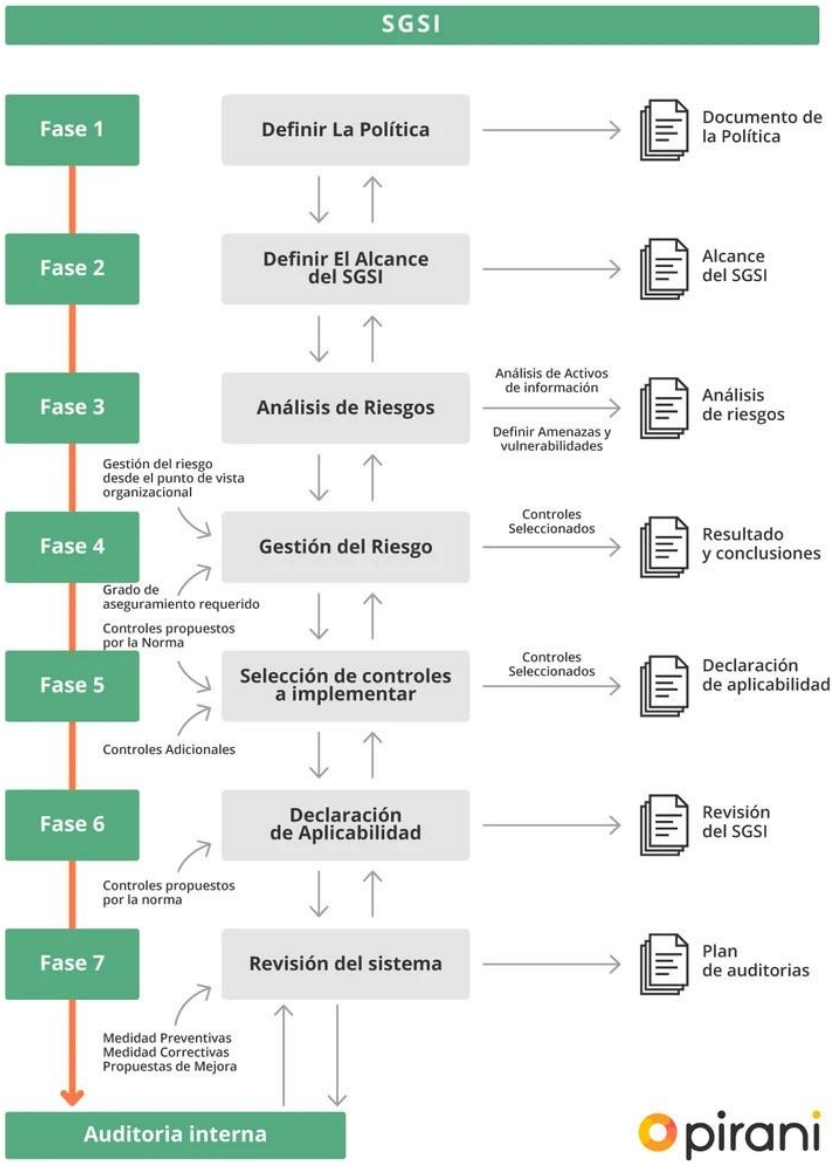

Figura 7. Fases generales para la implementación de un SGSI basado en ISO 27001.
Fuente: (piranirisk, 2024).

2.4.4 MAGERIT

MAGERIT, es la metodología de análisis y gestión de riesgos de la información de dominio público desarrollada por el Consejo Superior de Administración Electrónica (CSAE) del Gobierno de España (Portal administración tecnológica, 2024).

Según Alemán Novoa, H. & Rodríguez Barrera, C. (2015) esta metodología ayuda a

identificar y diseñar las acciones adecuadas para mantener los riesgos bajo control y preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación. Una de sus principales ventajas es que las decisiones que requieran validación por parte de la dirección estarán respaldadas por fundamentos sólidos y serán fácilmente justificables y defendibles.

2.4.5 INICIOS DE MAGERIT

Los antecedentes de la metodología MAGERIT se remontan al desarrollo de prácticas de gestión de riesgos en el ámbito de la seguridad de la información, especialmente en el contexto de la Administración Pública Española. Previo al desarrollo de MAGERIT, existían enfoques iniciales como el Análisis de Riesgos en Tecnologías de la Información (ARTI), que sentaron las bases para la evaluación sistemática de riesgos en sistemas informáticos. Además, la evolución de estándares internacionales relacionados con la seguridad de la información, como la serie ISO/IEC 27000, proporcionó directrices y requisitos que influyeron en el desarrollo de metodologías específicas como MAGERIT. En este contexto, el Centro Criptológico Nacional de España (CCN-CERT) desarrolló la metodología MAGERIT a finales de la década de 1990 y principios de los años 2000, como un marco estructurado y sistemático para la gestión de riesgos de sistemas de información en el sector público español.

2.4.6 ANÁLISIS DE RIESGOS DE LA METODOLOGÍA MAGERIT

Existen ciertos elementos dentro de la metodología que deben de ser considerados:

1. Identificar los recursos significativos para la organización, analizar cómo están relacionados entre sí y evaluar su valor para el funcionamiento y los objetivos de la entidad.
2. Analizar las posibles amenazas a las que están expuestos cada uno de los recursos identificados previamente.
3. Evaluar las medidas de protección implementadas para mitigar los riesgos y determinar su efectividad frente a las amenazas identificadas.
4. Evaluar el posible daño o impacto que sufriría un recurso en caso de que una amenaza se materialice.
5. Calcular el riesgo asociado a cada amenaza identificada, considerando tanto el impacto potencial como la probabilidad de ocurrencia de la amenaza.

2.5 HERRAMIENTAS

2.5.1 CICLO PDCA

Zapata (2016) menciona que el ciclo PDCA conocido como ciclo de la calidad, círculo de Deming o espiral de la mejora continua, es una herramienta planteada inicialmente por Walter Shewhart y trabajada por Deming en 1950; se fundamenta en cuatro pasos: planificar (Plan), hacer (DO), verificar (Check) y actuar (Act). Este como tal puede apoyar a la ejecución de los procesos de forma organizada; por tanto, es viable para su uso en las organizaciones ya que permite la ejecución de la componente de manera eficaz. En la Figura 8 se detallan las actividades básicas en cada componente.

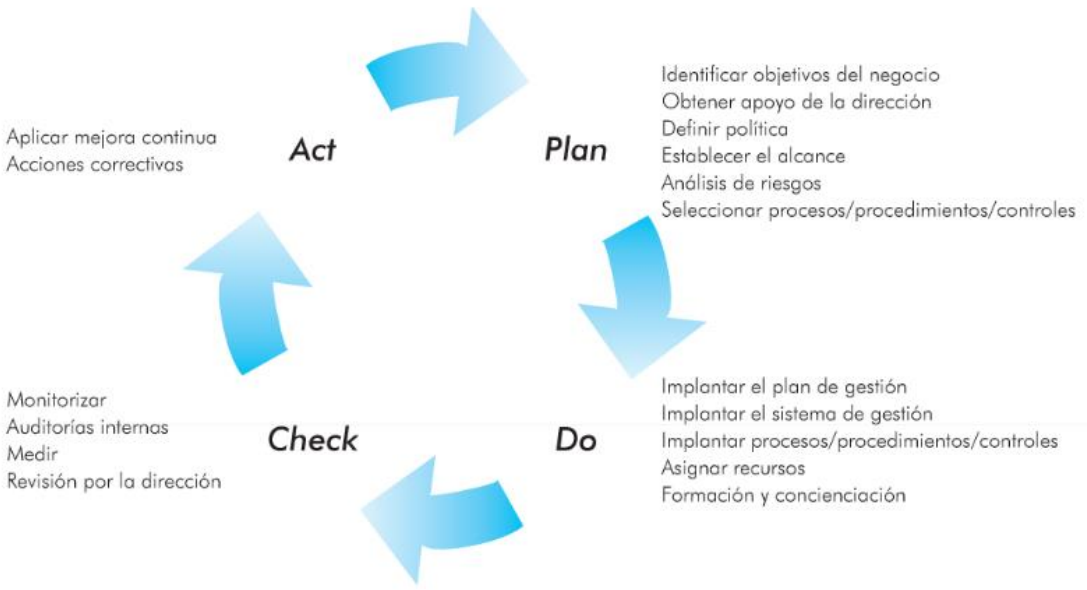

Figura 8. Ciclo PDCA.
Fuente: (Gómez Fernández, L. & Fernández Rivero, P. P., 2018).

En el contexto de la creación de un SGSI basado en ISO 27001 sería parte fundamental para asegurar la eficacia y la mejora continua del sistema.

En la fase de Planificar (Plan), se establecen los objetivos y el alcance del SGSI, se identifican los activos críticos, las amenazas y los riesgos, y se desarrollan políticas y procedimientos de seguridad. Durante la fase de Hacer (Do), se implementan las actividades y controles definidos, se capacita al personal y se establecen procedimientos operativos. La fase de Verificar (Check) implica realizar auditorías internas, evaluaciones de riesgos y revisar métricas

de desempeño para asegurar el cumplimiento y efectividad del SGSI. Finalmente, en la fase de Actuar (Act), se analizan los resultados de las auditorías y evaluaciones para identificar áreas de mejora, se implementan acciones correctivas y preventivas, y se actualiza el SGSI en función de las lecciones aprendidas y cambios en el entorno. Este enfoque cíclico garantiza que el SGSI evolucione de manera continua para enfrentar nuevas amenazas y mantener la seguridad de la información de manera efectiva.

2.5.2 EAR/PILAR

PILAR (Procedimiento Informático-Lógico para el Análisis de Riesgos) es un conjunto de herramientas EAR (Entorno de Análisis de Riesgos) cuya función es el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) (CCN-CER, 2024).

PILAR está diseñada para todas las organizaciones u organismos que disponen de infraestructuras de tecnologías de la información y necesitan gestionar eficazmente sus activos, llevando a cabo análisis tanto cuantitativos como cualitativos del impacto y la continuidad de las operaciones. Esta herramienta dispone de una biblioteca estándar de propósito general capaz de realizar calificaciones de seguridad y proponer salvaguardas respecto a normas internacionales como ISO 27001 y ENS (Esquema Nacional de Seguridad) del gobierno de España.

2.5.3 MATRIZ DE RIESGOS

Una matriz de riegos es una herramienta utilizada para la identificación de los riesgos relacionados con las actividades de cualquier rubro de una organización. Según RSM (2020) “Una matriz de riesgos, es una herramienta útil para toda empresa, que le permite identificar los riesgos a los que está expuesta. De esa forma, las compañías pueden determinar los niveles aceptables de exposición a aquellos.”.

Esta herramienta es una guía visual cuyo diseño facilita una identificación rápida de las prioridades a atender, lo que también agiliza el proceso de toma de decisiones y esta debe de tener las siguientes características:

- Se definen previamente niveles de probabilidad de los riesgos y su impacto, que permitan priorizar las acciones necesarias para la mitigación de estos.
- La matriz utiliza un sistema de colores para indicar visualmente el nivel del riesgo.

Por ejemplo: verde, amarillo, naranja y rojo.

- Debe de ser simple y clara para su fácil entendimiento e interpretación.

2.5.4 MODELO DE MADUREZ CMMI

Hoy en día, hay diversas metodologías, estándares, modelos de madurez y guías disponibles que pueden asistir a una organización en la mejora de sus operaciones. Los modelos de madurez representan una evolución de las metodologías empleadas para gestionar la calidad organizacional. Uno de ellos es el modelo CMMI (Capability Maturity Model Integration) creada por SEI (Software Engineering Institute), y gestionado a través de la universidad Carnegie-Mellon, actualmente la gestión la realiza el CMMI Institute, una empresa subsidiaria de ISACA. CMMI está contemplado como un marco de buenas prácticas que se define como un "modelo de madurez de estándar de calidad más utilizado a nivel internacional por las organizaciones desarrolladoras de software, aunque su uso no se limita solamente a este tipo de organización" (Pérez-Mergarejo et al., 2014).

CMMI se evalúa a través de un conjunto de áreas de proceso que incluyen objetivos y prácticas definidas. El nivel de madurez o capacidad asignado dependerá del grado de cumplimiento de estas áreas. Entre las características que destacan CMMI son:

- Un enfoque integral para la mejora de procesos.
- La incorporación de mejoras en el funcionamiento empresarial.
- Un enfoque gradual para implementar gestiones que optimicen la empresa.
- Una guía detallada para la mejora mediante niveles de madurez y capacidad.

2.5.5 ANÁLISIS DE BRECHAS

Para Viteri (2023) un análisis de brechas en el contexto de ISO 27001 es un proceso de evaluación diseñado para detectar las diferencias entre la situación actual de una organización en materia de Seguridad de la Información y los requisitos que establece la norma ISO 27001. Durante este análisis, se examinan varias áreas, como la gestión de activos, el control de acceso, la continuidad del negocio y la gestión de riesgos, entre otras, para identificar las brechas presentes y las áreas que requieren mejoras.

2.6 CONCEPTUALIZACIÓN

En este apartado, se hace una descripción general de ciertos conceptos generales de la investigación, los cuales serán de utilidad al lector para lograr apreciar la información presentada en esta tesis.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un sistema de gestión de seguridad de la información (SGSI) es un conjunto de directrices y procesos creados para ayudar a las organizaciones en un escenario de violación de datos. Al poseer un conjunto formal de directrices, las empresas pueden minimizar el riesgo y garantizar la continuidad del trabajo en caso de un cambio de personal. La ISO 27001 es una especificación de normas bien conocida para el SGSI a nivel empresarial. (Cisco, 2024)

BASE DE DATOS

Es una recopilación de datos sistemática y almacenada electrónicamente Puede contener cualquier tipo de datos, incluidos palabras, números, imágenes, videos y archivos. Suele usarse con un software denominado sistema de administración de base de datos (DBMS) para almacenar, recuperar y editar datos. (Amazon Web Services, 2024)

ACTIVO

Cualquier componente de un sistema de información que tenga valor para una organización, incluyendo, pero no limitándose a, hardware, software, infraestructura de red, información y personas (NIST SP 800-30)

RANSOMWARE

Es un tipo de malware que impide a los usuarios acceder a su sistema o sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes aparecieron al final de la década de los 80s, y en ese entonces pedían un pago por correo postal. Hoy en día, los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito. (MalwareByte, 2024)

SPYWARE

Es un software que se instala sin un consentimiento informado, ya sea en un ordenador tradicional, una aplicación en el navegador web o una aplicación móvil que se encuentra en el

dispositivo. El spyware comunica información personal confidencial de la víctima al atacante. (Kaspersky, 2024)

PHISHING

Es la combinación de Ingeniería Social y exploits técnicos, diseñados para convencer a una víctima de proporcionar información personal, generalmente realizado para obtener una ganancia monetaria por parte del atacante (Benavides et al., 2020)

SALVAGUARDAS

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. (Ministerio de Hacienda y Administraciones Publicas, 2024)

RIESGO

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. (Ministerio de Hacienda y Administraciones Publicas, 2024)

2.7 MARCO LEGAL

2.7.1 MARCO LEGAL A NIVEL INTERNACIONAL

El Convenio de Budapest sobre cibercrimen, que es un tratado internacional diseñado para combatir delitos informáticos y promover la cooperación internacional en este ámbito, fue adoptado en 2001 por el Consejo de Europa y tiene como objetivo principal armonizar las leyes nacionales relacionadas con la ciberdelincuencia, fortalecer las capacidades de investigación y facilitar la cooperación internacional en la lucha contra los delitos cibernéticos. Este tratado establece disposiciones legales para la prevención, investigación y enjuiciamiento de delitos informáticos, abordando temas como acceso ilegal a sistemas informáticos, interferencia con datos informáticos, fraude informático y delitos relacionados con la pornografía infantil.

El Convenio de Budapest establece un marco legal internacional para mejorar la seguridad cibernética y promover la cooperación entre los estados miembros, facilitando la extradición y asistencia legal mutua en investigaciones relacionadas con delitos informáticos. También enfatiza la protección de los derechos humanos y las libertades fundamentales en el contexto de las actividades de aplicación de la ley en línea.

En la actualidad, se está discutiendo en las Naciones Unidas un tratado internacional para combatir el cibercrimen, el cual podría convertirse en el primer instrumento vinculante de las Naciones Unidas en esta materia. El tratado buscaría crear un marco jurídico de alcance global para la cooperación internacional en materia de prevención e investigación del cibercrimen y para procesar penalmente a los cibercriminales. El mayor reto para dicho proyecto es solventar los desacuerdos que existen entre los miembros con respecto al alcance del tratado, las garantías en materia de derechos humanos, el modo de abordar las brechas en las capacidades de los Estados, la forma en el que tratado debe de cooperar con otros instrumentos y la importancia del género en el mismo.

2.7.2 MARCO LEGAL A NIVEL NACIONAL

En cada nación que existe sobre la Tierra, existe una serie de reglas y leyes que rigen a sus ciudadanos, la cual es conocida como la constitución. Esta se aplica tanto a instituciones como a individuos. Dentro de ella, se encuentran diversas series de códigos, reglamentos y normas de índole fiscal, comercial, civil y penal. En lo que respecta a la existencia de un marco legal de protección de la información, en nuestro país han existido diversos anteproyectos que han buscado establecer uno, pero lamentablemente ninguno ha pasado más allá de ser una simple iniciativa que no llama la atención a los políticos de turno.

De acuerdo con el informe de Eduardo Tome (IPANDETEC, 2019), en nuestro país no existe actualmente una ley vigente que regule la protección de datos personales. En 2015, se presentó un proyecto de ley de protección de datos personales, el cual fue impulsado por quien fuera vicepresidente del Congreso Nacional en ese entonces, el diputado Antonio Rivera Callejas. Este proyecto se había basado en otro anteproyecto presentado por el Instituto Nacional de Acceso a la Información Publica en el año 2013, el cual conto con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID). De dicho proyecto, a través de varios debates, al mes de abril de 2018 se habían aprobado 19 de los 97 artículos propuestos.

A pesar de que no existe una legislación especial, los datos personales si cuentan al menos con una protección que está reconocida en la Ley de Transparencia y Acceso a la Información Pública, mediante decreto legislativo No. 170-2006. Dentro de esta ley, en los artículos 24 al 26 se reconoce el Habeas Data, la protección de los datos personales y presenta a la oficina del Comisionado Nacional de Derechos Humanos como una oficina facultada para iniciar acciones

para la protección de datos personales, estableciendo además una prohibición en la cual ninguna persona puede solicitar a otros datos personales que puedan generar algún tipo de discriminación o poner en riesgo los derechos morales y patrimoniales del individuo.

Dentro de la Ley de Transparencia y Acceso a la Información Publica encontramos algunos de los siguientes artículos:

- Artículo 1: NATURALEZA Y FINALIDAD DE LA LEY: Esta ley es de orden público e interés social. Tiene por finalidad el desarrollo y ejecución de la política nacional de transparencia, así como el ejercicio del derecho de toda persona al acceso a la información pública para el fortalecimiento del Estado de Derecho y consolidación de la democracia mediante la participación ciudadana.
- Artículo 2: OBJETIVOS DE LA LEY: Son objetivos de esta Ley establecer los mecanismos para:
    - Garantizar el ejercicio del derecho que tienen los ciudadanos a participar en la gestión de los asuntos públicos.
    - Promover la utilización eficiente de los recursos del Estado.
    - Hacer efectiva la transparencia en el ejercicio de las funciones públicas y en las relaciones del Estado con los particulares.
    - Combatir la corrupción y la ilegalidad de los actos del Estado.
    - Hacer efectivo el cumplimiento de la rendición de cuentas, por parte de las entidades y servidores públicos.
    - Garantizar la protección, clasificación y seguridad de la información pública y el respeto a las restricciones de acceso en los casos de Información clasificada, información entregada al Estado, los datos personales confidenciales y la secretividad establecida por la Ley.
- Artículo 4: DEBER DE INFORMAR Y DERECHO AL ACCESO A LA INFORMACIÓN PUBLICA: Todas las instituciones obligadas deberán publicar la información relativa a su gestión o, en su caso, brindar toda la información concerniente a la aplicación de los fondos públicos que administren o hayan sido garantizados por el Estado.

- Artículo 6: PROMOCIÓN DE UNA CULTURA DE TRANSPARENCIA Y APERTURA DE LA INFORMACIÓN: Las instituciones obligadas deberán capacitar y actualizar de forma permanente a sus servidores públicos en la cultura de acceso a la información, la cultura de apertura informativa, transparencia de la gestión pública y el ejercicio de la garantía de Habeas Data.

Todos estos artículos y muchos más que no citaremos por la longitud del contenido, sentaron las bases para la creación del Instituto de Acceso a la Información Pública, el cual es el ente encargado de velar por mantener la transparencia en las operaciones del Estado, y de asegurar que solo aquella información que sea realmente necesaria se publique. Dicha ley fue la que sentó bases para la gestión de la información pública dentro de las entidades gubernamentales.

Asimismo, han existido diversas propuestas que se han derivado de esa ley, con el objetivo de crear un marco jurídico que permita proteger legalmente los datos personales de los ciudadanos. Una de estas propuestas fue la ley del Instituto de Acceso a la Información Pública que proponía regular lo relacionado a los datos personales. Mencionamos algunos de sus artículos:

- Artículo 23: HABEAS DATA: Se reconoce la garantía de Habeas Data
- Artículo 24: SISTEMATIZACIÓN DE ARCHIVOS PERSONALES Y SU ACCESO: Los datos personales serán protegidos siempre. El interesado, o en su caso el Comisionado de los Derechos Humanos por si o en representación de la parte afectada, y el Ministerio Publico, podrán iniciar las acciones legales necesarias para su protección. El acceso a los datos personales únicamente procederá por decreto judicial o a petición de la persona cuyos datos personales se contienen en dicha información o de sus representantes o sucesores.
- Artículo 25: PROHIBICIÓN DE ENTREGA DE INFORMACIÓN: Ninguna persona podrá obligar a otra a proporcionar datos personales que puedan originar discriminación o causar danos o riesgos patrimoniales o morales de las personas.

El artículo 3, numerales 8 y 9 del Proyecto de Ley de Protección de Datos Personales, define datos personales y datos sensibles de la siguiente manera:

- Datos personales: Cualquier información numérica, acústica, alfabética, biométrica, gráfica, fotográfica, de imagen, o de cualquier otro tipo concerniente a una

persona natural identificada o identificable

- Datos sensibles: Aquellos que se refieran a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada, tales como: hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud, físicos o psíquicos y preferencias sexuales, así como cualquier otro dato respecto de la libertad individual protegido por la Constitución de la Republica o en Convenios Internacionales suscritos por Honduras.

Todas estas propuestas no han avanzado en las discusiones del Congreso Nacional, seguramente por desconocimiento de la importancia que tienen para algunos sectores del país, y porque no son proyectos que permitan llamar la atención del electorado nacional, lo cual provoca que nuestro país no persiga estos tipos de crímenes, y que incluso criminales de otras naciones vengan a realizar sus actividades dentro de nuestro territorio de manera impune.

CAPÍTULO III – METODOLOGÍA DE LA INVESTIGACIÓN

3.1 ENFOQUE

De acuerdo con Hernández-Sampieri, R., & Mendoza, C. (2020) una investigacion mixta representan un conjunto de procesos sistematicos, empiricos y criticos de investigacion que implican la recoleccion y el analisis de datos tanto cualitativos como cuantitativos para realizar inferencias de toda la informacion recabada y lograr un mayor entendimiento del fenómeno bajo estudio.

Para el diseño de un SGSI basado en la norma ISO 27001, debe de permitir explorar en profundidad las experiencias, percepciones y desafíos internos; también debe de facilitar la comprensión de los factores contextuales y culturales específicos de la empresa mediante una cuantificación de los resultados que permita una fácil comprensión y que al final influyen en la adopción y efectividad del SGSI. Partiendo de la pregunta de investigación principal, que busca poder solventar un problema mediante la implementación de metodologías y técnicas que permitan aumentar la seguridad de la información, encontramos que el enfoque mixto ofrece un modelo que se adapta mejor al desarrollo de la investigación.

3.2 ALCANCE

De acuerdo con Greene et al. (1989), Morgan (2014), Morse (2003) y Hernandez-Sampieri et al. (2018), el diseño secuencial exploratorio es un enfoque de investigacion mixta que combina una fase cualitativa inicial de exploracion y comprension en profundidad, con una fase cuantitativa posterior de prueba y generalización de los hallazgos.

Según Balmaceda (2023), el diseño secuencial exploratorio implica una secuencia temporal en la cual se lleva a cabo primero una fase cuantitativa y luego una fase cuantitativa. La fase cualitativa se enfoca en la exploración y comprensión en profundidad del fenomeno estudiado, utilizando metodos como entrevistas, observacion participante o analisis de documentos. La fase cuantitativa se centra en la recopilacion y analisis de datos cuantitativos para probar y generalizar los hallazgos obtenidos en la fase cualitativa.

El alcance de esta investigación será secuencial exploratorio debido a la necesidad de entender y caracterizar los diversos aspectos y prácticas que la empresa puede implementar en el

proceso de adopción de un SGSI. La naturaleza exploratoria permite identificar las variables clave, desafíos y contextos específicos en los que se aplican los principios de ISO 27001, proporcionando una visión detallada y sistemática de cómo se implementan y gestionan los controles de seguridad de la información. Este enfoque facilitara una comprensión integral del estado actual y las mejores prácticas en la implementación de SGSI, sirviendo como base para futuras investigaciones y mejoras en el campo.

3.3 DISEÑO

Un diseño de investigación es definido como una estructura u organización esquematizada que adopta el investigador para relacionar y controlar las variables de estudio. El objetivo de cualquier diseño es imponer restricciones controladas a las observaciones de los fenómenos. (Hugo Sanchez Carlessi, 2015)

En esta sección, se describe brevemente el diseño de la investigación con el propósito de alcanzar los objetivos establecidos. Este estudio utiliza un diseño no experimental de tipo transversal.

3.3.1 POBLACIÓN

Cualquiera que sea el tipo o diseño de investigación que se realice, uno de los principales propósitos que debe de perseguirse es lograr que los resultados de un estudio puedan generalizarse a otros grupos diferentes del que sirvió de base. Una población comprende a todos los miembros de cualquier clase bien definida de personas, eventos u objetos. (Hugo Sanchez Carlessi, 2015)

En esta investigación, la población será todos los miembros que forman parte de los departamentos de TI que manejan acceso a los sistemas de información de San Services S. de R.L. que laboren en áreas encargadas de manejar el acceso y procesamiento de la información. Las áreas consideradas son las siguientes:

- Equipo de base de datos: El equipo de base de datos está compuesto por 1 jefe de área y 6 miembros del equipo.

- Equipo de DevOps: El equipo de DevOps este compuesto por 1 jefe de área, y 4 miembros del equipo.
- Equipo de Desarrolladores: El equipo de desarrolladores está compuesto por diversos equipos, con un total de 35 miembros.

3.3.2 MUESTRA

La muestra es un subconjunto que se toma de la población, con el objetivo de reducir el número de individuos o variables que se estudiaran, permitiendo dar facilidad de análisis al estudio y lograr llegar a conclusiones que puedan considerar como aplicables al resto de la población. (Hugo Sanchez Carlessi, 2015)

La muestra se escogió en base a los criterios de inclusión y exclusión, escogiendo individuos que pudieran proveer la información requerida para esta investigación, escogiendo un total de 7 personas, quienes fueron los que colaboraron con el levantamiento de datos.

3.3.3 TÉCNICA MUESTREO

Para esta investigación se definió utilizar una técnica de muestreo no probabilístico intencional ya que según Otzen & Manterola (2017) es una técnica donde el investigador selecciona las muestras basadas en un juicio subjetivo y de manera estratégica limitando la muestra a ciertas características de la población. Se necesita una muestra a partir de un criterio en base al conocimiento y la experiencia del análisis planteado sobre la situación actual en cuanto a seguridad de la información en la empresa y cuáles son las mejoras que pueden aplicar.

3.4 TABLA DE CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

A continuación, se presentan los criterios de inclusión y exclusión que se utilizaron para lograr escoger nuestra población de interés dentro de la organización.

Tabla 2. Criterios de Inclusión y Exclusión

CRITERIOS DE INCLUSIÓN	CRITERIOS DE EXCLUSIÓN
Formar parte del departamento de TI.	No formar parte del departamento de TI.
Formar parte de un área de TI que maneje el equipo o procesos que gestionen o procesen información clave	No formar parte de un área de TI que maneje equipos o procesos que manejen información clave para la

de la organización.	organización.
Tener el conocimiento relevante y adecuado de los procesos e información gestionada en el área.	No poseer los conocimientos necesarios de todos los procesos e información gestionada en el área.
Interactuar con diversos departamentos del área de TI que estén involucrados en el manejo de información	No interactúa con departamentos o áreas relevantes al manejo de la información de TI
Poseer más de 2 años en la posición que desempeña actualmente	No posee más de 2 años en la posición desempeñada actualmente.

Fuente: (Elaboración propia).

3.5 HIPÓTESIS

Como lo sostiene Marinas (2005) "si investigamos no es tanto para verificar (un modelo, una hipótesis cerrada) sino para descubrir. Precisamente porque el material con el que tratamos es un material sensible que dice tanto de quien lo dice, como del que está construyendo al decirlo así o por quien está investigando en ese momento" (p. 134).

Por lo tanto, en esta investigación no aplica una hipótesis debido a que se busca la exploración, descripción e interpretación de los factores relacionados con la seguridad de la información dentro de la empresa, sin la necesidad de formular y probar hipótesis específicas.

3.6 MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla 3. Matriz de operacionalización de las variables

Variable	Tipo de Variable	Categorías o dimensiones	Definición	Indicador	Nivel de medición	Unidad de medida
SGSI	Mixto	Política de Seguridad	Directrices y objetivos generales de la seguridad de la información	Existencia y aprobación de la política	Nominal	Revisión documental
		Control de Acceso	Medidas para asegurar que el acceso a la información esté restringido	Controles de acceso	Nominal	Reportes de seguridad
		Formación y Concienciación	Programas de formación y concienciación para empleados sobre seguridad	Plan de capacitaciones	Nominal	Registros de asistencias y encuestas aplicadas.
		Gestión de riesgos	Procesos para identificar, evaluar y tratar los riesgos de seguridad	Matriz de riesgos	Nominal	Informe de análisis de riesgos
Norma ISO 27001	Mixto	Contexto de la organización	Comprensión del entorno interno y externo de la organización	Fortalezas, Oportunidades, Debilidades y Amenazas	Nominal	Documentos
		Liderazgo	Compromiso y apoyo de la alta dirección para el SGSI	Reuniones de revisión de la dirección - Asignación de recursos	Nominal	Documento registro de reuniones

		Planificación	Identificación de riesgos y oportunidades, y establecimiento de objetivos	Análisis de riesgos	Nominal	Informe de análisis de riesgos
		Soporte	Recursos, competencias, concienciación y comunicación necesarios	Evaluaciones de competencias	Nominal	Registros de evaluación de competencias
		Operación	Implementación y control de los procesos del SGSI	Procedimientos documentados - Registros de incidentes de seguridad	Nominal	Procedimientos escritos
		Evaluación del desempeño	Monitoreo, medición, análisis y evaluación del desempeño del SGSI	Resultados de auditorías internas - Indicadores de desempeño (KPIs)	Nominal	Tableros de indicadores
		Mejora	Acciones correctivas y preventivas para mejorar el SGSI	Reporte de acciones correctivas implementadas - Resultados de revisiones de la dirección	Nominal	Informes de revisión

Fuente: Elaboración propia

3.7 TÉCNICAS, INSTRUMENTOS, PROCEDIMIENTOS Y ANÁLISIS

3.7.1 TÉCNICAS

Encuestas: De acuerdo con Alberto Marradi (Alberto Marradi, 2007), la encuesta o sondeo, es una técnica que permite recolectar datos sobre actitudes, creencias u opiniones de los individuos estudiados, permitiendo indagar sobre diversos temas tales como pautas de consumo, hábitos, prejuicios e intenciones. Se caracteriza por su adecuación para relevar muchas propiedades referidas a muchos individuos y sus ámbitos de aplicación son diversos: académicos, políticos y comerciales.

En esta investigación, la encuesta es unas de las fuentes de recolección de datos más importantes ya que por medio de esta determinamos el estado actual de la empresa con respecto a la implementación del SGSI para así poder realizar una planificación para el logro de metas.

Entrevistas: Según explica Alberto Marradi (Alberto Marradi, 2007), la entrevista se refiere a una forma especial de encuentro, la cual tiene como objetivo una conversación que tiene como fin el recolectar determinado tipo de informaciones en el marco de una investigación.

En la presente investigación, también se aplicó la entrevista para determinar el grado de conocimiento con respecto al análisis y evaluación de los riesgos que existen dentro de la organización, y poder escuchar una opinión de la población seleccionada sobre el desenvolvimiento del tema.

3.7.2 INSTRUMENTOS

Microsoft Forms: Microsoft Forms permite crear encuestas, cuestionarios y sondeos, invitar a otros usuarios para que respondan desde cualquier navegador web o dispositivo móvil, ver resultados en tiempo real, usar análisis integrados para evaluar respuestas y exportar resultados a Excel para realizar análisis adicionales o asignar notas. (Microsoft Corporation, 2024)

Microsoft Teams: es una aplicación de colaboración creada para el trabajo hibrido para que todos los equipos de trabajo dentro de una organización estén informados, organizados y conectados en un mismo lugar. (Microsoft Corporation, 2024)

Microsoft Excel: Excel es una herramienta eficaz que forma parte de la suite de Microsoft Office. Excel permite obtener información con significado a partir de grandes cantidades de datos. También funciona muy bien con cálculos sencillos y para realizar el seguimiento de casi cualquier

tipo de información. La clave para desbloquear todo este potencial es la cuadricula de las celdas. Las celdas pueden contener números, texto o formulas. Los datos se escriben en las celdas y se agrupan en filas y columnas. Esto permite sumar datos, ordenarlos y filtrarlos, ponerlos en tablas y crear gráficos muy visuales. (Microsoft Corporation, 2024)

3.7.3 PROCEDIMIENTOS

Se aplicó de manera digital dos encuestas previamente estructuradas, la primera encuesta fue en base al anexo A del ISO 27001:2022 donde se encuentran las referencias de los cuatro controles de seguridad de la información, está se desplegó por medio de Office Forms al personal de TI la cual permitió obtener una comprensión profunda de las percepciones, experiencias y practicas relacionadas a la seguridad de la información dentro de la empresa. La otra encuesta fue para realizar un análisis de la situación actual en San Services en base a los requisitos técnicos de la norma ISO 27001. Ambas encuestas buscan un análisis de GAP que evalúa la situación actual y cuál sería el plan de acción para llegar a la situación deseada según la postura de seguridad actual de la empresa.

También se agendó un espacio para llevar a cabo una entrevista con preguntas abiertas con las gerencias de TI (ver Anexo 3) anteriormente mencionadas a través de una sesión virtual por Microsoft Teams en la cual se abordó una agenda para poder llevar a cabo una identificación de activos y obtener datos relevantes para desarrollar un análisis de los riesgos.

3.7.4 PLAN DE ANÁLISIS DE DATOS

Un plan de análisis de datos es la columna vertebral de cualquier esfuerzo de investigación. Sirve como hoja de ruta y guía a los investigadores a través del proceso de extracción de información significativa a partir de datos sin procesar (Fastercapital,2024). En esta investigación por medio de técnicas como la encuesta y la entrevista podemos definir los siguientes pasos:

1. Investigación de situación actual y preparación de los datos.

   Se establecieron las fuentes correctas en las que se pudiera proporcionar más información sobre la situación actual y se determinó si los resultados obtenidos satisfacían las preguntas de investigación.

2. Revisión de la información.

   Se revisó los temas identificados para asegurar de que sean coherentes y abarquen todos

los datos relevantes, así como también tengan validez y confidencialidad dentro del contexto de seguridad de la información de la empresa.

3. Análisis de los datos

   Se procedió a la tabulación y codificación de los datos en Microsoft Excel, por medio de tablas y gráficas tanto para el análisis de brechas como para el análisis de riesgos como parte del diseño del SGSI.

4. Resultados

   Se mostraron los resultados obtenidos de manera gráfica para su mejor comprensión y se analizaron para lograr las conclusiones y recomendaciones.

3.8 FUENTES DE INFORMACIÓN

Las fuentes de información son herramientas fundamentales para adquirir conocimiento, estas nos permiten el "acceso y búsqueda de la información, su objetivo principal es el de buscar, fijar y difundir la fuente de información implícita en cualquier soporte físico" (García, 2019, p. 2) Juegan un papel esencial en la investigación y el aprendizaje, siendo la base para tomar decisiones informadas y construir conocimiento.

3.8.1 PRIMARIAS

De acuerdo con Sampieri, las fuentes primarias son el objetivo de la investigación bibliográfica o revisión de la literatura, y proporcionan datos de primera mano. (Sampieri, 1997)

Como fuentes de información primaria, se realizarán entrevistas y encuestas a la población seleccionada del departamento de TI de la organización San Services S. de R. L. La entrevista permitirá llevar a cabo una identificación de los activos existentes en la empresa que tengan que ver con el manejo de información, así como datos relevantes que permitan hacer una evaluación de los riesgos. Asimismo, la encuesta al personal permitirá saber las experiencias y practicas relacionadas a la seguridad de la información de la empresa.

3.8.2 SECUNDARIAS

Se utilizaron documentos, tesis académicas, artículos y libros relacionados con la implementación de SGSI basados en norma ISO 27001 en entornos empresariales. Además, se consultaron bases de datos académicas como Google Académico, Redalyc, el Centro de Recursos para el Aprendizaje e Investigación (CRAI) de UNITEC, artículos científicos en Internet y el documento oficial de ISO 27001 en su versión 2022 que respalda los argumentos con evidencia en la investigación.

3.9 MATRIZ DE CONGRUENCIA

Tabla 4. Matriz de congruencia

Pregunta General	Objetivo General	Preguntas de Investigación	Objetivos	Metodología	Variables	Indicadores	Instrumentos
¿Cómo se puede diseñar un Sistema de Gestión de Seguridad de la Información eficaz y conforme con la norma ISO 27001:2022 en la empresa San Services S. de R.L.?	Proponer el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para salvaguardar la integridad, confidencialidad y disponibilidad de la información de los procesos más críticos de San Services S. de R.L. basados en la norma ISO 27001:2022.	¿Cuál es la situación actual de San Services S. de R.L. en cuanto a la infraestructura de TI y sus sistemas de manejo de datos ante posibles vulnerabilidades y puntos de riesgos?	Diagnosticar el estado actual del manejo de la seguridad de la información en la empresa según norma ISO 27001:2022.	Mixto.	Estado actual de la Seguridad de la Información.	Reporte y graficas.	Encuestas / Análisis de brechas.
		¿Qué riesgos de seguridad de la información son más críticos para San Services S. de R. L., y cómo deberían ser abordados en el diseño del SGSI?	Realizar un análisis de riesgos de seguridad de la información específicos para San Services S. de R. L. y desarrollar estrategias para mitigar los riesgos identificados.		Gestión de riesgos.	Reporte y gráficas.	Matriz de riesgos.
		¿Cuáles son los principales riesgos asociados a los activos críticos de San Services S. de R. L., y qué salvaguardas recomienda fortalecer la metodología MAGERIT para mitigar estos riesgos?	Evaluar los principales riesgos asociados a los activos críticos de San Services S. de R. L. mediante la metodología MAGERIT, tomando en cuenta la recomendación de salvaguardas para mitigar dichos riesgos.		Lista de activos esenciales de la organización.	Reporte y graficas.	Mitología MAGERIT /PILAR RM.

		¿Cómo se puede elaborar un documento que defina claramente el alcance del SGSI, delimitando sus objetivos para asegurar la claridad y el enfoque en la gestión de la seguridad de la información en San Services S. de R. L.?	Elaborar un documento con el alcance del SGSI que delimite los objetivos de este y permita claridad y enfoque en la gestión de la seguridad de la información dentro de San Services S. de R. L.		Definición del documento	Documento finalizado.	Guía ISO 27001.

Fuente: Elaboración propia

CAPÍTULO IV – RESULTADOS Y ANÁLISIS

Este capítulo presenta los resultados obtenidos tras la aplicación de instrumentos de medición, con el objetivo emplear el diseño del SGSI basado en la norma ISO 27001:2022 en la empresa San Services S. de R. L. Estos resultados se basan en la percepción del grupo de personas seleccionadas que constituyen nuestras fuentes primarias acerca del cumplimiento de los controles técnicos, requisitos administrativos de la norma e identificación y tratamiento de los riesgos. Así como también la utilización de las fuentes secundarias para el diseño de los elementos esenciales de un SGSI.

4.1 NIVEL DE MADUREZ ACTUAL PARA LA ADOPCIÓN DE SGSI SEGÚN NORMA ISO 27001:2022

Como parte de una auditoría interna inicial, ISO 27001 recomienda el empleo de un análisis de brechas GAP el cual nos determina el estado actual del San Services con respecto a los requisitos administrativos de ISO 27001. Este establece un punto de partida para la implementación del SGSI ya que identificamos que requisitos dentro de la norma tienen ya implementados en la empresa y en qué nivel se encuentran.

4.1.1 INFORME DE RECOLECCIÓN DE INFORMACIÓN PARA EL CUMPLIMIENTO DE REQUISITOS ADMINISTRATIVOS

El análisis de brechas a nivel de cumplimiento de requisitos en San Services se basó en los lineamientos detallados en la norma ISO 27001 en la cual refleja la percepción de colaboradores con puestos claves dentro del área (ver Tabla 6) en una encuesta sobre los 7 requisitos para la implementación de un SGSI (ver Tabla 5).

Tabla 5. Cantidad de preguntas en cuestionario de requisitos administrativos ISO 27001

Requisito	Cantidad de preguntas
Contexto de la organización	8
Liderazgo	9
Planificación	8
Soporte	11
Operación	11
Evaluación del desempeño	12
Mejora	4

Fuente: Elaboración propia

Tabla 6. Personal encuestado en San Services

Área	Puesto
DevOps	Sr. Site Reliability Engineer
Data base	DBA
Oracle Database Development	Senior Database Engineer
Business Systems	Manager
Frontend Development	Frontend lead
Microservicios	Team Lead

Fuente: Elaboración Propia

Para poder obtener datos para el análisis de brechas y determinación de los requisitos, se utilizó una encuesta dentro de la empresa llamada: Test de cumplimiento normativo 27001:2022 en San Services S. de R. L. (Ver anexo 1).

La encuesta se desarrolló de la siguiente manera:

1. Elaboración de preguntas objetivas y relacionadas con el cumplimiento de los requisitos de la estructura de la norma ISO 27001.
2. Diseño y elaboración del cuestionario en la herramienta Microsoft Forms.
3. Compartir el link de la encuesta de Microsoft Forms a la muestra seleccionada dentro de San Services por medio medios digitales como correo electrónico y WhatsApp, con límite de 5 días para la obtención de la repuestas.
4. Tabulación de los datos por medio de Microsoft Excel y posteriormente realizar análisis estadístico y elaboración de gráficos.

4.1.2 PRESENTACIÓN DE RESULTADOS Y SU ANÁLISIS

La evaluación de la encuesta sobre el cumplimento de requisitos se basó en preguntas dicotómicas con solo dos respuestas posibles Si/No.

A continuación, se presenta el procedimiento para determinar el porcentaje de cumplimiento:

1. Organizar los resultados, donde cada columna es una pregunta y cada fila las respuestas obtenidas.

2. Agregar una fila adicional al final donde esté el conteo de las respuestas de Si y No, de cada columna.
3. Realizar sumatorias por cada requisito
4. Cálculo de porcentajes de cumplimiento y brecha.

El nivel de madurez será en base el modelo por etapas CMMI de 0 a 5 niveles y será evaluado según el rango de porcentaje de la siguiente manera:

Tabla 7. Modelo de Madurez CMMI para cumplimiento de requisitos

Nivel	Nivel de madurez	Rango de porcentaje	Observación
0	Inexistente	0%	No se encuentran implementados.
1	Inicial	1-20%	Se han implementado bajo una necesidad específica y ocasional sin evidencia documentada.
2	Repetible	21-40%	Se han implementado y existe un procedimiento. Pero no están completamente documentados.
3	Definido	41-60%	Se han implementado y documentado totalmente en procedimientos, políticas y estándares.
4	Administrado	61-80%	Se mantiene control sobre su eficacia y rendimiento.
5	Optimizado	81-100%	Se han establecido acciones que han logrado su mejora continua y óptimo cumplimiento.

Fuente: (6 pasos para realizar el análisis de brechas según la ISO 27001, 2024)

En la Tabla 8 se presenta un resumen del grado de cumplimiento de acuerdo con el nivel de madurez para los 7 requisitos establecidos por la norma ISO 27001 en San Services. Cada requisito muestra el porcentaje de cumplimiento actual según la percepción de los encuestados, el nivel deseado por la empresa para la implementación del SGSI, el porcentaje de la brecha entre ambos y se define para cada uno el nivel de madurez identificado según los criterios de evaluación planteados anteriormente, donde según el rango de porcentaje determine el nivel de modelo de madurez, siendo el nivel inexistente el más bajo y optimizado el mas alto. El detalle de los resultados se puede ver en el Anexo 4.

Tabla 8. Resumen de los resultados del cumplimiento de requisitos

Requisitos	% Cumplimiento actual	% Brecha	% Deseado	Nivel de Madurez
1. Contexto de la organización	89.58	10.42	100	Optimizado
2. Liderazgo	88.89	11.11	100	Optimizado
3. Planificación	56.25	43.75	100	Definido
4. Soporte	74.24	25.76	100	Administrado
5.Operación	74.24	25.76	100	Administrado
6. Evaluación del desempeño	59.72	40.28	100	Definido
7. Mejora	79.17	20.83	100	Administrado

Fuente: Elaboración propia

En el gráfico 4 se puede apreciar como resumen los porcentajes de cada requisito en la cual San Services se debe de enfocar en la adopción del SGSI. El cumplimiento deseado para todos los requisitos es de 100%, y se refleja que los requisitos de Planificación y la Evaluación del Desempeño requieren más atención por tener un porcentaje de brecha más amplio según los resultados, pero que aun así en la evaluación cumplen al posicionarse en un nivel de madurez definido**,** lo cual determina que estos requisitos aun como alcanzables, y en los cuales la organización deberá de emprender acciones puntuales para disminuir el porcentaje de brecha**.** Mientras que según la percepción interna indica que el Liderazgo y Contexto de la Organización tiene un nivel de cumplimiento optimizado, siendo estos dos requisitos con mejor valoración con un porcentaje de brecha aceptable, lo cual siendo los primeros requisitos administrativos planteados por ISO 27001 encamina a San Services positivamente a una futura implementación del SGSI ya que entienden muy bien el contexto de la operación de la organización tanto interna como externamente al conocer conceptos como madurez de los recursos, cultura organizacional, formatos y sensibilidad de los activos de información así como comprensión del entorno y la competencia, además temas de regulación y entornos políticos y económicos. También se comprende la importancia y relevancia del alcance del SGSI, la definición de políticas de seguridad de la información, funciones y responsabilidades definidas y comunicadas claramente.

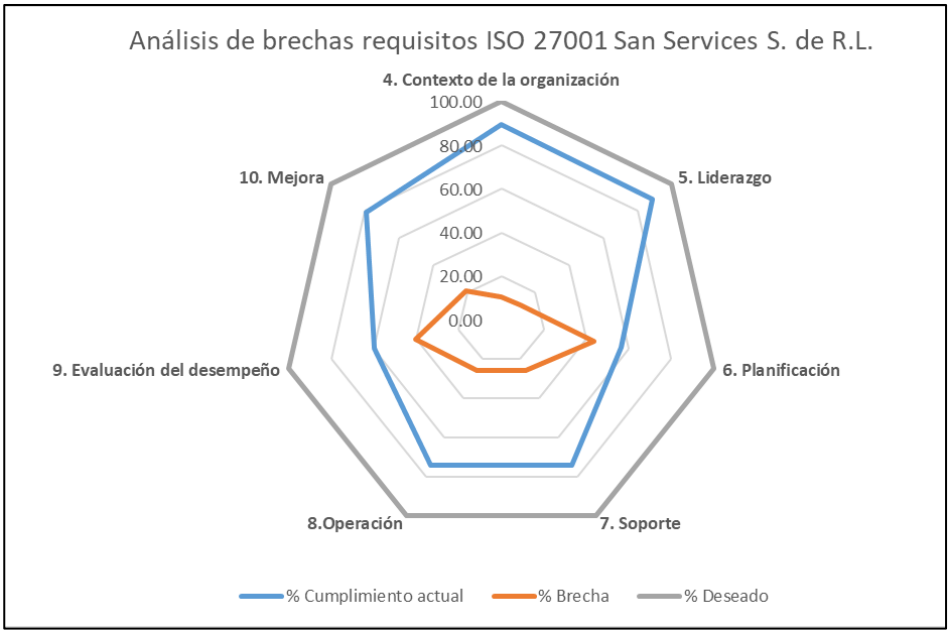

Gráfico 4. Gráfica de radar de resultados de análisis de brechas de requisitos ISO 27001 en San Services S. de R. L.
Fuente: (Elaboración propia).

Los otros requisitos como Operación, el cual exige una planificación y revisiones rigurosos para asegurar la efectiva implementación de controles y la gestión de riesgos, así como una evaluación adecuada de este requisito debe verificar la identificación y manejo de estos, el resultado de la investigación demuestra que San Services tienen un nivel administrado al contar con recursos para la evaluación y tratamiento de los riesgos. El requisito de Soporte también en los resultados contempló aspectos cruciales como la provisión de recursos, la competencia del personal, la concienciación y la comunicación, así como la documentación del SGSI. Por ultimo el requisito de Mejora el cual requiere que se implemente un enfoque sistemático para identificar y abordar oportunidades de mejora. Esto incluye la evaluación continua del desempeño del SGSI a través de auditorías internas, revisiones de gestión y el análisis de incidentes de seguridad, lo cual la percepción dé San Services es consciente de ello.

- **Contexto de la organización**

El porcentaje de cumplimiento para Contexto de la Organización es de 89.58% por lo tanto existe una brecha de 10.42%, por consiguiente, es el requisito mejor evaluado. La percepción de esta dimensión proyecta el entendimiento de los problemas internos y externos relevantes para la empresa, y comprende las necesidades y expectativas de las partes interesadas para la mejora de la seguridad de la información referente a reglamentos, requisitos legales y requisitos contractuales, además determina el alcance del SGSI. Uno de los aspectos a mejorar en este requisito es el proporcionar grupos de interés vinculados a la seguridad de la información para estar al tanto de las novedades y actualizaciones en el ámbito de la seguridad.

Gráfico 5. Cumplimiento requisito Contexto de la Organización
Fuente: (Elaboración propia).

- **Liderazgo**

Bajo este requisito que aborda diferentes incisos como liderazgo y compromiso, política y funciones, responsabilidades y autoridades de la organización. Este revela la percepción del compromiso de la alta dirección de San Services al tener una evaluación de 88.89% dejando una brecha de 11.11%. Lo cual indica que se percibe que las autoridades tienen la promesa de proveer los recursos materiales y humanos necesarios, delegando funciones además de establecer y comunicar el marco de políticas para cumplir los objetivos del SGSI. Es importante dejar claro los roles y responsabilidades de los involucrados en el SGI especialmente el liderazgo de los miembros de la auditoría interna el cual tendrá que realizar actividades importantes con la valoración de los riesgos y los oportunidades, establecimiento y comunicación de las políticas así como la asignación de recursos, responsabilidades y obligaciones adecuadas.

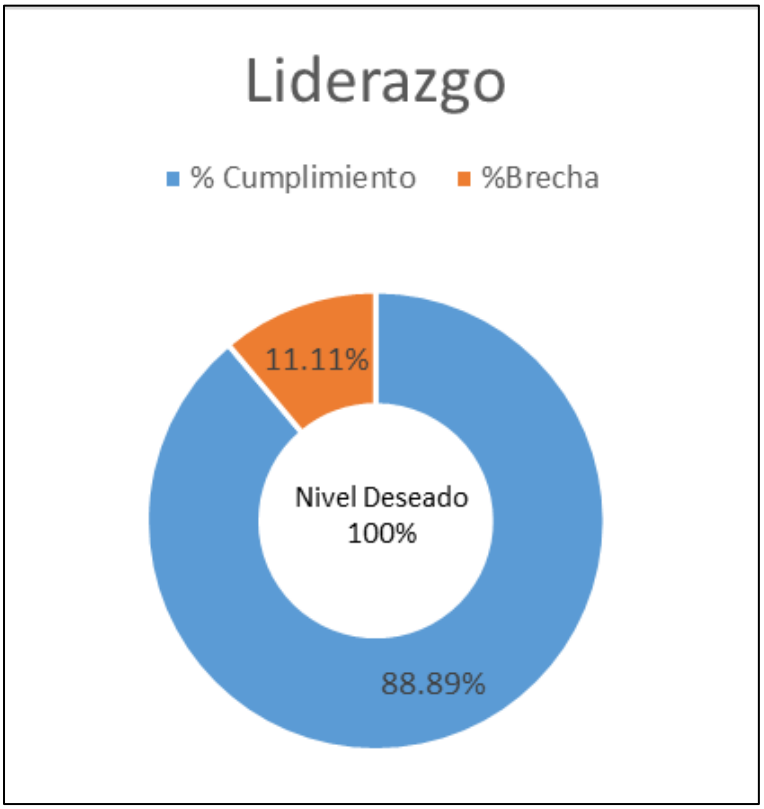

Gráfico 6. Cumplimiento requisito Liderazgo
Fuente: (Elaboración propia).

- **Planificación**

El grado de cumplimiento de este requisito es el que menos desempeño tiene, con un 56.25% de cumplimiento con una notable diferencia de brecha de 43.75% lo cual se traduce de la deficiencia en la elaboración de planes y procesos de evaluación de riesgos, como la falta de aplicabilidad y documentación de estos. Sin duda esta dimensión es el núcleo de un SGSI eficaz ya que la identificación y tratamiento de los riesgos garantiza que las actividades y los procesos operativos de una organización se desarrollen de forma eficiente. Y en San Services según la brecha existente demuestra que esta categoría debe ser foco de atención ya que se deben de disponer de un plan de acción detallado que se supervise de forma alineada y se apoye en revisiones periódicas de las gestiones de riesgos y que en esta investigación se apoyan en varias herramientas como la metodología MAGERIT/PILAR y la matriz de riesgos como tal.

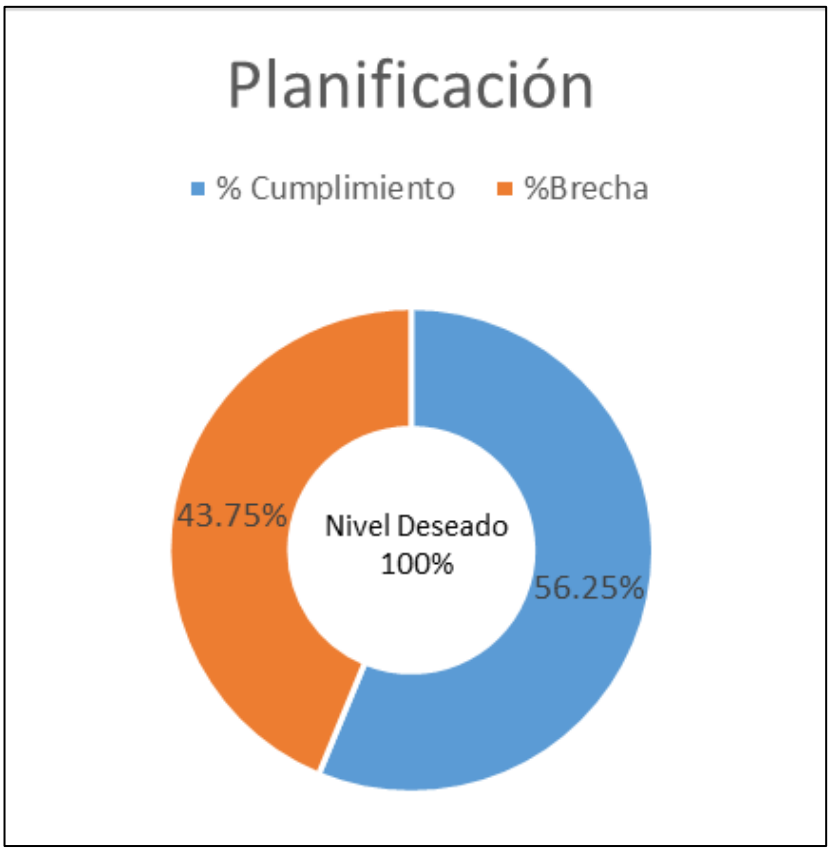

Gráfico 7. Cumplimiento requisito Planificación
Fuente: (Elaboración propia).

- **Soporte**

Existe una buena percepción de las capacidades y competencias de las personas de frente al desempeño del SGSI, además existe una conciencia del establecimiento de una política y comunicación de seguridad de la información, con un 74.24% de cumplimiento y un 25.76% de brecha queda como un requisito administrado según la evaluación del modelo de madurez. Sin embargo, se deben de fortalecer los puntos débiles según los resultados de la encuesta como el tener debidamente actualizadas las competencias del personal y el poder contar con la información crítica debidamente documentada, protegida bajo control de cambios y la cual pueda ser requerida por San Servides para el SGSI.

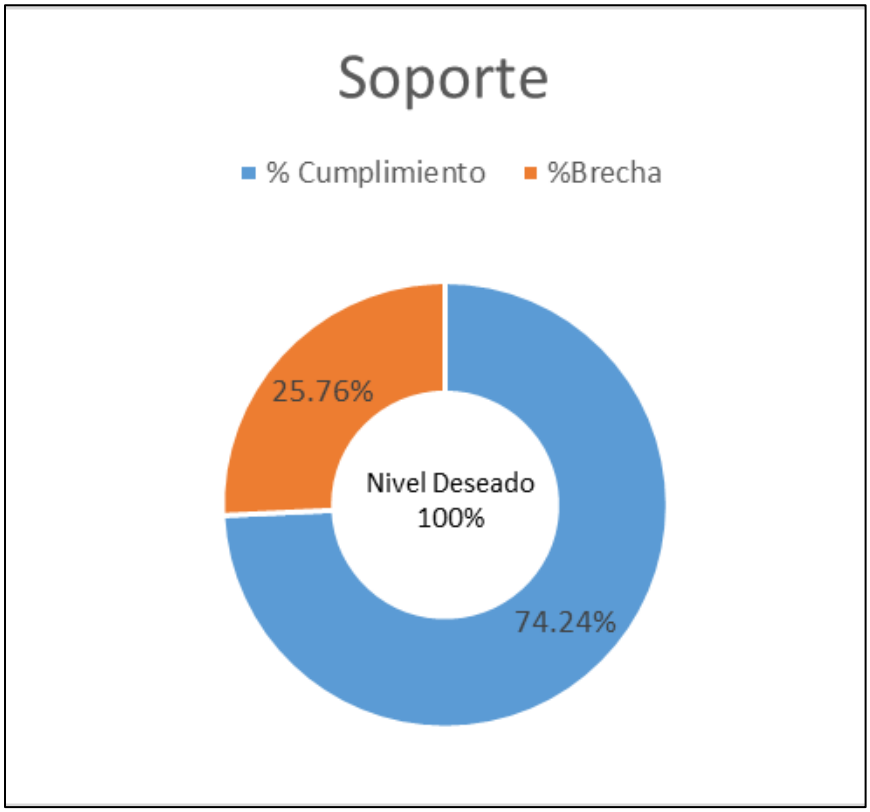

Gráfico 8. Cumplimiento requisito Soporte
Fuente: (Elaboración propia).

- **Operación**

En esta dimensión tiene exactamente el mismo resultado del requisito de Soporte, con un 74.24% de cumplimiento y un 25.76% de brecha, este apartado dentro del ISO 27001 hace mucha énfasis en la gestión y evaluación de los riesgos así como el control, planificación y documentación de los cambios, por lo cual hay ciertos indicios dentro de San Services de estarlo haciendo bien, sin embargo no hay una documentación oficial de dichos procedimientos ya que todo se basa según la apreciación de los encuestados, dicho esto San Services debe documentar las pruebas en la cual demuestren que los procesos se han llevado a cabo según lo planificado y además se debe de fortalecer un plan para determinar las necesidades de cambios y mejoras en el SGSI de igual manera asegurar que se lleven a cabo en su implantación.

Gráfico 9. Cumplimiento requisito Operación
Fuente: (Elaboración propia).

- **Evaluación del desempeño**

Puntualmente el requisito se centra en el seguimiento, medición, análisis y evaluación del desempeño tanto de los procesos como los controles, a su vez indica quien cuando y como se deben de hacer, con un 59.72% de cumplimiento y una brecha de 40.28% existe una oportunidad de mejora al establecer un procedimiento documentado de la evaluación del SGSI por medio de auditorías internas una vez implementado. Junto con el requisito de Planificación este tiene la mayor brecha comparado con los demás requisitos administrativos, puntualmente refleja poner más énfasis en la documentación antes mencionada en la cual debe de incluir los resultados del seguimiento y la medición del SGSI y los cuales deben de comunicarse a la alta dirección. También se deben de establecer los procesos adecuados para las no conformidades y acciones correctivas del SGSI.

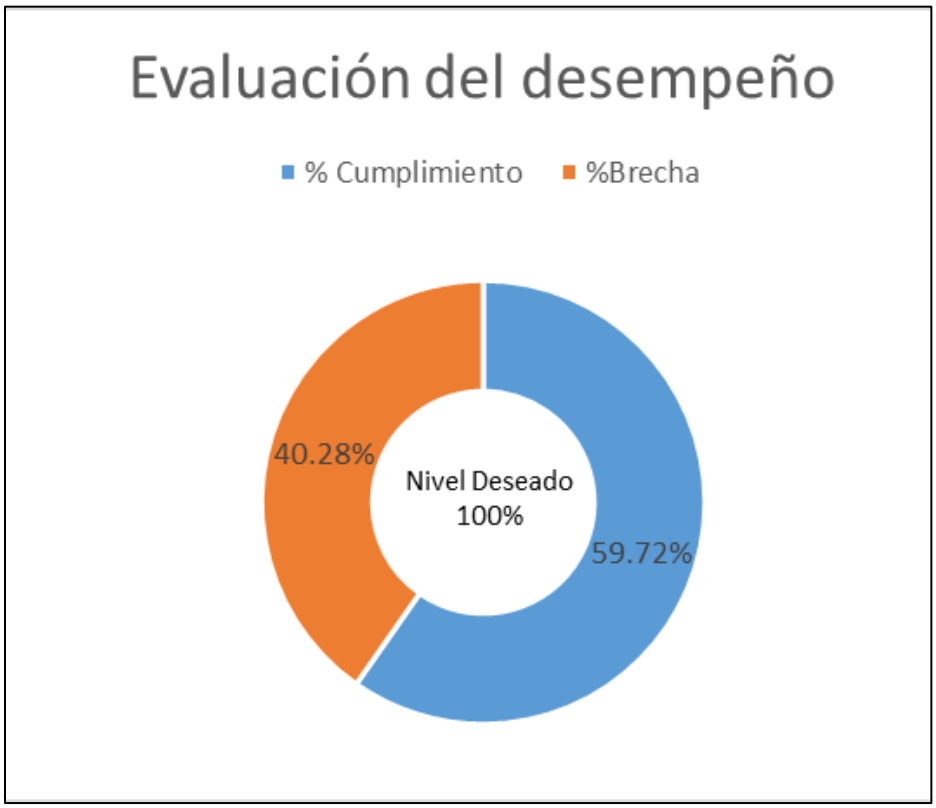

Gráfico 10. Cumplimiento requisito Evaluación del desempeño
Fuente: (Elaboración propia).

- **Mejora**

En este requisito encontramos un nivel de cumplimiento de 79.17% teniendo así una brecha de 20.83% del nivel deseado. San Services debe de prepararse para un reforzamiento de este requerimiento como parte del último ciclo del PDCA, ya que es muy importante el actuar en las acciones correctivas y la mejora continua del SGSI, así como revisar y determinar las causas de las no conformidades. Sabemos que el objetivo clave del SGSI es reducir la probabilidad de que se produzcan sucesos relacionados con la seguridad de la información y mitigar su impacto, sin embargo, ningún SGSI es infalible, pero este se puede fortalecer con el tiempo y a medida se realicen las mejoras señaladas y se apliquen técnicas para realizar medidas preventivas y correctivas eficaces para identificar causas raíz de los problemas como por ejemplo los "cinco porques".

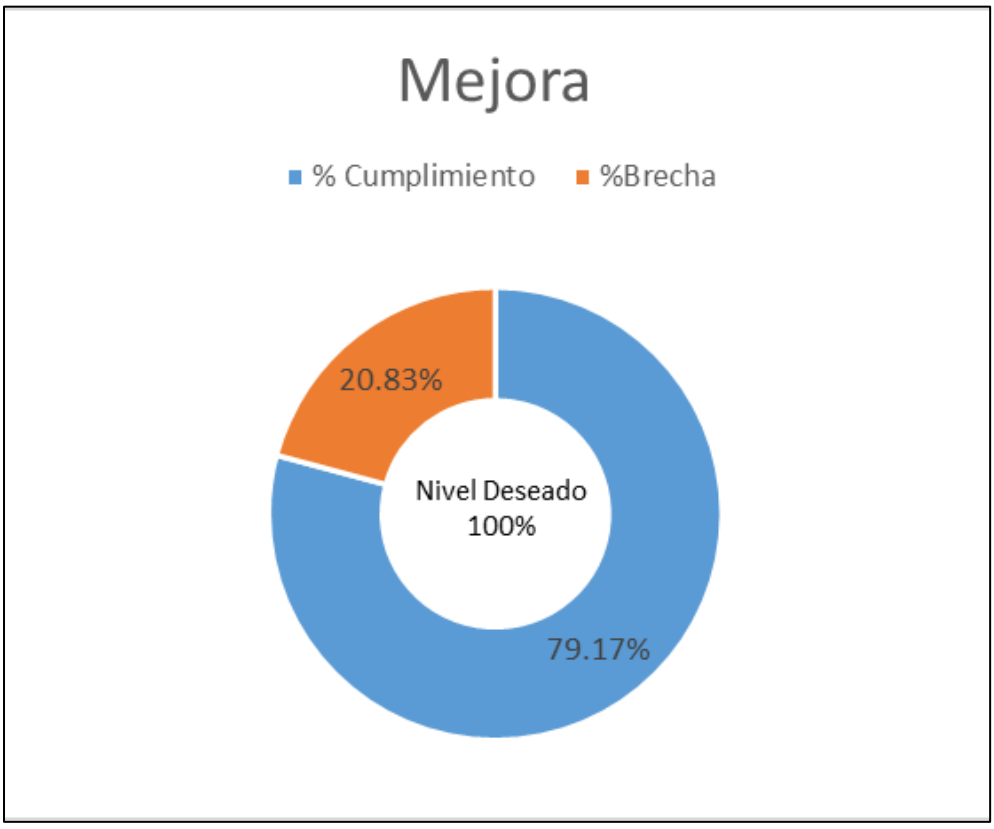

Gráfico 11. Cumplimiento requisito Mejora
Fuente: (Elaboración propia).

4.2 NIVEL DE MADUREZ ACTUAL PARA LOS CONTROLES TÉCNICOS DEL ANEXO A DE LA NORMA ISO 27001:2022

Tal como se realizó en el análisis de los requisitos administrativos también se requirió un análisis de brechas de las 4 categorías del anexo A de los controles planteados por el documento de ISO 271001 en su versión 2022 (ver Figura 9). Este se desarrolló por medio de una encuesta a los mismos colaboradores para determinar el nivel de madurez actual.

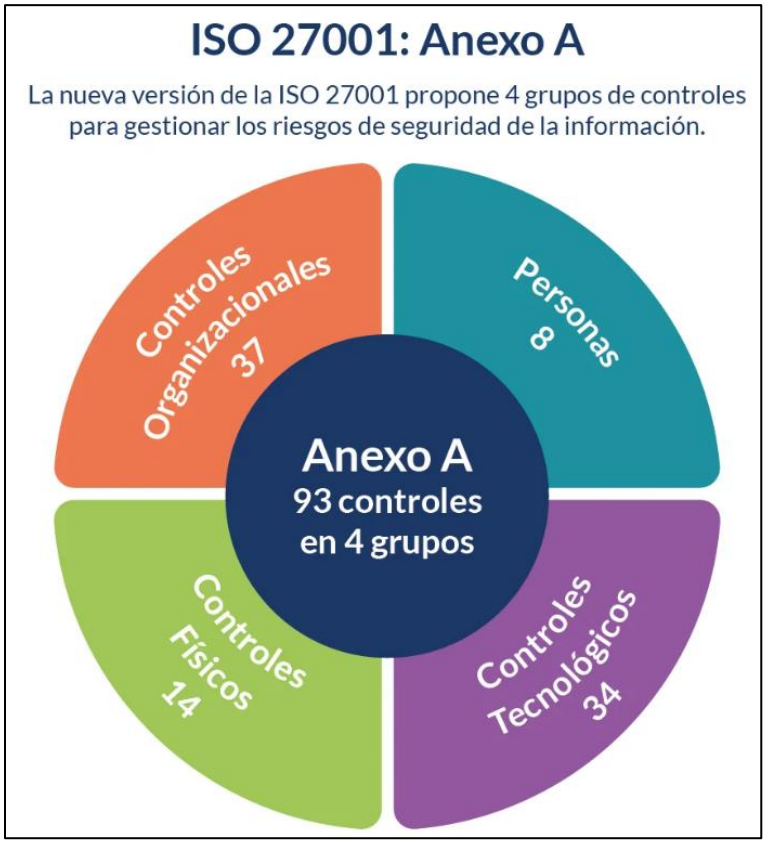

Figura 9. Cantidad de controles en la norma ISO versión 2022.
Fuente: (Elaboración propia).

4.2.1 INFORME DE RECOLECCIÓN DE INFORMACIÓN PARA EL CUMPLIMIENTO DE REQUISITOS

Para poder obtener datos para el análisis de brechas y determinación de los controles se utilizó una encuesta dentro de la empresa llamada: Test de cumplimiento de controles Anexo A ISO 27001:2022 en San Services S. de R. L. (Ver anexo 2).

La encuesta se desarrolló de la siguiente manera:

1. Elaboración de preguntas objetivas y relacionadas con el cumplimiento de los controles en anexo A de su versión 2022.
2. Diseño y elaboración del cuestionario en la herramienta Microsoft Forms.
3. Compartir el link de la encuesta de Microsoft Forms a la muestra seleccionada dentro de San Services por medio medios digitales como correo electrónico y WhatsApp, con límite de 5 días para la obtención de la repuestas.
4. Tabulación de los datos por medio de Microsoft Excel y posteriormente realizar análisis estadístico y elaboración de gráficos.

Tabla 9. Cantidad de preguntas en cuestionario de controles ISO 27001:2022

Control	Cantidad de preguntas
Controles Organizacionales	37
Controles de personas	8
Controles Físicos	14
Controles Tecnológicos	34

Fuente: Elaboración propia

Para la realización del GAP, la recomendación de ISO 27001 es utilizar un modelo de madurez con esquemas de 5 niveles para la evaluación del cumplimiento de controles (Ver Tabla 10), este modelo comúnmente es empleado como herramienta para la gestión de servicios de TI y que evalúa con mayor efectividad los procesos de gestión con respecto a los controles internos. En esta investigación decidimos también utilizar el modelo de madurez CMMI.

Tabla 10. Niveles de madurez de referencia para los controles

Nivel	Nivel de madurez	Observación
1	Inicial	El control es impredecible, es reactivo y pobremente controlado.
2	Administrado	El control es reactivo y se caracteriza por su aplicación a proyectos.

3	Definido	El control es proactivo y se ve a nivel de la organización.
4	Administrado Cuantitativamente	El control es medido y controlado.
5	Optimizado	El control se enfoca en la mejora continua.

Fuente: Elaboración propia

Para evitar crear confusiones en las respuestas se aplicó en esta encuesta una escala de likert con los mismos niveles de madurez del modelo seleccionado, el cual se puede observar en la Tabla 11.

Tabla 11. Complemento de niveles de madurez con escala de likert.

Nivel	Nivel de madurez	Likert	Valor
1	Inicial	Totalmente en desacuerdo	1
2	Administrado	En desacuerdo	2
3	Definido	Neutral	3
4	Administrado Cuantitativamente	De acuerdo	4
5	Optimizado	Totalmente de acuerdo	5

Fuente: Elaboración propia

Por lo tanto, se consideró establecer los resultados de la siguiente manera según la escala:

- Los controles “Cumple” serán aquellos que estén dentro de Totalmente de acuerdo y De acuerdo.
- Los controles “Cumple Parcial” serán aquellos que sea igual a “Neutral”
- Los controles “No Cumple” serán aquellos que estén dentro de Totalmente desacuerdo y Desacuerdo.

A continuación, se presente el cuadro resumen de los resultados obtenidos:

Tabla 12. Resultados de la evaluación de los controles del Anexo A ISO 27001:2022

Controles	%Cumplimiento	%Cumplimiento Parcial	%No cumplimiento
Organizativos	70.27	16.22	13.51
De Personas	89.58	4.17	6.25
Físicos	82.14	14.29	3.57
Tecnológicos	81.86	10.29	7.84

Fuente: Elaboración propia

Los controles de Personas tienen una percepción de mejor desempeño con un 89.58% de cumplimiento dentro de San Services, esto es debido a que actualmente existes políticas y procesos disciplinarios claros que se divulgan en la empresa.

Mientras tanto los controles Organizativos tienen la evaluación más baja con un 13.51% de no complimiento en el cual se deberá reforzar cada ítem tales como políticas de seguridad de la información, roles y responsabilidades, inventario de información y devolución de activos.

En el Gráfico 12 podemos observar como una representación de resumen de columnas 100% apiladas la diferencia notable del cumplimiento de los controles según la apreciación interna.

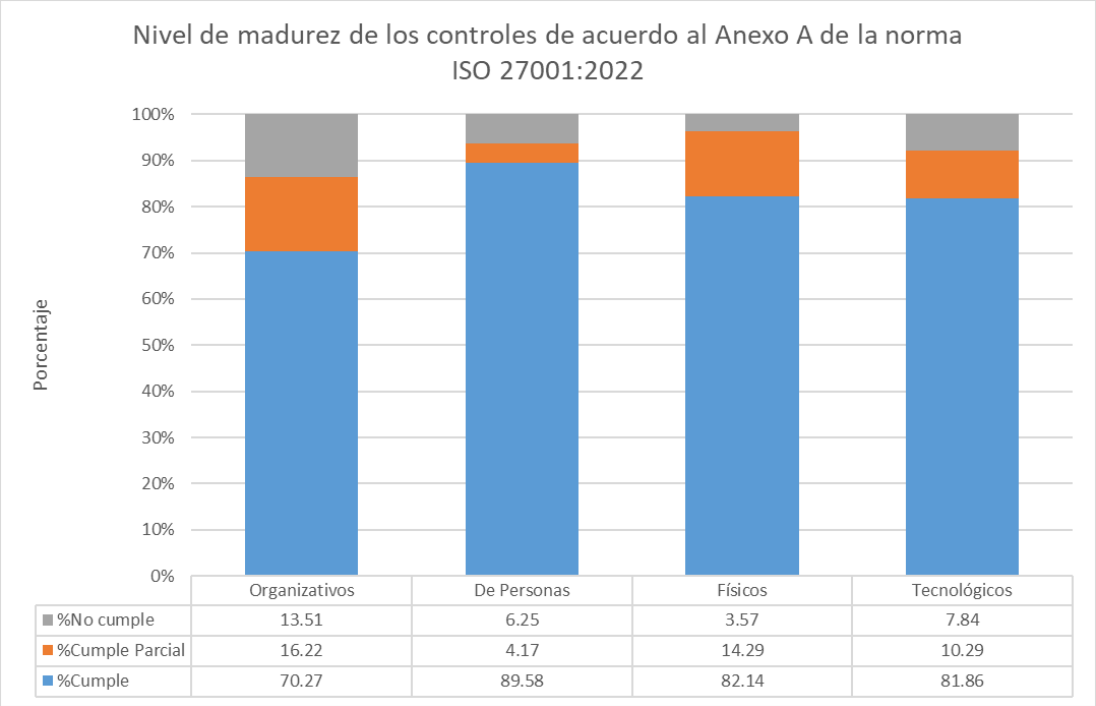

Gráfico 12. Nivel de madurez de los controles del Anexo A ISO 27001:2022
Fuente: (Elaboración propia).

A continuación, se presentan las gráficas de los resultados de las evaluaciones de cada uno de los 4 grupos de controles:

- **Controles Organizativos**

Es el grupo de controles con mayor puntación de no cumplimiento con un 2.25% de Totalmente en desacuerdo y 11.26% desacuerdo, además tiene un porcentaje neutralidad importante con un 16.22%; Existe una percepción en la cual los controles organizativos que tratan puntualmente la actitud de la organización de frente a protección de la información por medio de políticas, procedimientos y comportamientos individuales necesitan mayor atención, especialmente la publicación y comunicación de las políticas de seguridad a todo el personal relevante, así como su revisión periódica para verificar si ocurrieron cambios significativos, también se necesita reforzar la instalación de vías de comunicación con organizaciones especializadas en seguridad de la información donde haya un aviso sobre amenazas y vulnerabilidades de manera expedita, por último se necesita integrar conceptos de seguridad de la información en la gestión de proyectos en la organización.

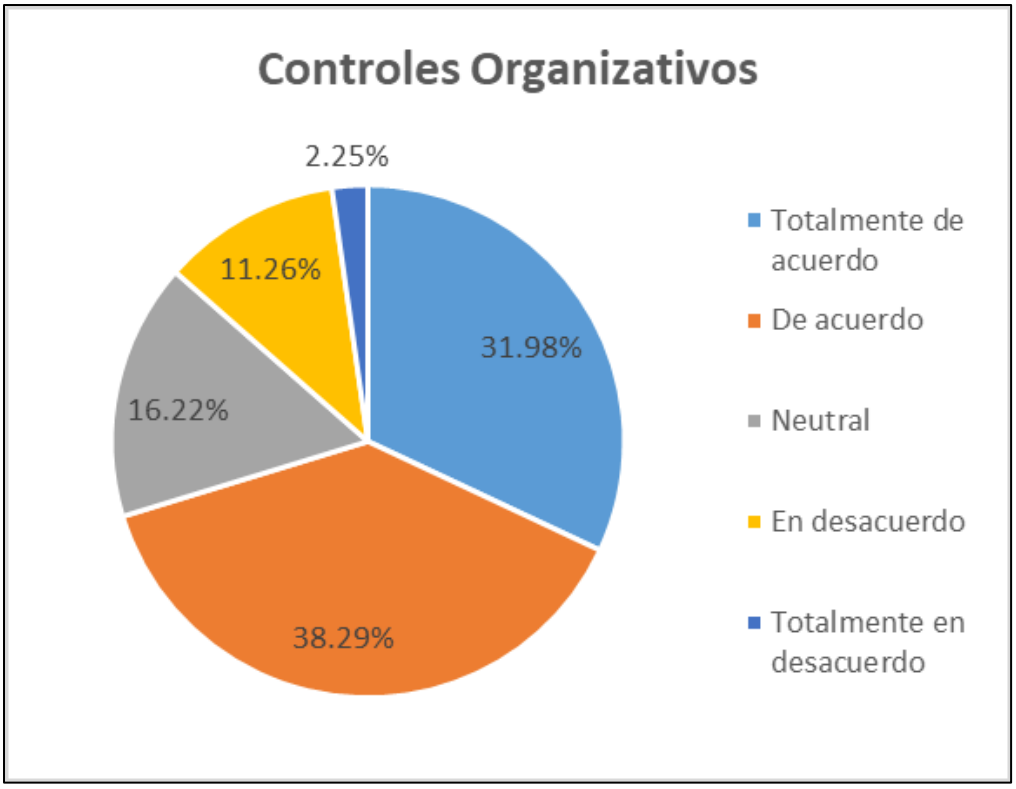

Gráfico 13. Resultados de la evaluación de Controles Organizativos
Fuente: (Elaboración propia).

- **Controles de Personas**

Es el grupo de controles con mejor puntuación teniendo un porcentaje de 41.67% de Totalmente de acuerdo y 47.92% De acuerdo. San Services demuestra que estos controles orientados a los colaboradores tienen buena interacción con la seguridad de la información, se tienen definidos los procesos disciplinarios, términos y condiciones sobre el empleo, así como el sentido de responsabilidad y sensibilización del uso de los datos por parte del personal. Los controles que destacan en la evaluación son donde la organización identifica, documenta y comunica los acuerdos de confidencialidad y no divulgación de la información sensible. También tienen buena calificación aquellos controles donde indican que San Services provee todas las medidas de seguridad para el personal que trabaja de manera remota y en la cual protege la información que se accede tanto dentro o fuera la organización, por ultimo se identifica que existen canales apropiados para que el personal informe sonde eventos de seguridad de la información.

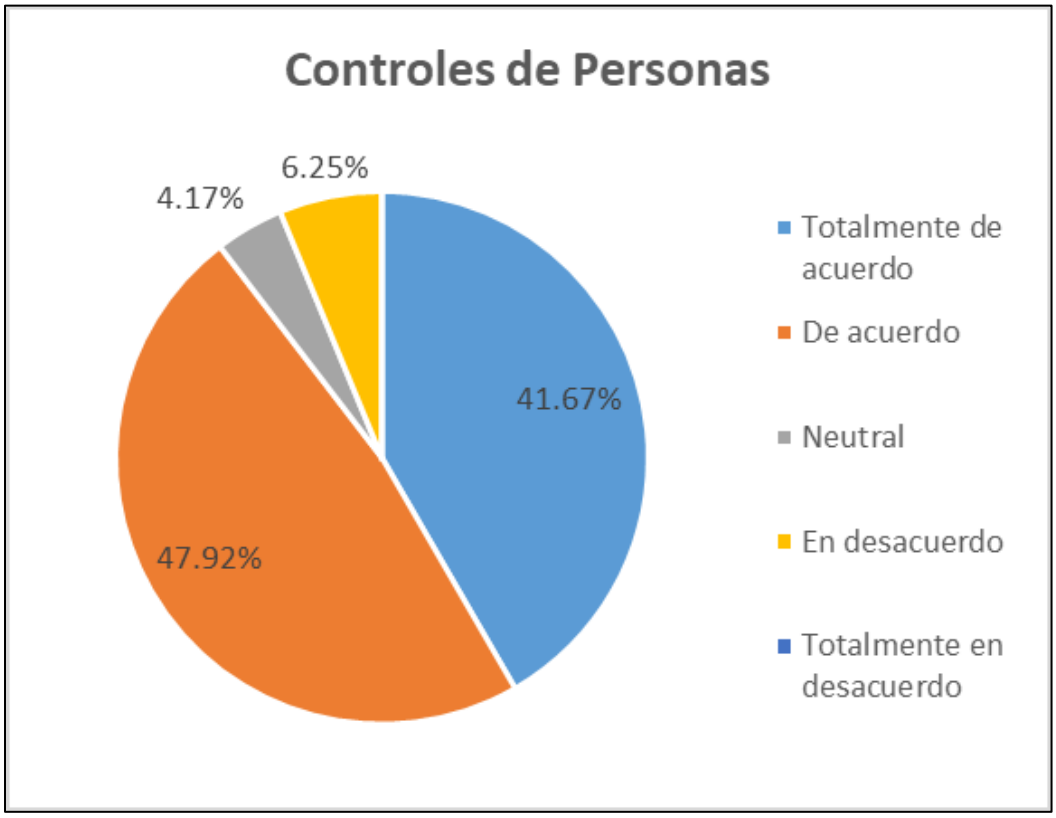

Gráfico 14. Resultados de la evaluación de los controles de Personas.
Fuente: (Elaboración propia).

- **Controles de Físicos**

Es el segundo grupo de controles con mejor puntuación de cumplimiento con un 46.43% Totalmente de acuerdo y un 35.71% De acuerdo. Existe una buena sensación sobre la seguridad de los activos tangibles en controles esenciales tales como sistemas de entrada al personal apropiados, definición de procesos para la disponibilidad de los activos y política claras de escritorio para garantizar la preservación de la confidencialidad de los datos. Destacan los controles relacionados con la protección de áreas seguras por medio de mecanismos de entrada y puntos de acceso apropiados, así como el monitoreo continuo para evitar el acceso no autorizado a estos, también destaca que San Services tiene protección contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.

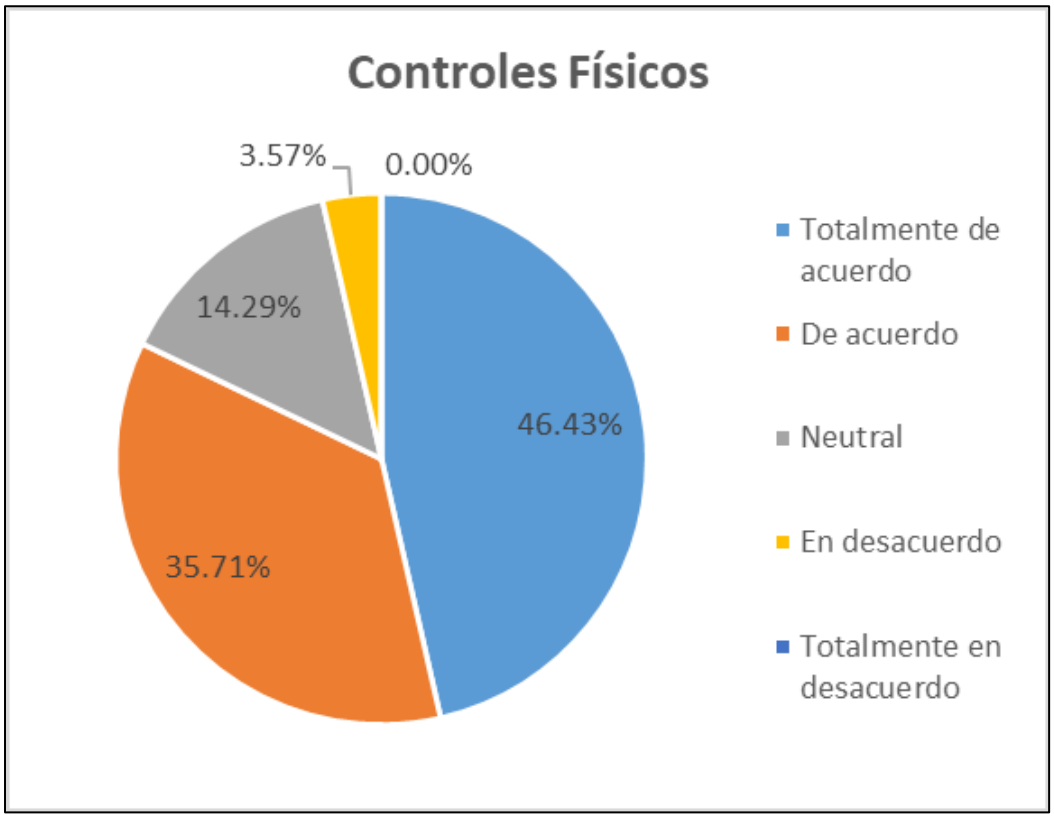

Gráfico 15. Resultados de la evaluación de los Controles Físicos.
Fuente: (Elaboración propia).

- **Controles Tecnológicos**

Este grupo de controles es de los más numerosos en el Anexo A del ISO 27001 con una cantidad de 34, de igual manera en la actualidad tiene un buen desempeño dentro de San Services con un 33.82% de Totalmente de acuerdo y un 48.04% De acuerdo, los controles son bien puntuales en cuanto a las regulaciones y procedimientos tecnológicos que deben de cumplir tanto la configuración, administración y acceso para salvaguardar los datos. Destacan la protección de los datos por medio de redes, sistemas y aplicaciones monitoreadas para detectar comportamientos anómalos, así como también segmentos de red separando ambientes de desarrollo, pruebas y producción, así como sistemas de servicios de información y usuarios. También un control con buena calificación es que determina que San Services posee procedimientos de gestión de cambios para la instalación de procesamiento de información.

Es un gran avance para la organización el cumplir con la mayoría de los controles de este grupo ya que de lo contrario requeriría de una inversión económica fuerte para la implementación del SGSI.

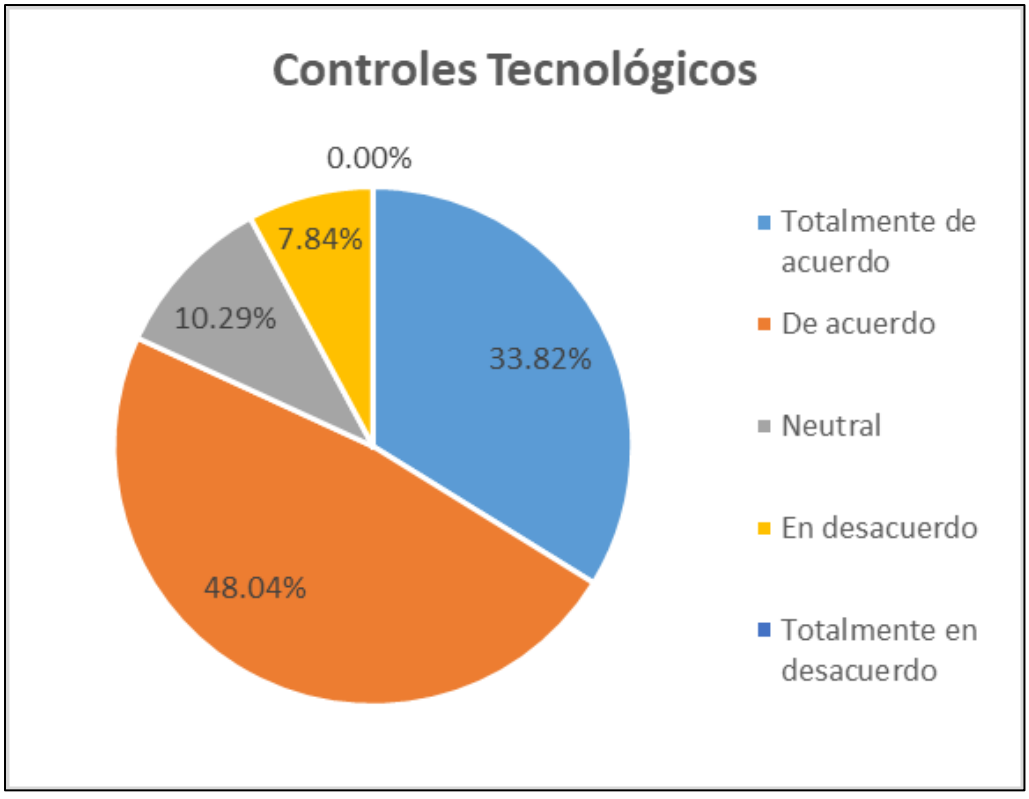

Gráfico 16. Resultados de la evaluación de los Controles Tecnológicos
Fuente: (Elaboración propia).

4.3 ALCANCE DEL SGSI

El documento del alcance de un SGSI es fundamental para proporcionar claridad y enfoque en la gestión de la seguridad de la información dentro de una organización. Este documento define de manera precisa qué áreas, procesos, sistemas, servicios y activos de información están cubiertos por el SGSI. Al establecer un límite claro, permite a San Services enfocar sus esfuerzos y recursos en las áreas más críticas, asegurando que los riesgos específicos sean identificados y mitigados adecuadamente. Además, un alcance bien definido facilita la gestión eficiente de los riesgos, optimiza el uso de recursos y garantiza que las medidas de seguridad sean efectivas y pertinentes para las necesidades específicas de la organización.

Asimismo, el documento del alcance es crucial para el cumplimiento normativo y la mejora continua del SGSI. Al delinear claramente el ámbito de aplicación, San Services puede asegurar el cumplimiento de requisitos legales, reglamentarios y contractuales, evitando sanciones y manteniendo la confianza de clientes y socios. También facilita la monitorización y revisión continua del SGSI, permitiendo identificar áreas de mejora y ajustar las políticas y controles según sea necesario. Este enfoque estructurado y bien definido en el alcance del SGSI no solo apoya la alineación con los objetivos estratégicos de la organización, sino que también simplifica el proceso de auditoría y certificación, proporcionando una base sólida para evaluar la conformidad y efectividad del sistema de gestión de seguridad de la información.

A continuación, se presentan las secciones diseñadas y elaboradas en el documento del alcance del SGSI para San Services y el cual se puede ver más a detalle en el Anexo 6.

1. OBJETIVO Y ALCANCE

El objetivo del alcance del SGSI es definir los límites y la aplicabilidad del sistema dentro del área de TI en San Services S. de R.L., estableciendo las responsabilidades, procesos, activos y controles necesarios para proteger la información crítica de la empresa, socios, proveedores y clientes.

Este documento se aplica a toda la documentación y actividades dentro de SGSI.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2022.

3. DEFINICIÓN DEL ALCANCE DEL SGSI

San Services necesita definir los límites del SGSI para decidir qué información quiere proteger.

El SGSI se aplicará específicamente al área de TI de San Services, abarcando todos los sistemas, redes, aplicaciones, datos y personal involucrado en el desarrollo, mantenimiento y soporte de software. Esto incluye:

- Infraestructura de TI: servidores, estaciones de trabajo, dispositivos de red (firewalls, switches, routers), almacenamiento y equipos de respaldo.
- Aplicaciones: software en desarrollo, aplicaciones en producción, sistemas de control de versiones, herramientas de desarrollo de código y pruebas.
- Datos: bases de datos, repositorios de código, documentos de diseño y especificaciones, información de clientes y proyectos.
- Comunicación: sistemas de correo electrónico, mensajería interna, videoconferencias y otras formas de comunicación dentro del área de TI.
- Personal: todos los empleados que trabajen en el área de TI o manejen información crítica.

También se aplica para los activos de información críticos como:

- Código fuente: de todas las aplicaciones en desarrollo y en producción.
- Documentación: proyectos, especificaciones técnicas, manuales de usuario y documentación administrativa.
- Configuraciones: de sistemas, redes y aplicaciones.
- Registros y logs: actividades del sistema, accesos y eventos de seguridad.

4. EXCLUSIONES DEL ALCANCE

El SGSI se aplicará exclusivamente al área de TI, por lo tanto, queda excluido todo tipo de proceso, registro de sistema de gestión etc., de otras áreas ajenas a TI.

A su vez queda excluido todo equipo personal de los colaboradores como laptops, teléfonos móviles, tabletas y otros dispositivos que nos son propiedad de la empresa y que no están registrados en la infraestructura de TI de San Services.

También serán excluidos todos los servicios que no estén bajo el control directo de San Services, tales como:

- Servicios en la nube gestionados por terceros.
- Sistemas que pertenecen a clientes o proveedores, que no son gestionados directamente por San Services.
- Software y herramientas que no hayan sido aprobadas por el área de TI de San Services y el cual no forme parte del inventario oficial de activos.

5. LÍMITES DEL SGSI

- Ubicaciones físicas: oficinas y centros de datos donde el equipo de TI realiza sus actividades.
- Tecnologías: hardware y software utilizados y administrados por el área de TI.
- Procesos de TI: desarrollo de software, pruebas, implementación, mantenimiento, soporte técnico, gestión de cambios, gestión de incidentes y proyectos.

6. RESPONSABLES

- Jefe de operaciones de TI.
- Equipo de personas del área de Seguridad de la Información.
- Equipo de personas de TI.

4.4 RIESGOS IDENTIFICADOS CON METODOLOGÍA MAGERIT/PILAR

Con el fin de identificar todos los posibles riesgos que pueden afectar a todos los activos esenciales de San Services S. de R.L. y como parte esencial del diseño en la sección de planificación un SGSI, decidimos hacer uso de la metodología MAGERIT a través de su herramienta de software PILAR RM. Este permite agilizar este tipo de análisis, y crear resultados que faciliten la evaluación de los riesgos a los que los activos están expuestos, especialmente aquellos riesgos sutiles que a simple vista podrían pasar desapercibidos.

Como primer paso, identificamos todos aquellos activos esenciales para las operaciones diarias de la organización, ya que PILAR hace distinción entre los tipos de activos que se evaluaran. Observamos que hay activos orientados a elementos abstractos, como información manejada por la organización, o servicios que se gestionan internamente. Asimismo, aquellos activos físicos que son usados por los empleados tienen su propia categoría, subdivididas de acuerdo con el tipo de funcionalidad que proveen dentro de la organización. Los servicios externos que la organización ha contratado también tienen su apartado dentro de este listado, así como también lo tienen los activos o recursos humanos, los cuales son tan importantes como el resto de los elementos previamente mencionados. La lista de estos activos se puede apreciar en la Figura 10.

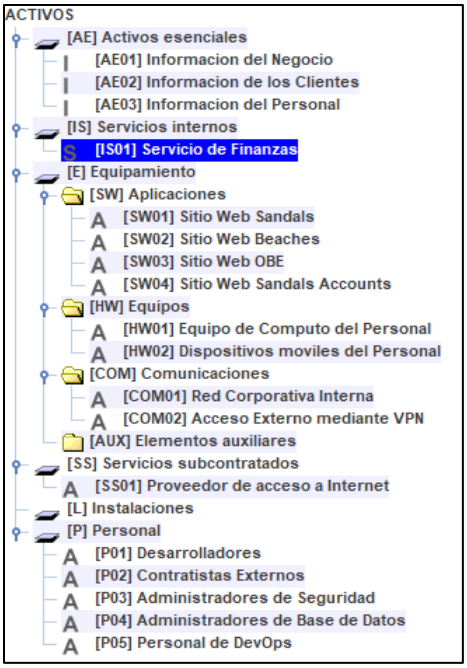

Figura 10. Activos esenciales de San Services listados en PILAR RM.
Fuente: (Elaboración propia).

Luego de haber listado los activos esenciales de la organización, es necesario hacer una evaluación de estos activos bajo ciertos casos que PILAR ofrece. No todos los casos aplican para todos los activos, pero es recomendable evaluar tantos como sean necesario a fin de proveerle a PILAR toda la información que necesita para la correcta identificación de riesgos, amenazas y posibles salvaguardas. En el caso de PILAR RM, son siete casos los que se evalúan, cada uno con criterios de valoración que permiten dar una puntuación que va desde cero a diez, con cero representando un valor muy bajo para la organización en términos de lo esencial que puede ser para la misma, y diez siendo el valor más alto, representando aquel activo que es casi que la vida de la organización. Los casos por evaluar son los siguientes, y entre paréntesis el identificador que se utiliza para su respectiva columna:

- Disponibilidad (D)
- Integridad de los datos (I)
- Confidencialidad de los datos (C)
- Autenticidad de los usuarios y de la información (A)
- Trazabilidad del servicio y de los datos (T)

- Valor (en términos de patrimonio corporativo) (V)
- Datos personales (DP)

Al evaluar cada uno de estos casos, se debe de seleccionar aquellos criterios de valoración que apliquen, escogiendo el nivel adecuado según el valor del activo dentro de la organización. Los criterios de valoración son los siguientes:

- Tiempo de recuperación del servicio
- Información personal
- Obligaciones legales
- Seguridad
- Intereses comerciales / económicos
- Interrupción del servicio
- Orden publico
- Operaciones
- Administración y Gestión
- Pérdida de confianza (reputación)
- Persecución de delitos
- Seguridad de las personas
- Datos personales
- Información clasificada

Finalmente, para aquellos casos no evaluados o que no apliquen, PILAR da la opción de marcarlos como “No aplica”, lo cual deja la columna en blanco sin ningún valor. El resultado de las valoraciones de los activos de la organización se puede apreciar en la Figura 11.

activo	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS							
[AE] Activos esenciales							
[AE01] Informacion del Negocio	[9]	[9]	[9]	[9]	[9]		[6]
[AE02] Informacion de los Clientes	[9]	[9]	[9]	[9]	[9]		[8]
[AE03] Informacion del Personal	[7]	[7]	[7]	[7]	[7]		[6]
[IS] Servicios internos							
[IS01] Servicio de Finanzas	[7]	[7]	[9]	[7]	[9]		[6]
[E] Equipamiento							
[SW] Aplicaciones							
[SW01] Sitio Web Sandals	[9]	[7]		[7]		[9]	
[SW02] Sitio Web Beaches	[9]	[7]		[7]		[9]	
[SW03] Sitio Web OBE	[9]	[9]	[9]	[9]	[9]	[9]	[6]
[SW04] Sitio Web Sandals Accounts	[5]	[7]	[9]	[7]	[7]	[7]	[6]
[HW] Equipos							
[HW01] Equipo de Computo del Personal	[3]						
[HW02] Dispositivos moviles del Personal	[3]						
[COM] Comunicaciones							
[COM01] Red Corporativa Interna	[7]	[7]	[7]				
[COM02] Acceso Externo mediante VPN	[5]	[5]	[5]				
[AUX] Elementos auxiliares							
[SS] Servicios subcontratados							
[SS01] Proveedor de acceso a Internet	[7]	[5]	[7]				
[L] Instalaciones							
[P] Personal							
[P01] Desarrolladores	[5]						
[P02] Contratistas Externos	[4]						
[P03] Administradores de Seguridad	[5]						
[P04] Administradores de Base de Datos	[5]						
[P05] Personal de DevOps	[5]						

Figura 11. Valoración de los activos en PILAR.
Fuente: (Elaboración propia).

Se puede ver que los activos de tipo abstracto son los que más casos tienen evaluados, y esto es porque son los que más valor poseen en este caso para la organización. Por otro lado, los activos de tipo humano solo fueron valorados en términos de la disponibilidad, al igual que el equipo de cómputo del que hacen uso. Podrán observar también que los activos más esenciales para San Services son aquellos relacionados a la información que se maneja, así como de sus sitios webs por donde realiza la venta de sus servicios.

Al estar valorados todos estos activos, y con sus puntajes asignados, PILAR puede automáticamente proveer una lista de amenazas para cada uno de ellos, como podemos ver en la Figura 12 hasta la Figura 18, donde PILAR enlista una serie de amenazas de varios indoles, algunas con mayor probabilidad y capacidad de destrucción que otras. Dentro de PILAR, existen cinco tipos de amenazas, las cuales son:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados

- [A] Ataques deliberados
- [PR] Riesgos de privacidad

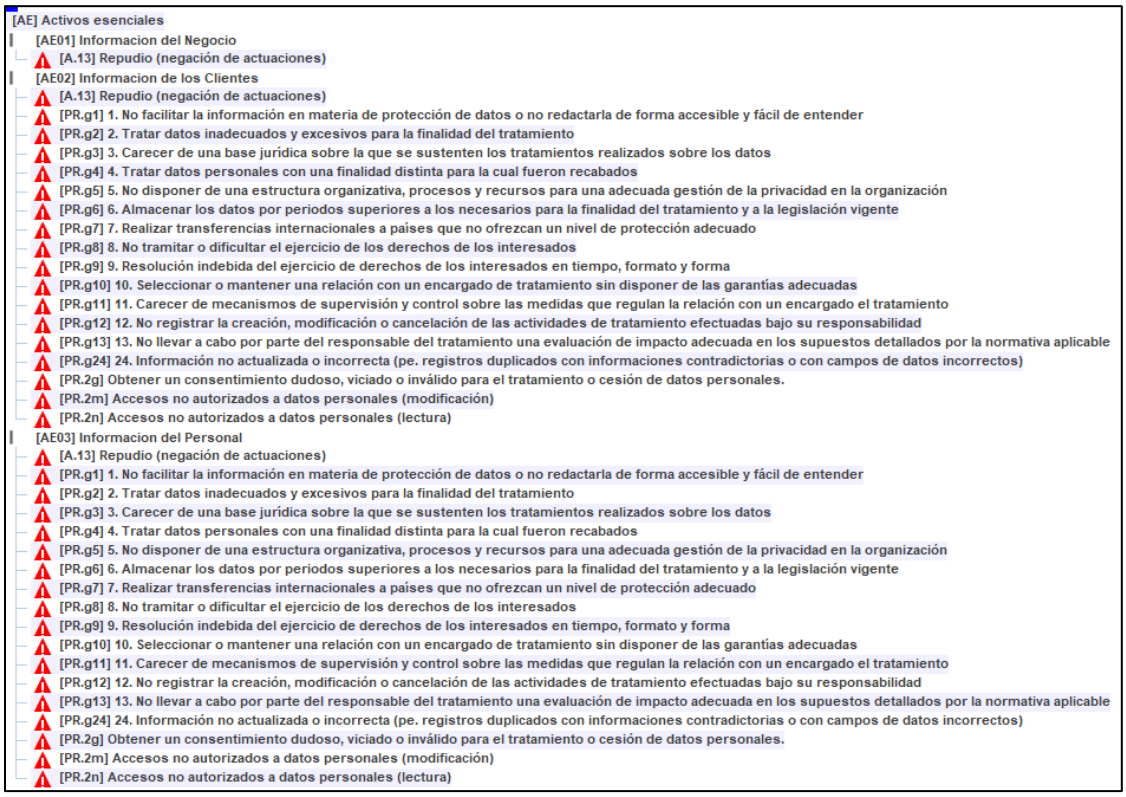

Figura 12. Amenazas para los activos de información según PILAR.
Fuente: (Elaboración propia).

En la Figura 12, podemos apreciar todas las amenazas que PILAR asigno a los activos esenciales de información de la organización basado en la valoración de estos y la importancia que tienen para la organización. Es de notar, que no todas las amenazas tienen las mismas posibilidades de ocurrir, pero PILAR las incluye debido al valor del activo y al impacto que estas amenazas pueden ocasionar en el caso de que realmente ocurran. Asimismo, podemos ver en la Figura 13, las amenazas que pueden impactar los servicios de finanzas de la organización.

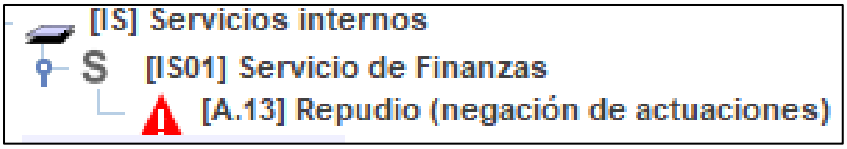

Figura 13. Amenazas para los servicios internos.
Fuente: (Elaboración propia).

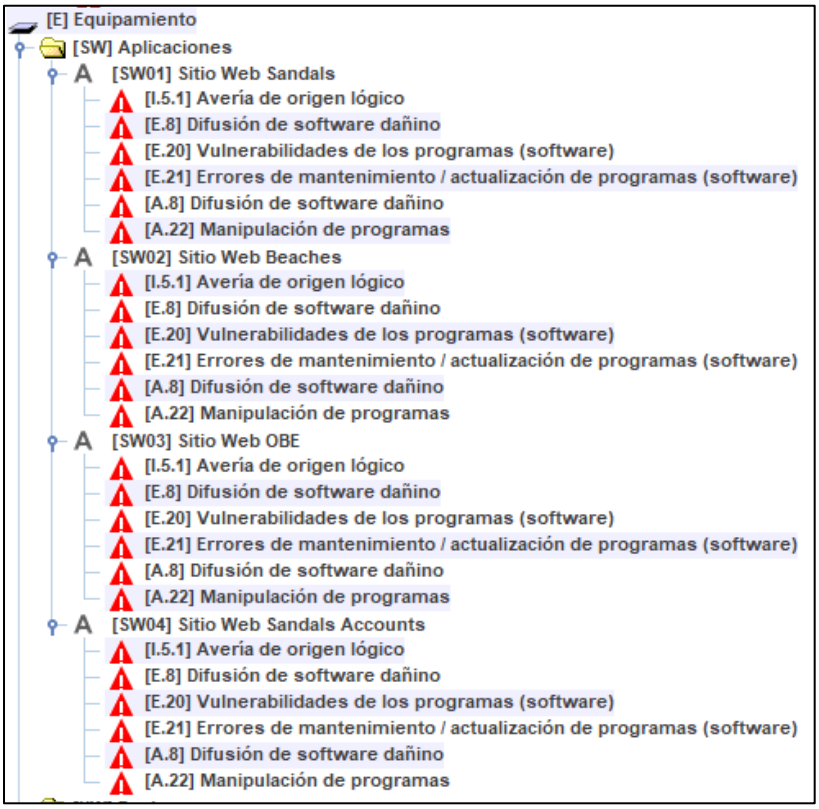

Figura 14. Amenazas para las aplicaciones.
Fuente: (Elaboración propia).

Para las aplicaciones de la organización, al ser todas del mismo tipo y tener una valoración de casi el mismo grado, las amenazas son las mismas para los 4 activos. Esto debido a que generalmente, los activos de este tipo comparten una política de configuración similar y suelen estar en ambientes compartidos, por lo que la amenaza que puede afectar a un activo, de igual manera puede afectar a otro, provocando que en cierta forma compartan el mismo nivel de impacto entre sus amenazas.

Figura 15. Amenazas para los equipos.
Fuente: (Elaboración propia).

En la Figura 15, podemos ver las amenazas asignadas a los equipos de cómputo de la organización. Es de notar que algunas de estas amenazas aparecen repetidas (Daños por agua). Esto es debido a que PILAR hace una evaluación de esa amenaza tanto como desastre natural como de origen industrial.

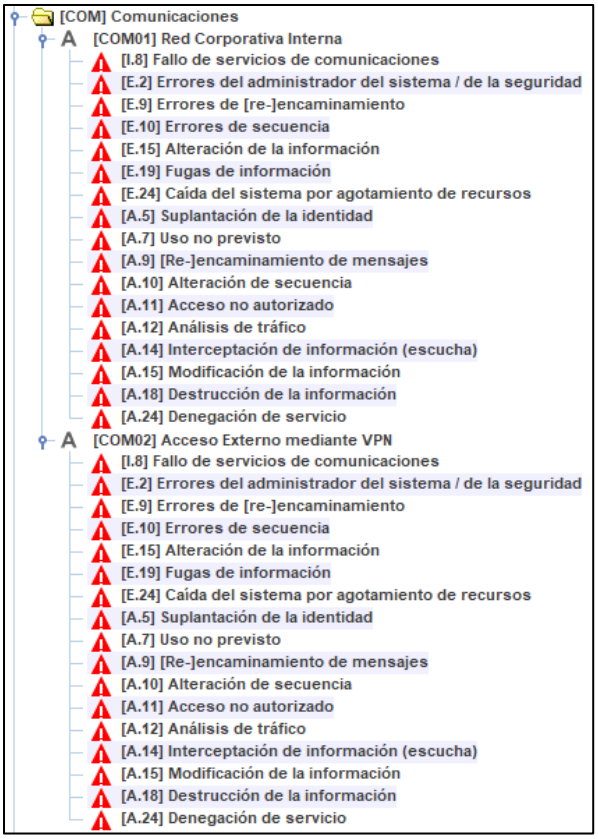

Figura 16. Amenazas para las comunicaciones.
Fuente: (Elaboración propia).

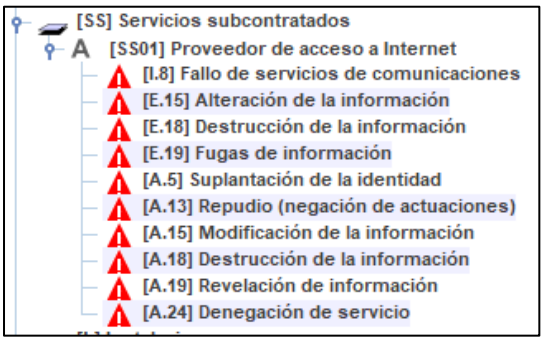

Figura 17. Amenazas para los servicios subcontratados.
Fuente: (Elaboración propia).

Las Figuras 16 y 17 presentan las amenazas para los activos de comunicaciones, así como los activos de los servicios subcontratados de internet. Dado que estos 3 activos comparten el mismo hardware y entra estrechamente relacionados entre sí, no es ninguna sorpresa que veamos que algunas de las amenazas son compartidas entre ellos.

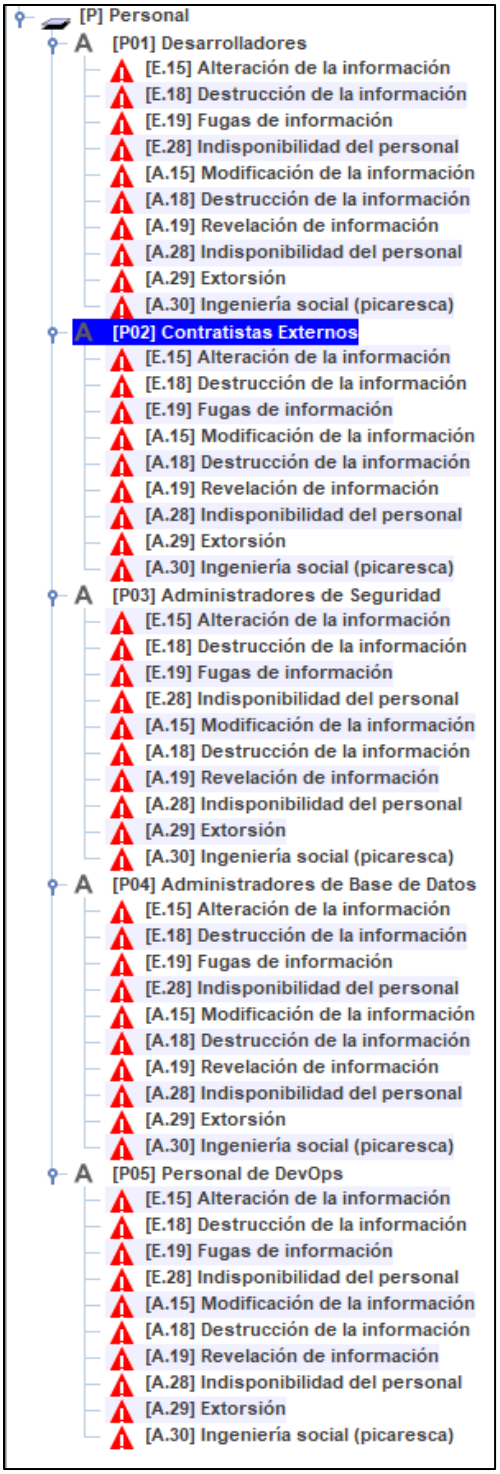

Figura 18. Amenazas para el personal.
Fuente: (Elaboración propia).

La Figura 18 muestra las amenazas para los activos de tipo personal, como lo es el personal asignado a cada área. Como estos activos son personal humano, las amenazas son más de carácter

manipulativo, errores humanos o ataques deliberados por parte de algún empleado insatisfecho.

Con las amenazas identificadas para cada activo, PILAR genera de manera automática los salvaguardas que pueden hacer frente a cada una de estas amenazas, proveyendo asimismo una visualización de aquellas salvaguardas que tienen mayor importancia para nuestro sistema. De la misma forma, PILAR provee un nivel de eficacia de cada salvaguarda con el cual es posible saber el impacto y el riesgo residual sobre los activos.

aspe...	tdp	reco...		nivel	salvaguarda	dudas	fuen...	base	com...	curr...	target	PILAR
					SALVAGUARDAS							L2-L5
G	EL				[IA] Identificación y autenticación							n.a.
T	EL	7			[AC] Control de acceso lógico							L2-L4
G	PR				[D] Protección de la Información							n.a.
G	EL				[K] Protección de claves criptográficas [SC-12]							n.a.
G	PR	5			[S] Protección de los Servicios							L2-L3
G	PR	5			[SW] Protección de las Aplicaciones Informáticas (SW)							L2-L3
G	PR	5			[HW] Protección de los Equipos Informáticos (HW)							L2-L3
G	PR	8			[COM] Protección de las Comunicaciones							L2-L5
G	PR				[M] Protección de los Soportes de Información							n.a.
G	PR	4			[AUX] Elementos Auxiliares							L2-L3
F	EL	5			[PPE] Protección física de los equipos							L3
F	PR				[L] Protección de las Instalaciones							n.a.
P	PR	5			[P] Gestión del Personal							L2-L3
G	CR	5			[IM] Gestión de incidentes							L2-L3
T	PR	7			[tools] Herramientas de seguridad							L2-L4
G	CR	3			[V] Gestión de vulnerabilidades							L2-L3
T	MN	4			[A] Registro y auditoría							L2-L3
G	RC	3			[BC] Continuidad del negocio							L2-L3
G	AD	4			[G] Organización							L2-L3
G	AD	4			[E] Relaciones Externas							L2-L3
G	AD	4			[NEW] Adquisición / desarrollo							L2-L3
G	PR				[PDS] Servicios potencialmente peligrosos							n.a.
G	PR				[IP] Sistema de protección de frontera lógica							n.a.
F	EL				[PPS] Protección del perímetro físico							n.a.
G	EL	1 (o)			[TEMPEST] Protección de emanaciones (TEMPEST) [PE-19]							L2

Figura 19. Salvaguardas en PILAR
Fuente: (Elaboración propia).

En la Figura 19, se ven las distintas salvaguardas, así como el peso que tienen para nuestro sistema. La valoración es la siguiente:

Tabla 13. Importancia de las salvaguardas

	Máximo Peso	Importancia critica
	Peso alto	Muy importante
	Peso normal	Importante
	Peso bajo	Interesante

Fuente: (Elaboración propia)

En este caso, los salvaguardas con mayor peso son aquellos que están directamente involucrados con la identificación, control de acceso y protección de la información, así como la

protección de llaves criptográficas, herramientas de seguridad, protección del perímetro físico, así como sistema de protección de frontera lógica. De la misma manera, en la columna de recomendaciones, PILAR asigna un numero de mayor a menor que define cuales son aquellas salvaguardas que poseen mayor importancia de prioridad a la hora de la implementación.

Podrá notar que, en la columna más derecha, hay ciertas valoraciones para cada salvaguarda. Esto es el nivel de eficacia que PILAR recomienda alcanzar para cada salvaguarda. Estos niveles van desde el nivel L0 al nivel L5, tal como muestra la siguiente tabla:

Tabla 14. Eficacia de las salvaguardas

Nivel	Significado	Eficacia
L0	Inexistente	0%
L1	Inicial / ad hoc	10%
L2	Reproducible pero intuitivo	50%
L3	Proceso definido	90%
L4	Gestionado y medible	95%
L5	Optimizado	100%

Fuente: (Elaboración propia)

Finalmente, pero no menos importante, PILAR aclara el aspecto de cada salvaguarda en la columna “aspecto”, así como el tipo de protección de cada uno, el cual es designado en la columna “tdp”. Los posibles valores para estas columnas son los siguientes:

- Aspecto
    - Gestión (G)
    - Aspectos Técnicos (T)
    - Seguridad Física (F)
    - Relacionado con el Personal (P)
- Tipo de protección
    - Prevención (PR)
    - Disuasión (DR)
    - Eliminación (EL)
    - Minimización de Impacto (IM)
    - Corrección (CR)

- Recuperación (RC)
- Administrativa (AD)
- Conciencia (AW)
- Detección (DC)
- Monitorización (MN)
- Normas (STD)
- Procedimiento (PROC)
- Certificación o Acreditación (CERT)

Con todos estos datos introducidos y procesados por PILAR, podemos también tomar ventaja de su capacidad de graficar el estado actual de los niveles de impacto y riesgo para cada uno de nuestros activos, como puede verse en las Gráficas 17 a 19.

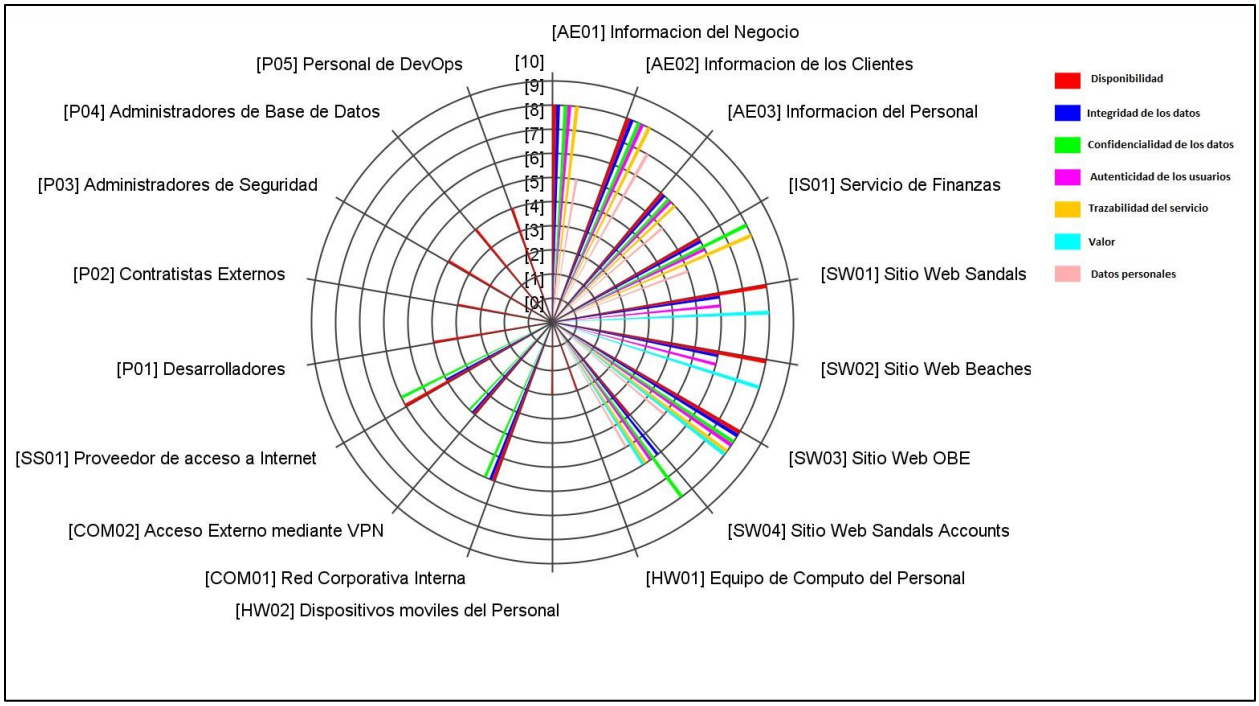

Gráfico 17. Valor / Activo
Fuente: (Elaboración propia).

La Gráfica 17 nos muestra el valor que cada activo posee según la valoración que se le dio a cada uno dentro de PILAR. Cada una de las columnas representa los casos evaluados para cada activo, con su respectivo puntaje.

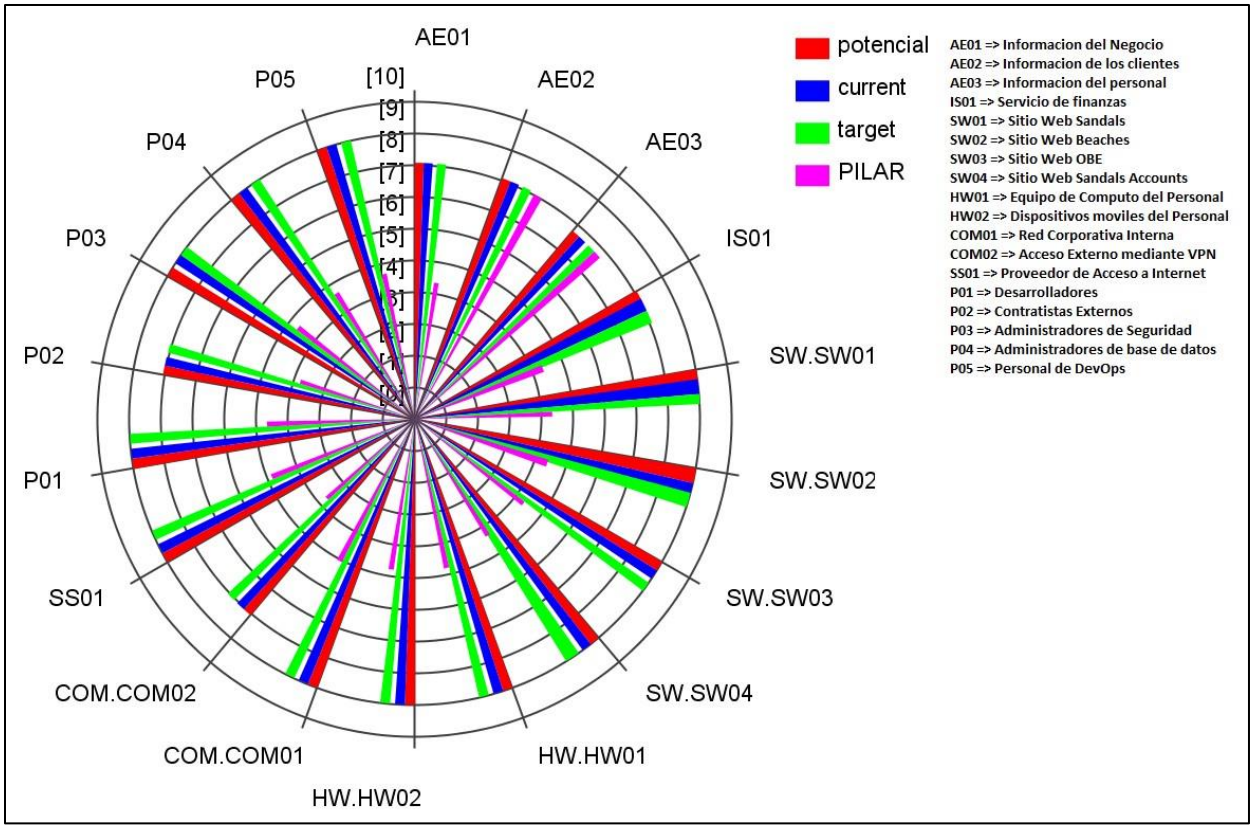

Gráfico 18. Impacto acumulado por activo
Fuente: (Elaboración propia).

En la Gráfica 18, podemos observar el impacto acumulado por activo, donde las columnas potenciales, “current” y “target” muestran los niveles de impacto potencial actuales. La columna PILAR muestra el nivel de impacto “ideal” que debería de representar dicho activo para la organización. Este impacto acumulado es el resultado de las valorizaciones dadas a cada activo, así como las amenazas que infieren en cada uno.

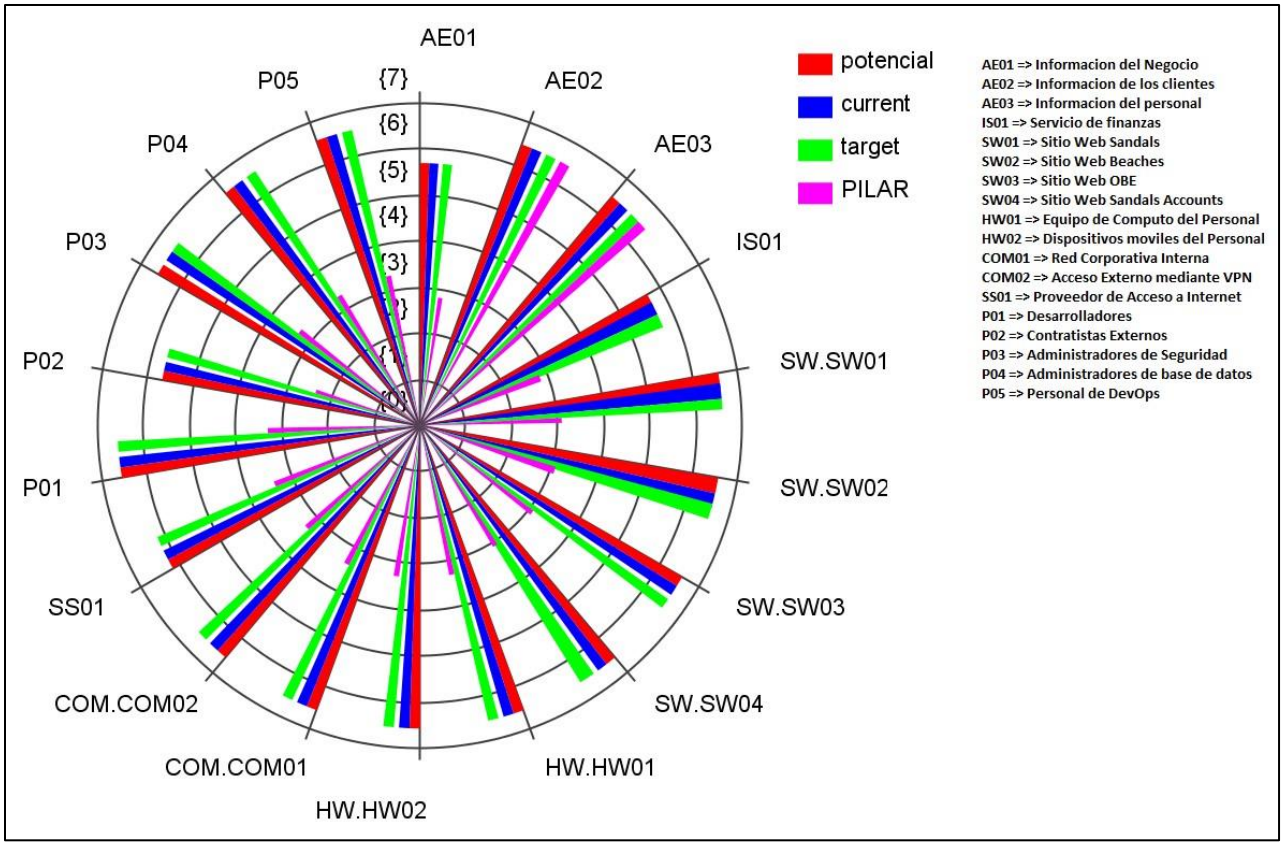

Gráfico 19. Riesgo acumulado por activo.
Fuente: (Elaboración propia).

La Gráfica 19 muestra el nivel de riesgo acumulado por cada uno de los activos. Este riesgo acumulado es el resultado de los cálculos realizados por PILAR tomando en cuenta la valorización de los activos y las amenazas.

Con toda esta información procesada de manera rápida por PILAR, podemos observar lo importante que es proteger los activos de la organización, sobre todo aquellos activos relacionados con la información de la compañía. Hay una cantidad sorprendente de amenazas que PILAR provee de manera eficiente que serán de utilidad para asegurar la correspondiente mitigación de dichas amenazas y lograr así reducir el nivel de riesgo inherente para cada uno de los activos de la organización, y garantizar que estos no se volverán un punto de quiebre interno.

4.5 MATRIZ DE RIESGOS

Con el objetivo de identificar y evaluar los riesgos potenciales que podrían afectar la seguridad de la información en San Services S. de R.L., recopilamos a través una entrevista información que nos permitiera saber más acerca de los riesgos más inminentes que podrían afectar a la organización y sus operaciones. Es importante recordar que toda operación dentro de una organización está expuesta a riesgos, pero esto no quiere decir que se deba de crear y preparar un plan de acción preventivo para cada uno de ellos. Hay riesgos que están fuera del control de la organización, y lo mejor que se puede hacer contra ese tipo de riesgos es contar con un plan de acción correctivo que permita recuperarse ágilmente del mismo. En esta ocasión, se han seleccionado 6 riesgos para los cuales se ha realizado la siguiente matriz de riesgos, la cual se divide en 3 secciones diferentes.

Para la valoración del nivel de riesgo inherente, se hicieron valoraciones con respecto a la probabilidad y el impacto que un riesgo tiene en las operaciones de la organización. Esto dio un total de 4 niveles de riesgos, los cuales puede ver en la Tabla 15.

Tabla 15. Nivel de riesgo inherente

Valor total	Riesgo inherente	Nivel de riesgo inherente	Significado
Rangos	Escala de 1 a 4		
De 1 a 3	1	**Muy bajo**	No afecta a la operatividad de la entidad
De 3 a 6	2	**Bajo**	Las consecuencias pueden ser solucionadas con algunos cambios, o actividades de rutina
De 6 a 9	3	**Medio**	Requerirá de cambios significativos en la forma de operar, pero no amenazará el cumplimiento de la actividad o proceso
Mayor a 9	4	**Alto**	Amenaza la efectividad del cumplimiento en los objetivos de la entidad

Fuente: (Superintendencia de Economia Popular y Solidaria, 2024)

Como se puede observar, cada nivel cubre un rango del valor total evaluado, con el rango de uno a tres para un nivel muy bajo de riesgo, un rango de tres a seis para un nivel bajo de riesgo, un rango de seis a nueve para un nivel medio, y a partir de nueve o más, el nivel de riesgo es alto.

La columna de “Significado” explica que significa cada uno de estos niveles y de qué forma pueden impactar a una organización u entidad.

Asimismo, es importante comprender de donde proviene este valor total evaluado, el cual nos es útil para obtener el nivel de riesgo inherente. Dicho valor sale de realizar la operación matemática de Probabilidad*Impacto. La “Probabilidad” en este caso, es una columna donde se asigna un valor numérico que representa el nivel de posibilidades que un riesgo tiene de concretarse. Esta divido en 4 niveles, los cuales son:

- 1 = Muy poco probable
- 2 = Poco probable
- 3 = Probable
- 4 = Altamente probable

Algo similar sucede con “Impacto”, el cual es otra columna que también tiene asignado un valor numérico que representa el nivel de daño que este riesgo podría ocasionar en la organización en caso de que ocurriera. Está dividido en 4 niveles, los cuales son:

- 1 = Insignificante
- 2 = Menor
- 3 = Moderado
- 4 = Con certeza

En la Tabla 16 se puede observar cada uno de los riesgos identificados establecidos por un código único y una breve descripción, los riesgos se determinan mediante un método de preguntas para una mejor comprensión, también se detalla el nivel de evaluación de cada uno de ellos. En el Gráfico 20 podemos ubicar mediante un mapa de calor los riesgos identificados para tener una mayor perspectiva del nivel de riesgo.

Tabla 16. Matriz de Riesgos - Sección Nivel de Riesgo

Código	Método de preguntas e interrogantes			Riesgo asociado	Factor de Riesgo	Probabilidad	Impacto	Valor total	Riesgo inherente	Nivel de Riesgo inherente
	Descripción del evento de Riesgo	Causa	Efecto			1 = Muy poco probable 2 = Poco probable 3 = Probable 4 = Altamente probable	1 = Insignificante 2 = Menor 3 = Moderado 4 = Con certeza	Probabilidad x impacto	Escala de calificación 1 a 4 1 = muy bajo 2 = bajo 3 = medio 4 = alto	
	¿Qué podría suceder?	¿Por qué podría suceder?	Consecuencia							
SAN-001	Ataque Ransomware a los sistemas informáticos de la organización	Un usuario podría contaminar su equipo mediante la descarga de algún archivo que provenga de un correo electrónico u sitio malicioso.	La seguridad de la infraestructura interna de la compañía se vería comprometida.	Operativo	Socio/ Cliente	2	4	8	3	Medio
SAN-002	Ataques de DDOS (Denegación de Servicio) contra los servidores públicos	Un usuario malicioso podría realizar un ataque a los sitios webs de la organización con el fin de tratar de encontrar alguna vulnerabilidad o impedir el acceso a los servicios de esta.	Los clientes no tendrán acceso a los servicios de reserva de habitaciones o a la información de los resorts.	Operativo	Producto	2	3	6	3	Medio

SAN-003	Fallas en el servicio de Internet	Una falla o daño a la fibra óptica que alimenta a las instalaciones físicas debido a un incidente poco usual.	Las operaciones se verían paralizadas debido a la falta de conexión con la red de Internet, impidiendo el acceso a diversos servicios.	Operativo	Producto	1	3	3	2	Bajo
SAN-004	Desastres naturales que afecten al Datacenter	Un desastre natural catastrófico (terremoto, incendio o huracán) puede ocasionar daños severos a nuestros datacenters.	Un daño certero al datacenter podría poner los datos de la organización en riesgo durante un periodo de tiempo indeterminado, y las tareas de restauración significarían un esfuerzo conjunto con altos costos.	Operativo	Zona geográfica	2	4	8	3	Medio
SAN-005	Suplantación del sitio web	Una persona mal intencionada podría empezar a enviar correos u anuncios a posibles clientes con el objetivo de redirigirlos a un sitio falso, con el objetivo de robar su información de pago digital.	La marca y el sitio oficial de la compañía podrían verse afectados en su reputación debido a esta suplantación.	Reputacional	Canal	3	3	9	4	Alto
SAN-006	Acceso físico no autorizado a la red interna	Una persona mal intencionada podría intentar conectarse a la red interna de la organización desde algún lugar poco sospechado (una oficina	La seguridad de la red interna de la compañía se vería comprometida.	Operativo	Socio/ Cliente	2	4	8	3	Medio

		asociada, un resort, etc.).								

Fuente: (Elaboración propia).

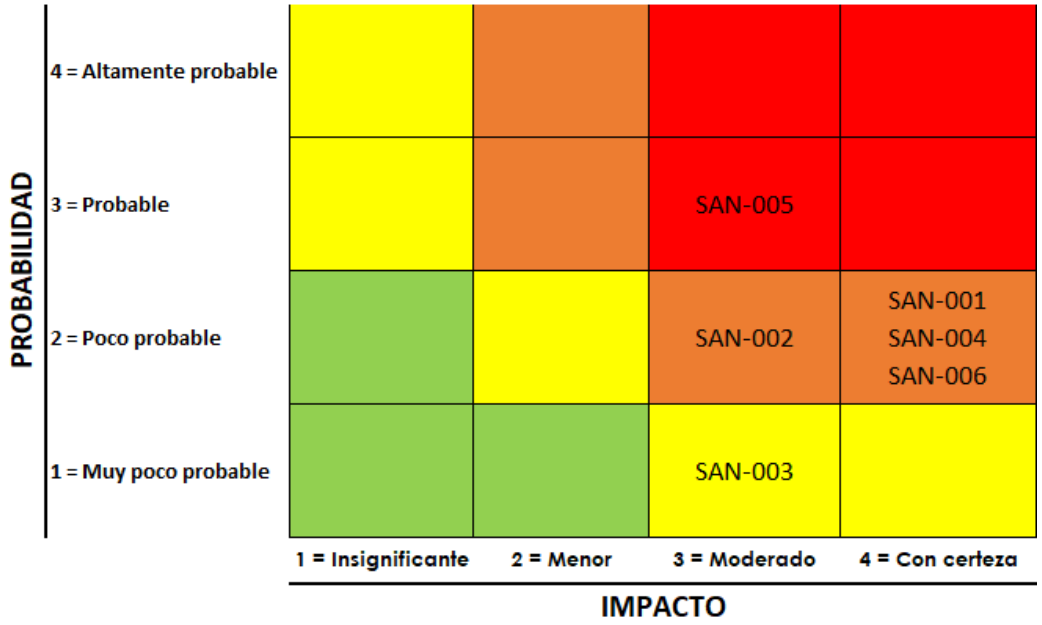

Gráfico 20. Mapa de calor para los activos de TI de San Services.
Fuente: (Elaboración propia).

Como podrá observar, se encontraron un total de seis riesgos, con uno de ellos siendo de categoría baja en la escala de riesgo inherente, cuatro siendo categoría media y uno de ellos con categoría alta. Los factores de riesgo que se presentan en la tabla indican cual podría ser la variable determinante para que este riesgo ocurra, y el riesgo asociado define el carácter del riesgo. Es decir, si es un riesgo de tipo Operativo, quiere decir que dicho riesgo puede impactar las operaciones de la organización. Es interesante destacar en esta tabla, que, si bien todos los riesgos tienen poca probabilidad de ocurrir debido al perfil de la compañía, los mismos tienen un alto impacto en la misma en una hipotética situación de que ocurran. Y cinco de estos riesgos, impactarían las operaciones diarias de la organización. Pasaremos a revisar, los controles que se pueden aplicar para mantener estos riesgos en el nivel más bajo de ocurrencia.

Para la sección de controles de riesgo, cada uno de los seis riesgos tuvo como propuesta un control, el cual tiene como objetivo minimizar el impacto o las posibilidades de que alguno de estos riesgos ocasione dificultades a la organización. Cada uno de los controles es evaluado en base a cuatro criterios: clase, tipo, frecuencia y modalidad. Cada uno de estos cuatros criterios está dividido en 3 niveles:

- Clase: Define el tipo de control según su función.
    - Preventivos: Valor numérico de uno.
    - Detectivos: Valor numérico de dos.
    - Correctivos: Valor numérico de tres.
- Tipos: Define la forma de operación del control.
    - Automático: Valor numérico de uno.
    - Semiautomático: Valor numérico de dos.
    - Manual: Valor numérico de tres.
- Frecuencia: Define el tiempo de operación del control.
    - Permanente: Valor numérico de uno.
    - Periódico: Valor numérico de dos.
    - Ocasional: Valor numérico de tres.

- Modalidad: Define el estado actual de la implementación del control.
    - Implementado: Valor numérico de uno.
    - En desarrollo: Valor numérico de dos.
    - Sin implementar: Valor numérico de tres.

Al asignar cada uno de estos valores dentro de la columna correspondiente, se calcula el un valor promedio que nos permite evaluar el estado del control con respecto al riesgo inherente. Así, podemos ver en la Tabla 17 los cuatro niveles anteriormente mencionados y lo que significa cada uno de ellos.

Tabla 17. Nivel de riesgo residual

Valor promedio	Tipo de control	Tipo de control	Significado
Rangos	Escala de 1 a 4		
De 1 a 2	1	Apropiado	Fuerte, permite mitigar el riesgo.
De 2 a 3	2	Aceptable	Moderado, permite mitigar el riesgo.
De 3 a 4	3	Mejorable	Insuficiente, debe mejorarse para mitigar el riesgo.
Mayor a 4	4	Deficiente	Débil, debe reforzarse para mitigar el riesgo.

Fuente: (Superintendencia de Economia Popular y Solidaria, 2024)

Estas figuras se entenderán mejor al verlas en funcionamiento junto con los datos en la Tabla 18. Cada uno de los controles pertenece a uno de los riesgos anteriormente mencionados. A cada control, se le da una calificación según cada uno de los 4 criterios anteriormente mencionados, lo cual nos provee el valor promedio de su valoración. Asimismo, cada control está asignado a un área encargada, el cual se encargará de su implementación. Finalmente, se realiza el cálculo del riesgo residual, el cual es una multiplicación entre el riesgo inherente * valor promedio del control. A cada riesgo residual, se le asigna una calificación dependiendo del resultado. Los valores son asignados de la siguiente forma:

Tabla 18. Calificación del nivel de riesgo residual

Valor Riesgo Residual	Calificación	Nivel
Rangos	Escala de 1 a 4	
Menor que 2.99	1	Muy bajo
De 3 a 5.99	2	Bajo
De 6 a 8.99	3	Medio
Mayor a 9	4	Alto

Fuente: (Superintendencia de Economia Popular y Solidaria, 2024)

Existirán casos en donde el nivel residual pudiera no alcanzar los niveles deseados, y esto se podría deber a multitud de circunstancias, muchas de ellas pudiendo ser circunstancias externas que escapan del control de la organización, por lo que prepararse para ello de la mejor forma. Aun así, es recomendable que se coloquen tantos controles como se crean necesarios, y que se evalué que cada control esté en funcionamiento de manera efectiva antes de empezar a implementar otro. A continuación, la Tabla 19 junto con los controles elegidos:

Tabla 19. Matriz de Riesgo – Sección de controles de riesgo

Descripción del Control	Factores de análisis o evaluación				Responsable del control	Total, valoración de los controles		Riesgo Residual		
	Clase	Tipos	Frecuencia	Modalidad	Área de Ciberseguridad Área de Base de Datos Área de DevOps	Valor promedio	Nivel 1= Apropiado 2= Aceptable 3= Mejorable 4= Deficiente	Cálculo R.I.* V.P.Control	Escala de calificación 1 a 4 1 = muy bajo 2 = bajo 3 = medio 4 = alto	Nivel
	1 = Preventivos 2 = Detectivos 3 = Correctivos	1= Automático 2= Semiautomático 3 = Manual	1= Permanente 2= Periódico 3= Ocasional	1= Implementado 2= En desarrollo 3= Sin implementar						
(SAN-001) Normas de Seguridad y Reglas del uso de la red interna.	1	1	1	2	Área de Ciberseguridad	1	Aceptable	4	2	Bajo
(SAN-002) Protección de los sitios públicos mediante el uso de sistemas de Firewall que protejan contra DDOS.	1	1	1	2	Área de DevOps	1.3	Aceptable	4	2	Bajo
(SAN-003) Redundancia de Red.	1	1	1	3	Área de Ciberseguridad	2	Aceptable	3	2	Bajo
(SAN-004) Aseguramiento de los datos y réplicas del Datacenter mediante servicios externos en otras zonas geográficas.	1	1	1	3	Área de DevOps	2	Aceptable	5	2	Bajo

(SAN-005) Creación de un plan de acción legal para el caso de que dicha situación suceda.	3	1	1	3	Área de Ciberseguridad	2	Aceptable	8	3	Medio
(SAN-006) Plan de control de red para prevención de tráfico no autorizado.	1	1	1	2	Área de Ciberseguridad	1	Aceptable	4	2	Bajo

Fuente: (Elaboración propia)

Como se podrá observar en la Tabla 19, cinco de los controles definidos son de clase preventivo y de frecuencia permanente, pero con modalidades bien distintas los unos de los otros. Algunos de ellos están en desarrollo, mientras que otros aún no han empezado a desarrollarse. Se puede observar que aun con un plan de control en marcha, el riesgo SAN-005 (Suplantación del sitio web) fue el control que quedo con un riesgo residual de nivel medio. Esto es porque, como mencionábamos anteriormente, habrá ciertos riesgos que no dependen completamente de lo que la organización pueda hacer, sino también de que tan llamativa pueda ser para un ciberdelincuente, así como las legislaciones de la nación donde opere, la agilidad de la justicia, entre otros factores.

Finalmente, llegamos a la última sección de esta matriz de riesgo, que muestra las actividades relacionadas con los controles previamente definidos, las fechas de inicio y fin, los responsables, la fecha de seguimiento, evidencias, evaluaciones y algunas recomendaciones. Todo esto puede verse a continuación en la Tabla 20:

Tabla 20. Matriz de Riesgo - Sección de plan de acción para los riesgos

Plan de acción					Monitoreo			
Actividades	**Responsable**	**Fecha de inicio**	**Fecha fin**	**Indicador**	**Fecha de seguimiento**	**Evidencia del cumplimiento**	**Evaluación de la efectividad del control**	**Observación/ Recomendación**
(SAN-001) Crear reglas de control de los recursos de Internet a los que los usuarios tienen acceso.	Área de Ciberseguridad	1/9/2024	30/9/2024	Reportes semanales de las nuevas reglas implementadas.	1/10/2024	Reglas aplicadas y notificadas a los empleados.	Test de prueba de navegación.	Asegurarse que las reglas no impiden a los usuarios realizar tareas cotidianas de su posición en la organización.
(SAN-002) Asegurar que todos los sitios públicos estén protegidos mediante el uso de servicios como CloudFlare u otras alternativas.	Área de DevOps	1/11/2024	31/12/2024	Reportes semanales de los avances del desarrollo.	1/1/2025	Los sitios estarán protegidos por el servicio externo.	Pruebas de ataques simulados para verificar que la protección es eficaz.	
(SAN-003) Asegurar que exista una conexión redundante a Internet que permita garantizar las operaciones sin interrupción de la organización.	Área de Ciberseguridad	1/1/2025	1/2/2025	Reporte de las capacidades y ofertas de otros proveedores.	1/3/2025	La organización podrá usar cualquiera de las dos conexiones mediante un cambio en Switch sin que se note ninguna disrupción.	Evaluar que el nuevo proveedor no utilice las mismas rutas de redes.	
(SAN-004) Asegurar que el DataCenter tenga replicas en distintas áreas geográficas que garanticen la seguridad al acceso de los datos y un riesgo mínimo en caso de desastres naturales.	Área de DevOps	Q2 2025	Q3 2025	Reportes semanales de las evaluaciones de posibles regiones según las necesidades de la organización.	Q3 2025	Las nuevas regiones geográficas escogidas deben de estar en zonas de pocas incidencias de desastres y cumplir con los requerimientos de redundancia.	Las réplicas de los datacenter deben de ser capaces de entrar en línea en el momento que algún otro datacenter sale del sistema.	Controlar el costo/beneficio sobre cuantas replicas son necesarias.
(SAN-005) Garantizar que el equipo legal esté preparado para tomar acciones legales en caso de ser necesario, así como de estar vigilantes	Área de Ciberseguridad	Q2 2025	Q4 2025	Creación de un marco interno apoyado en leyes internacionales que permitan la defensa de la marca.	Q3 2025	La organización cuenta con un equipo de respuesta ante este tipo de incidentes, así como un sistema que	N/a	

ante cualquier caso de suplantación que se reporte por parte de empleados o clientes.						permita denunciar dichos incidentes.		
(SAN-006) Garantizar que los equipos que se conecten a la red interna únicamente puedan navegar si poseen las credenciales válidas para ello. Desconectar de la red a todo equipo que no presente credenciales pasado un periodo de tiempo corto.	Área de Ciberseguridad	Q1 2025	Q2 2025	Asignación de credenciales individualizadas para cada asociado/empleado.	Q2 2025	La organización y sus colaboradores son los únicos autorizados a navegar en la red internar. Todo equipo no autorizado es desconectado.	N/a	

Fuente: (Elaboración propia)

Como se puede observar, la mayoría de las actividades tienen fechas de implementación de por lo menos 30 días, con otras tomando 3 meses o más. El área encargada de la mayoría de estas actividades es el área de ciberseguridad, lo cual tiene sentido ya que muchas de estas actividades se enfocan en asegurar los recursos de la compañía para no sufrir disrupciones en sus operaciones. Todas las actividades tienen evaluaciones orientadas a asegurar que lo implementado pueda proteger los recursos existentes de un ataque real, así como algunas observaciones para algunas de ellas. Dado que el área de ciberseguridad es el encargado de la mayoría de estas actividades, algunas de las mismas no pueden correr en paralelo debido al tiempo requerido para diseñarlas, implementarlas y ponerlas a prueba. Las fechas de seguimiento son posterior a la implementación de cada actividad, con el fin de recopilar información que permita el mejoramiento de cada una luego de su lanzamiento, empezando así un ciclo de mejora continua que se espera se efectué cada cierto tiempo.

CAPÍTULO V – CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Según el estudio de análisis de brechas aplicado dentro de San Services S. de R.L. sobre el estado actual y el estado deseado del manejo de la seguridad de la información basado en los lineamientos de la norma ISO 27001:2022, se determina que los requisitos que mejor están posicionados dentro de la empresa son Contexto de la Organización y Liderazgo, con una brecha de 10.42% y 11.11% respectivamente, ambos con un nivel de madurez optimizado. Mientras tanto en la percepción de los controles del Anexo A se refleja un nivel de cumplimento aceptable con un promedio de 80.96%, siendo el grupo de controles de Personas con mayor valoración con un 89.58%. Esto es importante ya que la empresa está de cierta manera preparada para una futura adopción del SGSI.
- Se identifican 6 riesgos importantes que pueden afectar seriamente las operaciones de San Services, los cuales mediante una evaluación de escalas se determina el riesgo inherente siendo el riesgo de suplantación de sitio web el riesgo con un nivel más alto, y los riesgos de ataque de ransomware, ataque DoS, daños por desastres naturales y accesos físicos no autorizados en un nivel medio, mientras que el fallo en el servicio de internet en un nivel bajo. El riesgo de suplantación de sitio web es el único que queda con un riesgo residual medio luego de la evaluación del control aplicar, ya que la aplicación del control no depende de la organización si no que dependerá de otros factores como las legislaciones de cada país. Para cada control se define un plan de acción y monitoreo.
- El levantamiento de los activos más importantes para San Services se dividen en categorías como ser: activos esenciales, servicios internos, equipamiento, servicios subcontratados, instalaciones y personal, cada uno de ellos cuentan con una valoración dentro de la herramienta de PILAR, estos adquieren mediante la metodología MAGERIT una lista de amenazas posibles. Los activos con mayor número de amenazas son aquellos que tienen que ver con la información como tal (negocios, clientes y personal) y le siguen los activos de equipos físicos como PCs personales, dispositivos móviles y equipos de redes y comunicaciones. De todos estos riesgos en los activos, PILAR ofrece una serie de salvaguardas o controles con el cual es posible saber el impacto del riesgo inherente y el

riesgo residual, para su debido tratamiento.

- El alcance SGSI en San Services se centra específicamente en el área de TI, incluyendo todos los sistemas, redes, aplicaciones, datos y personal involucrado en el desarrollo, mantenimiento y soporte de software. Este sistema abarca la infraestructura de TI, aplicaciones, datos, comunicación y personal, excluyendo equipos personales de los empleados y servicios no gestionados directamente por San Services. Además, se definen claramente los límites físicos y tecnológicos, así como los responsables de la implementación y mantenimiento del SGSI, garantizando la protección de la información crítica de la empresa, socios, proveedores y clientes.

5.2 RECOMENDACIONES

- La alta dirección de San Services debe de involucrarse en la iniciativa de implementación del SGSI, para ofrecer el apoyo y compromiso que el proyecto requiere, así como los recursos humanos y materiales que permitan un buen desempeño del mismo y de la misma forma, dar la jerarquía de funcionamiento con roles y responsabilidades para cada una de las etapas del desarrollo del SGSI.
- El alcance del SGSI debe de estar bien delimitado en función de las características del negocio, organización, localización, activos y tecnología. Cualquier cambio en el alcance debe de ser previamente evaluado, aprobado y documentado por todas las partes involucradas.
- Se recomienda el uso de la metodología PMBOK para el desarrollo del proyecto de implementación del SGSI, ya que es un marco estructurado y aprobado para la gestión de proyectos, así como un facilitador en la planificación, ejecución y control de proyectos, asegurando una implementación alineada con los objetivos estratégicos de la empresa.
- Los riesgos identificados deben de ser atendidos en la mayor brevedad posible, llevando a cabo las labores de implementación de cada uno de los controles previamente definidos, así como las acciones que permitan reducir cualquier incidencia, reduciendo el impacto que puedan causar en el caso que terminen ocurriendo, y reconociendo el riesgo que representan en caso de no tomar medidas para mitigarlos.

- Revisar periódicamente la lista de riesgos a las que hace frente la organización, y hacer las evaluaciones pertinentes para asegurar que los mismos tengan todas las mitigaciones necesarias con el fin de reducir cualquier incidencia, así como asegurar que nuevos riesgos se tomen en cuenta según los cambios de mercado y el avance de las tecnologías.

CAPÍTULO VI – APLICABILIDAD

6.1 NOMBRE DE LA PROPUESTA

Plan de implementación de un Sistema de Seguridad de la Información (SGSI) basado en la norma ISO 27001:2022 para el área de TI de San Services S. de R.L.

6.2 JUSTIFICACIÓN DE LA PROPUESTA

Hemos visto durante la evaluación de los requisitos y controles como pueden existir algunas grietas digitales dentro la empresa que pueden dar cabida a vulnerabilidades que a su vez afloren amenazas que atenten contra los datos sensibles. Al implementar un SGSI no solo se hará frente a esa situación, sino que también se harán cumplir normativas internacionales y mitigara los riesgos encontrados según como lo hemos evidenciado en la investigación. Esto no solo garantiza la confidencialidad, integridad y disponibilidad de la información crítica, sino que también fortalecerá la confianza de los clientes y socios comerciales, mejorará la capacidad de respuesta ante incidentes, y promoverá una cultura organizacional centrada en la seguridad. Además, al prevenir incidentes de seguridad, un SGSI con un alcance definido y estructurado ayudará a San Services a reducir costos operativos y protegerá la reputación de la empresa en un mercado altamente competitivo.

6.3 ALCANCE DE LA PROPUESTA

El desarrollo de este plan es poder lograr un procedimiento claro para ayudar que San Services pueda establecer los cimientos para lograr una implementación de ISO 27001 y si es posible una certificación de esta, por lo cual los objetivos serán los siguientes:

a. Definir una guía por fases para llevar a cabo la implementación de un SGSI basado en ISO 27001 en su versión 2022.

b. Establecer los controles seleccionados que se adapten a las funciones de San Services según lo desarrollado en el análisis de brechas.

6.4 DESCRIPCIÓN DE LA PROPUESTA

6.4.1 RUTA DE NAVEGACIÓN

Como parte del guía de implementación debemos de seguir una ruta en la cual debemos atravesar para lograr el objetivo general que es la implementación del SGSI tal como se muestra en la Figura 20.

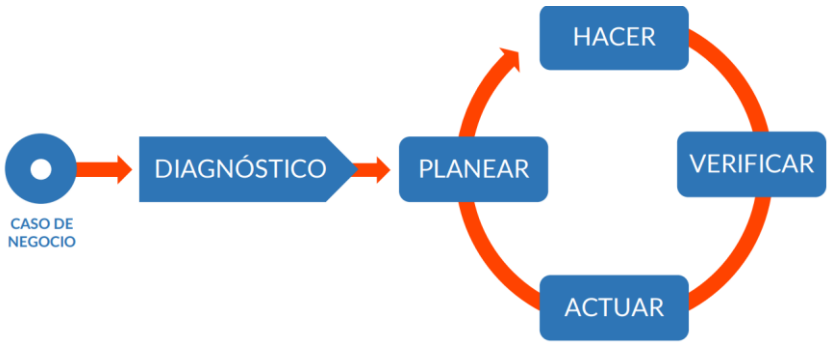

Figura 20. Ruta de navegación para la implementación del SGSI.
Fuente: (certiprof, 2022).

La implementación del SGSI debe de verse como un proyecto, que al finalizar el primer hito del ciclo debe de mantenerse en constante mejora en la operación.

Lo primero es poder identificar el caso de negocio, el cual es mejorar la seguridad de información en San Services. Seguidamente, tal como se abordó en la investigación, llevar a cabo un diagnóstico actual de la situación de las condiciones actuales tanto administrativas como técnicas dentro de la empresa para la adopción del SGSI. Luego entran una serie de actividades a desarrollar en el ciclo PDCA o PHVA las cuales detallaremos en esta sección.

6.4.2 PLAN DE IMPLEMENTACIÓN

Para llevar a cabo todo el desarrollo del proyecto debemos primero establecer las fases de seguimiento las cuales quedaran de la siguiente manera:

- Fase I: Diagnóstico y Organización
- Fase II: Planificación (PLAN)

- Fase III: Despliegue (DO)
- Fase IV: Revisión (CHECK)
- Fase V: Consolidación (ACT)

También es importante conocer que el ciclo PDCA conlleva ciertos ítems de la estructura del ISO 27001 como lo podemos ver en la Figura 21:

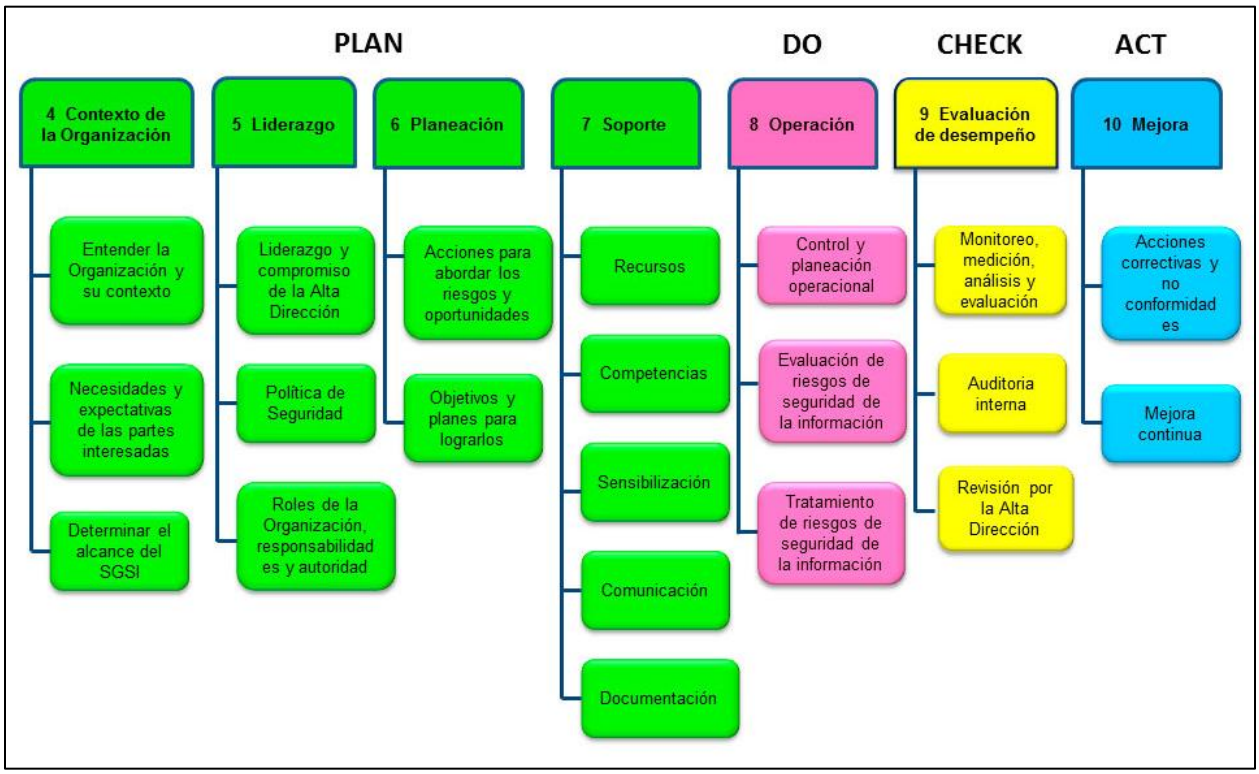

Figura 21. Etapas del ciclo PDCA para el desarrollo de actividades del SGSI según norma ISO 27001.
Fuente: (Elaboración propia).

- **Fase I: Diagnóstico y Organización**

Caso de negocio

Primeramente, se deberá elaborar un caso de negocio para la alta dirección de San Services para exponer formalmente el caso y poder asegurar el apoyo en todos los sentidos para llevar a cabo la implementación del SGSI. El caso de negocio deberá de llevar las

siguientes secciones:

- Resumen ejecutivo.
- Análisis de oportunidad.
- Análisis costo – beneficio.
- Análisis de riesgos y recompensas.
- Plan de implementación.

Análisis de contexto

En esta etapa se debe de llevar a cabo todo lo relacionado con las actividades esenciales para dirigir y comenzar la implementación del proyecto tales como.

- Análisis GAP.
- Plan y alcance del proyecto.

- **Fase II: Planificación (PLAN)**

Comprensión de la organización y su contexto

Se deberá entender el contexto de la organización para realizar análisis interno y externo, así como las expectativas de las partes interesadas por medio de herramientas como el FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) y PESTEL (Político, Económico, Social, Tecnológico, Ecológico y Legal).

Definir el alcance del SGSI

Definición y redacción del documento del alcance del SGSI oficial aprobado, firmado y sellado por la dirección ejecutiva y autoridades de TI de San Services, donde se incluyan por lo menos las siguientes secciones:

- Objetivo y alcance.
- Documentos de referencia.
- Definición del alcance.
- Exclusiones del alcance.
- Límites del SGSI.

- Responsables.

Elaboración de políticas de seguridad de la información

Estas políticas describirán la importancia estratégica del SGSI para la empresa, en la cual detallará las actividades de seguridad de la información dentro de San Services y además revelará explícitamente las necesidades de seguridad de la información y sus responsables en un contexto real.

Desarrollar identificación de activos y análisis de riesgos

La identificación de activos para la operatividad critica de San Services y el análisis de riesgos se realizará utilizando una metodología estructurada que generalmente sigue los principios de la norma ISO 27001 como MAGERIT el cual se detalló en esta investigación. Primero, se identifican y catalogan todos los activos de información, incluyendo hardware, software, datos, personas y procesos importantes para la organización. A cada activo se le asigna un valor en función de su importancia y su papel en las operaciones empresariales. Luego, se realiza un análisis de riesgos en el que se identifican las amenazas y vulnerabilidades asociadas a cada activo.

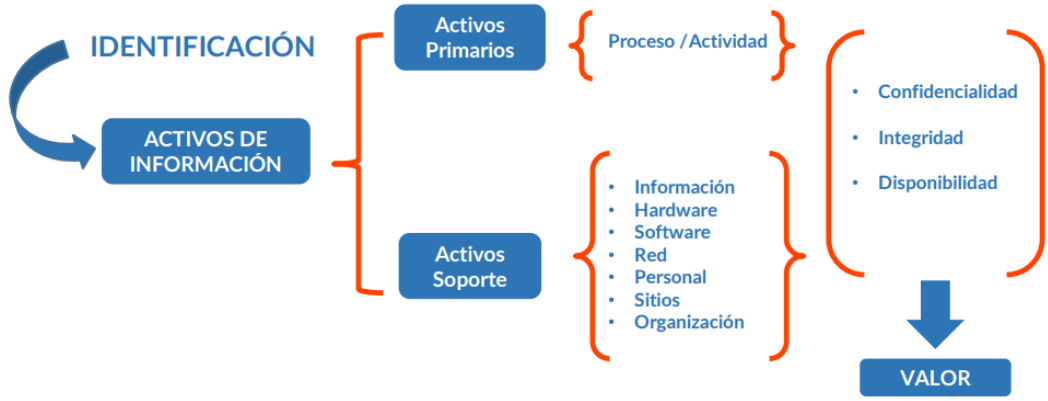

Figura 22. Estructura para la identificación de activos.
Fuente: (certiprof, 2022).

SoA (Declaración de aplicabilidad)

En este punto se deberán identificar aquellos controles técnicos del Anexo A del documento ISO 27001 que fueron evaluados en el análisis GAP para ver cuáles son los que deben de ser incluidos y justificados y que en definitiva deben de partir del análisis de los

riesgos.

- **Fase III: Despliegue (DO)**

Evaluación de los riesgos

Poder identificar, evaluar y gestionar los riesgos que podrían afectar la seguridad de la información en San Services es algo que se puede hacer por medio de una matriz de riesgos la cual se desarrolló en esta investigación. Esta matriz clasifica los riesgos según su probabilidad de ocurrencia y el impacto potencial en la organización. Cada riesgo se evalúa y se asigna una puntuación que refleja su gravedad, permitiendo priorizar las acciones de mitigación. La matriz también ayuda a definir controles y medidas preventivas específicas, asignar responsabilidades y establecer planes de contingencia para asegurar que los riesgos se gestionen de manera eficaz y que el SGSI se implemente con éxito, alineado con los estándares de ISO 27001.

Tratamiento de riesgos de seguridad de la información apoyado en ISO 27002:2022

Según el análisis de brechas realizado para los requisitos del Anexo A del ISO 27001:2022, se identifican controles de los cuales algunos necesitan reforzamiento, en este caso el grupo de controles Organizativos el cual requiere mayor atención, basándose en el documento de apoyo ISO 27002:2022 este ofrece recomendaciones sobre las mejores prácticas para el establecimiento, implementación, mantenimiento y mejora de cada uno de los controles según sea la necesidad. Puntualmente seguir las directrices en los controles A5.1, A5.6, A5.8, A5.9, A5.12, A5.13, A5.19 y A5.37.

Diseño y planificación de planes de capacitación y comunicación

El diseño y la planificación de planes de capacitación y comunicación son esenciales para garantizar que todos los empleados dentro del alcance comprendan y cumplan con las políticas y procedimientos de seguridad. El proceso comienza con la identificación de las necesidades de capacitación de acuerdo con los roles y responsabilidades de cada empleado en relación con la seguridad de la información. Se desarrollan programas de capacitación específicos que incluyen módulos sobre concienciación en seguridad, prácticas seguras de manejo de la información, y respuesta a

incidentes. Además, se planifican sesiones regulares de formación continua y talleres prácticos para reforzar los conocimientos.

Paralelamente, se diseña un plan de comunicación que asegura la difusión efectiva de la información de seguridad dentro de la organización. Este plan incluye la creación de canales de comunicación claros y accesibles, como boletines informativos, correos electrónicos, y reuniones de equipo, donde se discuten las políticas de seguridad, se reportan incidentes, y se actualiza al personal sobre nuevas amenazas y medidas de protección. La comunicación bidireccional también es fomentada para que los empleados puedan expresar sus inquietudes y sugerencias. Esta estrategia integrada de capacitación y comunicación es crucial para cultivar una cultura de seguridad de la información y asegurar la conformidad con el SGSI.

- **Fase IV: Revisión (CHECK)**

  Monitoreo del desempeño del SGSI

  En esta fase se debe de realizar un seguimiento, medición, análisis y evaluación del SGSI, teniendo como objetivo verificar si todas las actividades que se han desarrollado para fortalecer la seguridad de la información, incluidas la evaluación de los riesgos y tratamiento de estos, se han logrado de forma esperada.

  San Services debe de determinar según su interés, que procesos se deben de seguir y como medirlos, quien es el responsable de ese seguimiento, quien es el responsable de la medición y con qué frecuencia se realizara. También es importante el establecimiento de métodos para la obtención de los resultados por medio de la definición de indicadores de clave de desempeño (KPIs). De esta manera podemos evaluar la eficacia del SGSI determinando la medida en que los objetivos de la seguridad de la información se cumplen.

  Algunos aspectos a medir son:

  - Avance del proyecto de implementación.
  - Cubrimiento del presupuesto asignado.
  - Mejora de la percepción de seguridad de las partes interesadas.

- Disminución de incidentes de seguridad.
- Eficacia de acciones correctivas.
- Disminución de vulnerabilidad técnicas identificas de un periodo a otro.
- Lecciones a usuarios sobre los factores de riesgo que podrían causar incidentes de seguridad.

Auditorías Internas

Las auditorías internas funcionan como una radiografía del SGSI, permitiéndonos comprobar si este cumple a cabalidad con los estándares establecidos por la organización y la norma ISO 27001. En otras palabras, son una evaluación exhaustiva que nos brinda la certeza de que el SGSI se encuentra en óptimas condiciones.

La auditoría debe de caracterizarse por varios principios como:

- Integridad
- Presentación justa
- Confidencialidad
- Independencia
- Enfoque basado en evidencia

La función de la auditoría interna en San Services será definir un alcance y objetivos de esta, determinar que procesos específicos serán auditados y que se espera lograr con la auditoría; Luego desarrollar un plan que contenga una calendarización de actividades, y la asignación de responsables. Seguidamente, se debe desarrollar la ejecución de la auditoria por medio de la revisión de la documentación del SGSI, entrevistas, observaciones y prueba de los controles para finalmente por medio de un informe presentar los resultados a las partes interesadas.

- **Fase V: Consolidación (ACT)**

Implementación de acciones correctivas.

En esta fase se deben de definir las no conformidades presentadas en la fase revisión. Una no conformidad es el incumplimiento de un requisito del SGSI. Un requisito es una

necesidad o expectativa establecida y son implícitas u obligatorias.

Ejemplos de no conformidades en San Services serian:

- Proyectos de desarrollo de software que no arrojan los resultados deseados.
- Debilidades de seguridad en el análisis y diseño de las bases de datos.
- Comportamientos del personal que atentan contra los procedimientos y políticas de seguridad.

Las acciones correctivas están dirigidas a examinar y erradicar las causas de una no inconformidad y evitar su recurrencia. El proceso de las acciones correctivas es el siguiente:

- Decidir si es necesario realizar una acción correctiva según los criterios establecidos.
- Revisar la no conformidad considerando registros de no conformidades similares, todas las consecuencias y efectos secundarios causados, y las correcciones realizadas.
- Realizar un análisis exhaustivo de la causa de la no conformidad.
- Evaluar las posibles consecuencias sobre el SGSI.
- Determinar las acciones necesarias para corregir la causa, evaluando si son proporcionales a las consecuencias e impacto de la no conformidad.
- Planificar las acciones correctivas priorizando, si es posible, las áreas con mayor probabilidad de recurrencia y las consecuencias más significativas de la no conformidad.
- Implementar las acciones correctivas según el plan establecido.
- Evaluar las acciones correctivas para determinar si han abordado realmente la causa de la no conformidad y si se ha evitado la ocurrencia de no conformidades relacionadas.

Desarrollo de las actividades para evidenciar la mejora continua del SGSI.

La mejora continua del SGSI debe implicar que el sistema y todos sus componentes

sean evaluados teniendo en cuenta factores internos y externos, los requisitos de las partes interesadas y los resultados de la evaluación del desempeño.

La evaluación también puede incluir un análisis de la eficiencia del SGSI y sus componentes, considerando si el uso de los recursos es adecuado, si hay riesgo de que la falta de eficiencia pueda llevar a una pérdida de efectividad, o si existen oportunidades para mejorar la eficiencia.

Las oportunidades de mejora también pueden identificarse al gestionar las no conformidades y las acciones correctivas.

6.6 CRONOGRAMA DE IMPLEMENTACIÓN

Tabla 21. Cronograma de actividades del plan de implementación del SGSI.

CRONOGRAMA DE ACTIVIDADES DEL PLAN DE IMPLEMENTACIÓN DEL SGSI - ÁREA DE TI SAN SERVICES S. DE R.L.									
FASE/OBJETIVO	**ACTIVIDADES**	**DETALLE DE ACTIVIDADES**	**ABR-JUN**	**2024**		**2025**			
			2024	**JUL-SEP**	**OCT-DIC**	**ENE-MAR**	**ABR-JUN**	**JUL-SEP**	**OCT-DIC**
FASE I DIAGNÓSTICO Y ORGANIZACIÓN Llevar a cabo las actividades esenciales para dirigir y comenzar la implementación del SGSI.	Desarrollo y evaluación de datos y documentos recopilados requeridos para el SGSI. Realizar un análisis de brechas.	1. Caso de negocio. 2. Obtener apoyo de la alta dirección. 3. Aplicación de encuestas y entrevistas. 4. Validación de documentos.	Evaluación y recopilación de información para el desarrollo del plan de implementación del SGSI.	X					
FASE II PLANIFICACIÓN (PLAN) Realizar de manera metódica las actividades de planificación exigidas por la norma, alineándolas con la política y los objetivos del SGSI dentro de su ámbito de aplicación.	Realizar análisis de Riesgos	5. Definir metodología para la gestión de los riesgos. 6. Inventario de activos de información. 7. Desarrollar matriz y plan de tratamiento de riesgos.			X	X			

	Declaración de la política y los objetivos de seguridad de la información. Comprensión de la organización y su contexto.	8. Reformulación de la política y objetivos de seguridad de la información. 9. Confeccionar una SOA (Statement of Applicability). 10. Análisis FODA, PESTEL.			X				
	Definir el alcance del SGSI.	11. Definición y redacción de documento de alcance y límites del SGSI			X				
FASE III DESPLIEGUE (DO) Desplegar las actividades planificadas para la implementación del SGSI.	Elaborar planes de trabajo priorizado. Implementación de controles seleccionados. Evaluación de los riesgos.	12. Políticas de SI implementadas. 13. Plan de comunicación y capacitación. 14. Documento oficial de controles seleccionados. 15. Desarrollar matriz y plan de tratamiento de riesgos.				X	X	X	

FASE IV **REVISIÓN(CHECK)** Llevar a cabo actividades de revisión del SGSI para demostrar el cumplimiento de los requisitos de la NTP ISO 27001:2022	Monitorear el desempeño del SGSI. Estableces KPIs.	16. Informe de Evaluación de la eficacia de los procesos y procedimientos implementados en el SGSI.				X	X	X	
	Auditorías internas.	17. Informe de los resultados de la auditoría interna.						X	
FASE V **CONSOLIDACIÓN (ACT)** Aplicar las mejoras y correcciones al SGSI para asegurar el cumplimiento de los requisitos	Implementación de acciones correctivas. Desarrollar, corregir y mejorar documentación nueva o existente. Desarrollo de las actividades para evidenciar la mejora continua del SGSI.	18. Definir un proceso para resolver problemas y no conformidades. 19. Definir un procedimiento de acción y correctiva. 20. Elaborar planes de acción.							X

Fuente: (Elaboración propia)

6.7 PRESUPUESTO

Los valores especificados en el siguiente presupuesto no cuentan con cotizaciones oficiales para los productos y servicios considerados, ya que son aproximaciones; sin embargo, se han basado en la opinión y valoraciones de expertos en el tema e investigación propia.

Tabla 22. Presupuesto de la implementación del SGSI

Concepto	Descripción	Cantidad	Costo Mínimo	Costo Máximo
Consultoría y Asesoría				
Contratación de consultoría de empresa certificadora en Seguridad de la Información	Evaluación inicial, desarrollo de políticas y procedimientos, asesoría durante la implementación.	1	$ 10,000.00	$ 20,000.00
Formación y Capacitación				
Capacitación del Personal	Cursos y talleres para empleados sobre prácticas de seguridad, peligros informáticos y concienciación.	1	$ 5,000.00	$ 8,000.00
Certificación de Auditor Interno ISO 27001	Formación y certificación de personal interno para realizar auditorías del SGSI.	2	$ 1,000.00	$ 2,000.00
Herramientas y Tecnología				
PILAR RM	Licencias y configuración de software específico para la gestión de la seguridad de la información.	1	$ 1,000.00	$ 2,500.00
Herramientas de Seguridad	Firewall, antivirus, sistemas de detección de intrusiones, cifrado de datos, etc.	2	$ 7,000.00	$ 12,000.00
Documentación y Procedimientos				

Desarrollo de Documentación	Creación de políticas, procedimientos, manuales y registros necesarios para el SGSI.	1	$ 1,000.00	$ 3,000.00
Auditorías y Certificación				
Auditoría Externa Inicial	Evaluación por parte de una entidad certificadora para la conformidad con ISO/IEC 27001.	1	$ 5,000.00	$ 7,000.00
Certificación ISO/IEC 27001	Proceso de certificación formal, incluyendo auditorías de seguimiento.	1	$ 4,000.00	$ 6,000.00
Mantenimiento y Mejoras Continuas				
Costos Anuales de Mantenimiento	Actualizaciones, auditorías internas, y ajustes continuos para mantener la conformidad y mejorar el sistema.	1	$ 3,000.00	$ 5,000.00
TOTAL			**$ 37,000.00**	**$65,500.00**

Fuente: (Elaboración propia)

REFERENCIAS BIBLIOGRÁFICAS

Alberto Marradi, N. A. (2007). Metodología de las Ciencias Sociales. Emece Editores. Consultado el 22 de abril de 2024.

Alemán Novoa, H. & Rodríguez Barrera, C. (2015). Metodologías Para el análisis de riesgos en los SGSI. https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1754. Consultado el 20 de mayo de 2024.

Amazon Web Services. (11 de mayo de 2024). What is a database. https://aws.amazon.com/es/what-is/database/. Consultado el 29 de abril de 2024.

Benavides, E., Fuertes, W., Sanchez, S., & Nuñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. Ciencia y Tecnología, 13(1), 97-104. Consultado el 2 de mayo de 2024.

Bhat, A., (mayo 2024). Investigación exploratoria: tipos y características. Questionpro. https://www.questionpro.com/blog/exploratory-research/ . Consultado el 6 de mayo de 2024.

Centeno, C. M. (diciembre de 2017). Innovare - Ciencia y Tecnología. https://www.unitec.edu/innovare/published/volume-6/number-2/6210-la-brecha-existente-en-la-ciberseguridad-en-honduras.pdf. Consultado el 28 de abril de 2024.

Certiprof, (2022) .ISO 27001 LEAD IMPLEMENTER CERTIFIED. https://certiprof.com/pages/iso-27001-certified-lead-implementer-i27001cli . Consultado el 15 de mayo de 2024.

Cisco. (11 de mayo de 2024). What is Information Security? https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html . Consultado el 11 de mayo de 2024.

Confianza SA-FGR. (23 de enero de 2021). https://www.confianza.hn/norma-iso-iec-270012013-confianza-sa-fgr-certificada-en-seguridad-de-la-informacion/ . Consultado el 2 de mayo de 2024.

Cortes Malagón, J. & Pulido Espinosa J. (2023). Diseño de un Sistema de Gestión de Seguridad

de la Información (SGSI) para los procesos críticos de Summum Project basado en la norma NTC-ISO-IRC-27001: 2022. http://repository.unipiloto.edu.co/handle/20.500.12277/13402. Consultado el 29 de mayo de 2024.

Costa, C. (2019). LinkedIn. https://es.linkedin.com/pulse/la-gesti%C3%B3n-de-seguridad-informaci%C3%B3n-se-detiene-con-claudio-costa . Consultado el 2 de mayo de 2024.

Costa, C. (Feb de 2019). https://es.linkedin.com/pulse/certificaci%C3%B3n-del-sistema-de-gesti%C3%B3n-seguridad-la-claudio-costa?trk=articles_directory . Consultado el 2 de mayo de 2024.

Criterio. (30 de octubre de 2019). Ley de ciberseguridad de Honduras es ambigua y se enmarca en el odio. https://criterio.hn/ley-de-ciberseguridad-de-honduras-es-ambigua-y-se-enmarca-en-el-odio/ . Consultado el 2 de mayo de 2024.

Cruz Garcia, M. A. (2019). Fuentes de Información. Boletín Científico De Las Ciencias Económico Administrativas Del ICEA, 8(15), 57-58. https://doi.org/10.29057/icea.v8i15.4864 . Consultado el 12 de mayo de 2024.

ECIIA (septiembre 2021). Risk in Focus 2022: hot topics for internal auditors. https://www.eciia.eu/2021/09/risk-in-focus-2022-hot-topics-for-internal-auditors/ . Consultado el 15 de mayo de 2024.

FARN, Kwo-Jean, LIN, Shu-Kuo y FUNG, Andrew Ren-Wei. A study on information security management system evaluation: assents, threat and vulnerability. En: Computer Standards& Interfaces. Vol. 26, No. 6 (2004); p. 507 . Consultado el 12 de mayo de 2024.

Fastercapital. (25 de abril 2024). Propuesta de investigación cualitativa como redactar y presentar su propuesta de investigación de mercados. https://fastercapital.com/es/contenido/Propuesta-de-investigacion-cualitativa--como-redactar-y-presentar-su-propuesta-de-investigacion-de-mercados.html#Plan-de-an-lisis-de-datos . Consulado el 6 de mayo de 2024.

García, M. A. (2019). Boletín Científico de las Ciencias Económico Administrativas del ICEA. https://repository.uaeh.edu.mx/revistas/index.php/icea/article/view/4864 . Consultado el

12 de mayo de 2024.

Global Standards. (2024). ¡ISO CUMPLE SU 70 ANIVERSARIO. https://www.globalstd.com/blog/iso-cumple-su-70-aniversario/ . Consultado el 2 de mayo de 2024.

Gómez Fernández, L. & Fernández Rivero, P. P. (2018). Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad: (ed.). AENOR - Asociación Española de Normalización y Certificación. https://elibro.net/es/lc/unitechn/titulos/53624 . Consultado el 20 de mayo de 2024.

Grupo-fraga. (2024). 6 pasos para realizar el análisis de brechas según la ISO 27001. https://grupo-fraga.com/6-pasos-para-realizar-el-analisis-de-brechas-segun-la-iso-27001/ . Consultado el 2 de junio de 2024.

Guerrero-Aguiar, M., Medina-León, A., & Nogueira-Rivera, D. (2020). Procedimiento de gestión de riesgos como apoyo a la toma de decisiones. Ingeniería Industrial, XLI (1), 4101. Consultado el 20 de mayo de 2024.

Guía para implementar un sistema de gestión de riesgos, según la ISO 31000. (2024). piranirisk. https://www.piranirisk.com/es/academia/especiales/guia-del-sistema-de-gestion-de-riesgos-iso-31000. Consultado el 20 de mayo de 2024.

Harán, J. (31 de agosto de 2023). ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina. Welivesecurity. https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/ . Consultado el 2 de mayo de 2024.

Hernández-Sampieri, R., & Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Consultado el 6 de mayo de 2024

Hugo Sanchez Carlessi, C. R. (2015). Metodología y Diseños en la Investigación Científica. Business Support Aneth SRL. Consultado el 5 de mayo de 2024

Instituto de Previsión Militar. (13 de diciembre de 2022). https://grupoipm.hn/certificacion-de-norma-iso/ . Consultado el 8 de mayo de 2024.

Intedya. (12 de mayo de 2024). Impact Mobile alcanza su certificación ISO 27001:2013. https://honduras.intedya.com/formacion/actualidad.php?id=3638 . Consultado el 8 de mayo de 2024.

IPANDETEC. (enero de 2019). Estudio Centroamericano de Protección de Datos - Honduras. Consultado el 8 de mayo de 2024.

Kaspersky. (15 de mayo de 2024). https://latam.kaspersky.com/resource-center/threats/spyware . Consultado el 8 de mayo de 2024.

LADINO A., M. I., VILLA S., P. A., & LÓPEZ E., A. M. (2011). FUNDAMENTOS DE ISO 27001 Y SU APLICACIÓN EN LAS EMPRESAS. Scientia Et Technica, XVII (47), 334-339. Consultado el 22 de mayo de 2024.

Leeuw, K. d. (2007). The History of Information Security: A Comprehensive Handbook. Elsevier B.V. Consultado el 28 de abril de 2024.

López Rimari, R. P. (2020). Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura [Tesis de Grado en Académico de Bachiller en Ingeniería de Sistemas, Universidad Peruana Unión]. Repositorio de Tesis, Universidad Peruana Unión. http://hdl.handle.net/20.500.12840/3699 . Consultado el 20 de mayo de 2024.

MAGERIT versión 3. (2023). Portal administración tecnológica. https://administracionelectronica.gob.es/ctt/magerit . Consultado el 10 de mayo de 2024.

MalwareByte. (17 de mayo de 2024). Que es ransomware. https://es.malwarebytes.com/ransomware/ . Consultado el 2 de mayo de 2024.

Marinas, J. M. (2005). “10 temas comunes al psicoanálisis y a la investigación so-cial”, Arxius de Ciències Socials, 12-13, pp. 129-140. Consultado el 29 de abril de 2024.

Microsoft Corporation. (25 de mayo de 2024). ¿Qué es Microsoft Forms?: https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-microsoft-forms-6b391205-523c-45d2-b53a-fc10b22017c8 . Consultado el 12 de mayo de 2024.

Microsoft Corporation. (25 de mayo de 2024). Introducción a Microsoft Teams.

https://support.microsoft.com/es-es/office/introducci%C3%B3n-a-microsoft-teams-b98d533f-118e-4bae-bf44-3df2470c2b12 . Consultado el 12 de mayo de 2024.

Microsoft Corporation. (25 de mayo de 2024). Tareas básicas en Excel. https://support.microsoft.com/es-es/office/introducci%C3%B3n-a-microsoft-teams-b98d533f-118e-4bae-bf44-3df2470c2b12 . Consultado el 12 de mayo de 2024.

Movitext. (5 de mayo de 2024). https://www.movitext.com/ES/ismp.html . Consultado el 12 de mayo de 2024.

Moya, J. G. (2023). Revolución de la ciberseguridad en la cuarta revolución industrial. Revista Ingeniería e Innovación del Futuro, 2(2), 6-20. Consultado el 11 de mayo de 2024.

Natalucci, F., Qureshi, M, Suntheim, F. (10 de abril de 2024). Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera. IMF. https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability . Consultado el 10 de mayo de 2024.

NIST. (Junio de 2017). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1 . Consultado el 10 de mayo de 2024.

Ordoñez, W., (19 de Julio de 2023). Todos los principios de la seguridad de la información. Grouphacking. https://www.grouphacking.com/ciberseguridad/todos-los-principios-de-la-seguridad-de-la-informacion/ . Consultado el 10 de mayo de 2024.

Organización Internacional de Normalización. (2022). About ISO. https://www.iso.org/about-us.html . Consultado el 12 de mayo de 2024.

Organización Internacional de Normalización. (2022). ISO Survey of certifications to management system standards - Full results. https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top. Consultado el 12 de mayo de 2024.

Otzen, T., & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. International journal of morphology, 35(1), 227-232. Consultado el 10 de mayo de 2024.

Palomino., D., (7 diciembre 2022) Cambios en el ISO/IEC 27001 versión 2022.Cynthus. https://www.cynthus.com.mx/cambios-en-el-iso-iec-27001-version-2022/. Consultado el 13 de mayo de 2024.

Pérez-Mergarejo, E., Pérez-Vergara, I., & Rodríguez-Ruíz, Y. (2014). Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. *Ingeniería Industrial*, *35*(2), 184-198. Consultado el 18 de mayo de 2024.

Presentación, G. S. B. (2023). BENEFICIOS DE LAS NORMAS ISO 27000. HIGH TECH-ENGINEERING JOURNAL, 3(2), 86-88. Consultado el 18 de mayo de 2024.

¿Qué es PILAR? (2024). CCN-CERT.https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar. Consultado el 19 de mayo de 2024.

Ramos Galarza, C.A., (2020). Los alcances de una investigación. EDITORIAL CienciAmérica. Revista de divulgación científica de la Universidad Tecnológica Indoamérica Vol. 9 Núm. 3 Pág. 1-6. Consultado el 10 de mayo de 2024.

Referencias normativas ISO 27000. (mayo 2024). normaiso27001.https://normaiso27001.es/referencias-normativas-iso-27000/. Consultado el 13 de mayo de 2024.

Robitiki, Ayo. (2015). Guideline for Critical Information Infrastructure Protection in Nigeria. Abuja: Research Gate. https://doi.org/http://dx.doi.org/10.13140/RG.2.1.2407.8321. Consultado el 3 de mayo de 2024.

Rodríguez Parra, C. F., (2010). SEGURIDAD DE LA INFORMACIÓN: ESTRATEGIA PARA FORTALECER EL GOBIERNO CORPORATIVO. Revista de Derecho Privado, (43), 3-24. Consultado el 20 de mayo de 2024.

Rodríguez, J. L. (2017). Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO27001 para laboratorios servicios farmacéuticos de calidad SFC LTDA... [Monografía, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/12598. Consultado el 20 de mayo de 2024.

RSM. (9 de junio 2024). ¿En qué consiste una matriz de riesgos?

https://www.rsm.global/peru/es/aportes/blog-rsm-peru/en-que-consiste-una-matriz-de-riesgos. Consultado el 24 de mayo de 2024.

Sampieri, R. H. (1997). Metodología de la Investigación. Enero. Consultado el 28 de abril de 2024.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI). (16 de enero de 2023). cstbusiness. https://cstbusiness.co/. Consultado el 20 de mayo de 2024.

Solano Méndez, G. E. (2020). Propuesta mediante la normativa ISO 27001 para la gestión de la seguridad de la información en la empresa Udersol en Costa Rica. [Proyecto de Graduación de Licenciatura, Universidad Latina de Costa Rica]. Repositorio Institucional de la Universidad Latina de Costa Rica. https://hdl.handle.net/20.500.12411/293. Consultado el 25 de mayo de 2024.

Superintendencia de Economía Popular y Solidaria. (1 de junio de 2024). Superintendencia de Economía Popular y Solidaria. https://www.seps.gob.ec/ . Consultado el 1 de junio de 2024.

Villamizar. C., (28 de septiembre de 2023). 5 claves para la implementación de su SGSI: https://www.globalsuitesolutions.com/ . Consultado el 1 de junio de 2024.

Viteri, P. (7 de noviembre 2023). Análisis de Brechas de ISO 27001.LinkedIn https://es.linkedin.com/pulse/an%C3%A1lisis-de-brechas-iso-27001-c%C3%A9sar-paul-viteri-pe%C3%B1afiel-w97ze. Consultado el 2 de junio de 2024.

Zapata, A. (2016). Ciclo de la calidad PHVA. Universidad Nacional de Colombia. Consultado el 2 de junio de 2024.

Ministerio de Hacienda y Administraciones Publicas. (1 de Junio de 2024). *CCN-CERT*. Obtenido de https://www.ccn-cert.cni.es/es/documentos-publicos/1789-magerit-libro-i-metodo/file?format=html. Consultado el 1 de junio de 2024.

Balmaceda, C. (2023). Métodos mixtos de investigación para principiantes. Julio del 2023. Consultado el 7 de agosto de 2024

ANEXOS

ANEXO 1 - TEST DE CUMPLIMIENTO NORMATIVO 27001-2022 EN SAN SERVICES S. DE R. L

Test de cumplimiento normativo 27001:2022 en San Services S. de R. L.

Posibles respuestas:

- Si
- No

La Organización y su Contexto

1. ¿Están identificados los objetivos del SGSI (Sistema de Gestión de la Seguridad de la Información)?
2. ¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?
3. ¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la información?
4. ¿Se han identificado las partes interesadas?
5. ¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?
6. ¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?
7. ¿Se ha determinado el alcance del SGSI y se conserva información documentada?
8. ¿El sistema de Gestión de Seguridad de la Información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?

Liderazgo

1. ¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?
2. ¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?
3. ¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?
4. ¿Se ha definido una Política de la Seguridad de la Información?
5. ¿Se ha establecido un marco que permita el establecimiento de objetivos?

6. ¿Se ha comunicado la política de la Seguridad de la Información a las partes interesadas y a toda la empresa?
7. ¿Se mantiene información documentada de la política del SGSI y de sus objetivos?
8. ¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?
9. ¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?

Planificación

1. ¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?
2. ¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?
3. ¿Se ha definido y desarrollado el proceso de evaluación de riesgos para la seguridad de la información para que sea repetible y garantice resultados coherentes, válidos y comparables?
4. ¿Se han establecido criterios para elaborar una declaración de aplicabilidad?
5. ¿Se mantiene información documentada de los puntos anteriores?
6. ¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?
7. ¿Se ha planificado los objetivos de la Seguridad de la información mediante alguno de los siguientes métodos: ¿Asignación de Responsabilidades - Cronograma de ejecución temporal - Método de evaluación?
8. ¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?

Soporte

1. ¿Ha determinado y proporcionado los recursos necesarios para establecer, implantar, mantener y mejorar continuamente el SGSI?
2. ¿Ha determinado las competencias necesarias para quienes desempeñan las funciones del SGSI?
3. ¿Se mantiene información actualizada sobre la competencia del personal?
4. ¿Se ha asegurado de que las personas que realizan trabajos bajo el control de la organización conocen la política del SGSI?
5. ¿Se ha asegurado de que las personas que realizan trabajos bajo el control de la organización conocen su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de un mejor rendimiento de la seguridad de la información?
6. ¿Se ha asegurado de que las personas que realizan trabajos bajo el control de la organización conocen las implicaciones de no ajustarse a los requisitos del sistema de gestión de la seguridad de la información?
7. ¿Se comunica la política de Seguridad de la Información con las responsabilidades de cada uno?
8. ¿Existe un proceso para comunicar las deficiencias o malas prácticas en la Seguridad de la Información?

9. ¿Se ha establecido la información documentada requerida por la norma y necesaria para la implantación y el funcionamiento eficaces del SGSI?
10. ¿Ha determinado la organización qué comunicaciones internas y externas pueden ser relevantes?
11. ¿Se controla la información documentada de forma que esté disponible y adecuadamente protegida, distribuida, almacenada, retenida y bajo control de cambios, incluyendo los documentos de origen externo requeridos por la organización para el SGSI?

Operaciones

1. ¿Se han guardado pruebas documentadas que demuestren que los procesos se han llevado a cabo según lo previsto?
2. ¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el SGSI o procesos de Seguridad?
3. ¿Existe un plan para determinar la necesidad de introducir cambios en el SGSI y gestionar su implantación?
4. Cuando se planifican cambios, ¿se llevan a cabo de forma controlada y se toman medidas para mitigar cualquier efecto adverso?
5. En el caso de los procesos proporcionados externamente, ¿se controlan y aplican adecuadamente?
6. ¿Se llevan a cabo evaluaciones de los riesgos para la seguridad de la información a intervalos planificados o cuando se producen cambios significativos, y se conserva la información documentada?
7. ¿Ha planificado la organización acciones para abordar los riesgos y las oportunidades y las ha integrado en los procesos del sistema?
8. ¿Existe un proceso para conservar la información documentada sobre los resultados de la evaluación de riesgos para la seguridad de la información?
9. ¿Existe un proceso para obtener la aprobación del tratamiento del riesgo y del riesgo residual por parte de los responsables del riesgo?
10. ¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?
11. ¿Se documenta el nivel de aplicación de todos los controles a aplicar?

Evaluación del Desempeño

1. ¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?
2. ¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?
3. ¿Ha determinado qué debe supervisarse y medirse, cuándo, por quién, los métodos que deben utilizarse y cuándo se evaluarán los resultados?
4. ¿Están documentados los resultados del seguimiento y la medición?
5. ¿Ha establecido la organización un programa de auditorías internas para comprobar que el SGSI es eficaz y se ajusta a los requisitos de la norma ISO/IEC 27001 y a los propios requisitos de la organización?

6. ¿Los resultados de estas auditorías se comunican a la dirección, se documentan y se conservan?
7. Cuando se identifican no conformidades, ¿ha establecido la organización procesos adecuados para gestionar las no conformidades y las acciones correctivas relacionadas?
8. ¿Lleva a cabo la alta dirección revisiones regulares y periódicas del SGSI?
9. ¿Incluyen las aportaciones a la revisión de la dirección los cambios en las cuestiones externas e internas y los cambios en las necesidades de las partes interesadas?
10. ¿Se han tenido en cuenta los comentarios sobre el rendimiento de la seguridad de la información como una forma de contribuir a la revisión de la gestión?
11. ¿El resultado de la revisión de la gestión del SGSI identifica cambios y mejoras?
12. ¿Se dispone de información documentada que demuestre los resultados de la revisión de la gestión?

Mejora

1. ¿Se han identificado acciones para controlar, corregir y tratar las consecuencias de las no conformidades?
2. ¿Se ha evaluado la necesidad de actuar para eliminar la causa raíz de las no conformidades y evitar que vuelvan a producirse?
3. ¿Se han implantado y revisado las acciones identificadas para comprobar su eficacia y han dado lugar a mejoras en el SGSI?
4. ¿Se guarda información documentada como prueba de la naturaleza de las no conformidades, las acciones tomadas y los resultados?

ANEXO 2 – TEST DE CUMPLIMIENTO DE CONTROLES ANEXO A ISO 27001-2022 EN SAN SERVICES S. DE R. L

Test de cumplimiento de controles Anexo A ISO 27001:2022 en San Services S. de R. L.

Posibles respuestas:

- Totalmente en desacuerdo
- En desacuerdo
- Neutral
- De acuerdo
- Totalmente de acuerdo

Sección A5 - Controles Organizacionales

1. A5.1 ¿La dirección ha publicado y aprobado las políticas de la seguridad de la información, y son estas comunicadas a todo el personal relevante, y revisada cada cierto tiempo de manera planificada para verificar si ocurrieron cambios significativos?
2. A5.2 ¿Se han definido los roles y responsabilidades de seguridad de la información de acuerdo con las necesidades de la organización?
3. A5.3 ¿Se ha hecho una separación entre los deberes y las áreas conflictivos en términos de responsabilidad?
4. A5.4 ¿Existe una exigencia para aplicar la seguridad de la información de forma acorde con la política y procedimientos ya establecidos por la organización?
5. A5.5 ¿Existe comunicación entre la organización y las autoridades pertinentes?
6. A5.6 ¿Existen vías de comunicación con foros especializados, organizaciones o asociaciones especializados en Seguridad por parte de la organización?
7. A5.7 ¿Se recopila y analiza información relacionada a las nuevas amenazas a la seguridad de la información con el objetivo de generar información que sirva a la organización?
8. A5.8 ¿Se integra la seguridad de la información en la gestión de los proyectos de la organización?
9. A5.9 ¿Se mantiene un inventario de información que liste activos asociados?
10. A5.10 ¿Se han implementado reglas para la regulación de procedimientos para el manejo de la información y otros activos asociados?
11. A5.11 ¿Existe alguna cláusula que exija que el personal u otras partes interesadas devuelvan todos los activos que estén en su poder a la organización al terminar su empleo/acuerdo/contrato?

12. A5.12 ¿Se clasifica la información de acuerdo a las necesidades de seguridad de la información de la organización?
13. A5.13 ¿Existe un procedimiento que permita el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización?
14. A5.14 ¿Existen reglas/procedimientos/acuerdos de transferencia de información dentro de la organización?
15. A5.15 ¿Las reglas de control de acceso físico y lógico a la información fueron establecidas en base de los requisitos de seguridad de la información y del negocio?
16. A5.16 ¿Existe un ciclo de vida para las identificaciones usadas por los empleados con acceso a la información?
17. A5.17 ¿Existe un proceso de gestión de la información de autenticación que provea asesoramiento al personal sobre el manejo adecuado de sus credenciales de autenticación?
18. A5.18 ¿Se gestionan los derechos de acceso a la información de acuerdo con la política y las reglas de control de acceso específicas de la organización?
19. A5.19 ¿Existen procesos definidos para gestionar la seguridad de la información asociada con el uso de los productos o servicios de los proveedores de la organización?
20. A5.20 ¿Se han establecido los requisitos de seguridad de la información con cada proveedor en función del tipo de relación que la organización tiene con ellos?
21. A5.21 ¿Existen procesos definidos para gestionar la seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnologías de la información y la comunicación?
22. A5.22 ¿Se gestionan y revisan periódicamente los cambios en las prácticas de seguridad de la información de los proveedores de servicios?
23. A5.23 ¿Se han establecido procesos de adquisición, uso y gestión de los servicios en la nube de acuerdo con los requisitos de seguridad de la información de la organización?
24. A5.24 ¿Se han definido y establecido procesos que permitan a la organización estar preparada para la gestión de incidentes de seguridad?
25. A5.25 ¿La organización evalúa los eventos de seguridad y decide si se clasificaran como incidentes de seguridad de la información?
26. A5.26 ¿Se responden a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados?
27. A5.27 ¿Se utiliza el conocimiento adquirido de incidentes previos para fortalecer y mejorar los controles de seguridad existentes?
28. A5.28 ¿La organización posee procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información?
29. A5.29 ¿Existe un plan que permita a la organización mantener la seguridad de la información en un nivel adecuado durante una interrupción?
30. A5.30 ¿Las TIC (Tecnologías de la Información y Comunicación) están debidamente planificadas y probadas según los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC?
31. A5.31 ¿La organización tiene identificados y documentados los requisitos legales y contractuales relevantes para la seguridad de la información?
32. A5.32 ¿La organización posee procedimientos apropiados para proteger los derechos de propiedad intelectual?

33. A5.33 ¿La organización protege sus registros contra perdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada?
34. A5.34 ¿La organización ha identificado y cumplido los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y requisitos
35. A5.35 ¿La organización revisa de forma independiente los enfoques para gestionar la seguridad de la información en intervalos planificados?
36. A5.36 ¿La organización revisa periódicamente las políticas, reglas y estándares específicos que permitan el cumplimiento de la política de seguridad de la información?
37. A5.37 ¿La organización documenta y pone a disposición del personal los procedimientos operativos que permitan el procesamiento de información?

Sección A6 - Controles de Personas

1. A6.1 ¿La organización realiza controles de verificación de antecedentes de todos los candidatos antes de que se unan a la organización bajo las leyes, reglamentos y requisitos comerciales y según la clasificación de la información a la que accederá y los riesgos relacionados con ello?
2. A6.2 ¿Los acuerdos contractuales de trabajo establecen las responsabilidades del personal y de la organización en materia de seguridad de la información?
3. A6.3 ¿El personal de la organización reciben capacitaciones y actualizaciones periódicas de la política de seguridad y sus procedimientos?
4. A6.4 ¿La organización ha definido y comunicado acerca del proceso disciplinario que se tomara contra el personal que haya cometido una violación a la política de seguridad de la información?
5. A6.5 ¿La organización comunica a su personal acerca de las políticas de confidencialidad que aplican aun cuando el contrato laboral haya terminado?
6. A6.6 ¿La organización ha identificado/documentado/revisado y comunicado a su personal acerca de los acuerdos de confidencialidad o no divulgación?
7. A6.7 ¿La organización ha implementado medidas de seguridad para el personal que trabaja de manera remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización?
8. A6.8 ¿La organización ofrece un mecanismo para que el personal informe eventos de seguridad de la información que hayan observado o sospechado a través de canales apropiados?

Sección A7 - Controles Físicos

1. A7.1 ¿La organización ha definido perímetros de seguridad que permitan proteger las áreas que contienen información y otros activos asociados?
2. A7.2 ¿Las áreas seguras de la organización están protegidas por controles de entrada y puntos de acceso apropiados?
3. A7.3 ¿La organización ha diseñado e implementado la seguridad física de las oficinas, salas e instalaciones?
4. A7.4 ¿La organización monitorea continuamente sus locales para evitar el acceso físico no autorizado?
5. A7.5 ¿La organización ha diseñado e implementado medidas de protección contra amenazas físicas y ambientales, y contra otras amenazas físicas intencionales o no intencionales a la infraestructura?

6. A7.6 ¿La organización ha diseñado e implementado medidas de seguridad para trabajar en áreas seguras?
7. A7.7 ¿La organización ha definido y hace cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles, y las reglas de pantalla limpia para las instalaciones de procesamiento de información?
8. A7.8 ¿La organización se asegura de colocar el equipo que requiere acceso autorizado de forma segura y protegida?
9. A7.9 ¿La organización protege sus activos fuera del sitio?
10. A7.10 ¿Los medios de almacenamiento se gestionan a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización?
11. A7.11 ¿Las instalaciones de procesamiento de la información están protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo?
12. A7.12 ¿Los cables que transportan energía, datos o servicios de información de apoyo están protegidos contra intercepciones, interferencias o daños?
13. A7.13 ¿El equipo se mantendrá de forma correcta para garantizar la disponibilidad, integridad y confidencialidad de la información?
14. A7.14 ¿Se verifican los medios de almacenamiento con el fin de garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización?

Sección A8 - Controles Tecnológicos

1. A8.1 ¿Se protege la información almacenada, procesada o accesible a través de los dispositivos finales del usuario?
2. A8.2 ¿La asignación y uso de los derechos de acceso privilegiado se restringe y se gestiona?
3. A8.3 ¿El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica sobre el control de acceso?
4. A8.4 ¿El acceso de lectura y escritura al código fuente, las herramientas de desarrollo, y las bibliotecas de software se gestionarán adecuadamente?
5. A8.5 ¿Los procedimientos de autenticación se han implementado en función de las restricciones de acceso a la información y la política específica sobre el control de acceso?
6. A8.6 ¿El uso de los recursos se controla y ajusta de acuerdo con los requisitos de capacidad actuales y previstos?
7. A8.7 ¿La protección contra el malware es implementada y respaldada mediante la conciencia adecuada del usuario?
8. A8.8 ¿La organización toma las medidas apropiadas contra las vulnerabilidades técnicas de los sistemas de información en uso, y hace evaluaciones periódicas para verificar que vulnerabilidades presentan dichos sistemas?
9. A8.9 ¿Las configuraciones de seguridad, hardware, software, servicios y redes han sido debidamente establecidos, documentados, implementados y revisados?
10. A8.10 ¿La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento es eliminada cuando ya no es necesaria?
11. A8.11 ¿El enmascaramiento de datos se utiliza de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el

tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable?

12. A8.12 ¿Las medidas de prevención de fuga de datos se aplica a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible?
13. A8.13 ¿Las copias de seguridad de la información, el software y los sistemas se mantienen y prueban periódicamente de acuerdo con la política de copia de seguridad?
14. A8.14 ¿Las instalaciones de procesamiento de información se implementaron con suficiente redundancia para cumplir con los requisitos de disponibilidad?
15. A8.15 ¿Se producen, almacenan, protegen y analizan los registros de actividades, excepciones, fallas y otros eventos relevantes de las cuentas de usuario?
16. A8.16 ¿Las redes, los sistemas y las aplicaciones son monitoreados por comportamiento anómalo y se tomaran las acciones apropiadas para evaluar posibles incidentes de seguridad de la información?
17. A8.17 ¿Los relojes de los sistemas de procesamiento de información utilizados por la organización están sincronizados con las fuentes de tiempo aprobadas?
18. A8.18 ¿El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación están restringidos y estrictamente controlados?
19. A8.19 ¿Los procedimientos y medidas para gestionar la instalación segura de software en los sistemas operativos están implementados de forma adecuada?
20. A8.20 ¿Las redes y dispositivos de red están asegurados, administrados y controlados para proteger la información en los sistemas y aplicaciones?
21. A8.21 ¿Se ha identificado, implementado y controlado los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red?
22. A8.22 ¿Los grupos de servicios de información, usuarios y sistemas de información están segregados en las redes de la organización?
23. A8.23 ¿El acceso a sitios web externos se gestiona para reducir la exposición a contenido malicioso?
24. A8.24 ¿Se definieron e implementaron reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas?
25. A8.25 ¿Se establecieron y aplicaron reglas para el desarrollo seguro de software y sistemas?
26. A8.26 ¿Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones?
27. A8.27 ¿Se establecieron, documentaron y aplicaron principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información?
28. A8.28 ¿Los principios de codificación segura son aplicados al desarrollo de software?
29. A8.29 ¿Los procesos de pruebas de seguridad se definen e implementan en el ciclo de vida del desarrollo?
30. A8.30 ¿La organización dirige, monitorea y revisa las actividades relacionadas con el desarrollo de sistemas subcontratados?
31. A8.31 ¿Los entornos de desarrollo, prueba y producción están separados y protegidos?
32. A8.32 ¿Los cambios en las instalaciones de procesamiento de información y los sistemas de información están sujetos a procedimientos de gestión de cambios?
33. A8.33 ¿La información de las pruebas se seleccionó, protegió y gestiono adecuadamente?

34. A8.34 ¿Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos es planificado y acordado entre el evaluador y la gerencia correspondiente?

ANEXO 3. ENTREVISTA APLICADA PARA IDENTIFICACIÓN DE RIESGOS

ENTREVISTA

Como parte del diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001, estamos llevando a cabo esta entrevista abierta con el objetivo de identificar y evaluar los riesgos potenciales que podrían afectar la seguridad de la información en San Services. Su experiencia y conocimiento son fundamentales para comprender mejor las amenazas y vulnerabilidades que enfrentamos, así como para desarrollar estrategias efectivas de mitigación. Apreciamos sinceramente su colaboración en este proceso y su disposición para compartir sus perspectivas y experiencias. La información recopilada será tratada con la más estricta confidencialidad y se utilizará exclusivamente para fines académicos.

Identificación de Riesgos

1. ¿Qué eventos o situaciones podrían impedir el éxito de las operaciones o proyectos?
2. ¿Hay algún riesgo que haya enfrentado en proyectos similares en el pasado?
3. ¿Qué áreas o fases del proyecto/proceso considera más vulnerables a riesgos?
4. ¿Existen riesgos externos (económicos, políticos, legales, etc.) que puedan afectar este proyecto/proceso?

Causas de los Riesgos

5. ¿Cuáles son las principales causas de los riesgos que ha mencionado?
6. ¿Qué factores internos podrían contribuir a la ocurrencia de estos riesgos?
7. ¿Hay condiciones específicas que aumentarían la probabilidad de que estos riesgos se materialicen?

Consecuencias de los Riesgos

8. ¿Qué consecuencias tendría para el proyecto/proceso si estos riesgos se materializan?
9. ¿Cómo impactarían estos riesgos en el presupuesto, el cronograma, la calidad o la seguridad?
10. ¿Qué impacto tendrían estos riesgos en los stakeholders (clientes, empleados, proveedores, etc.)?

Probabilidad de Ocurrencia

11. ¿Qué tan probable consideras que es la ocurrencia de cada uno de los riesgos identificados?
12. ¿Existen indicadores o señales tempranas que podríamos monitorear para anticipar estos riesgos?
13. ¿Con qué frecuencia han ocurrido estos riesgos en proyectos/procesos anteriores?

Medidas de Mitigación

14. ¿Qué controles o medidas existen actualmente para prevenir o mitigar estos riesgos?
15. ¿Qué tan efectivas consideras que son las medidas de mitigación actuales?
16. ¿Qué acciones adicionales se podrían tomar para reducir la probabilidad o el impacto de estos riesgos?

Monitoreo y Respuesta

17. ¿Cómo se monitorean actualmente los riesgos en este proyecto/proceso?
18. ¿Quién es responsable de gestionar cada uno de estos riesgos?
19. ¿Qué planes de contingencia se tienen en caso de que los riesgos se materialicen?

Percepción y Prioridades

20. ¿Qué riesgos consideras más críticos y que deberían ser priorizados?
21. ¿Existen riesgos que, aunque tengan una baja probabilidad, podrían tener consecuencias catastróficas?
22. ¿Qué riesgos consideras aceptables y que pueden ser asumidos sin medidas adicionales?

Riesgos Tecnológicos y Operacionales

23. ¿Hay alguna tecnología clave que, si falla, podría poner en riesgo el proyecto/proceso?
24. ¿Cuáles son los riesgos operacionales más significativos que podríamos enfrentar?
25. ¿Existen dependencias críticas (proveedores, sistemas, infraestructuras) que podrían generar riesgos?

ANEXO 4. RESULTADOS DE LA ENCUESTA TEST DE CUMPLIMIENTO NORMATIVO 27001-2022 EN SAN SERVICES S. DE R. L

Encuestados			Contexto de la organización								Liderazgo									Planificacion							
			1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8
1	DevOps	Sr. Site Reliability Engineer	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
2	Bases de Datos	DBA	Si	Si	Si	Si	Si	No	No	Si	Si	Si	No	Si	Si	No	Si	Si	Si	No	Si	No	Si	Si	Si	Si	No
3	Business Systems (Databases)	Manager	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No	No	No	Si	Si	Si
4	Oracle Database Development	Senior Database Engineer	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No	Si	Si	No	Si	No	Si
5	Frontend development	Frontend Lead Engineer	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No
6	Microservicios	Team Lead	No	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	No	Si	No	No	No	No	No	No	No	No	No	No	No
		Total Si por Columna	**5**	**6**	**6**	**6**	**5**	**4**	**5**	**6**	**6**	**6**	**5**	**6**	**5**	**5**	**5**	**5**	**5**	**3**	**3**	**3**	**4**	**3**	**5**	**3**	**3**
		N° Población	**6**								**6**									**6**							
		Total Respuestas	**48**								**54**									**48**							
		Total Si por Requisito	**43**								**48**									**27**							
		% Cumplimiento	**89.6**								**88.89**									**56.25**							
		% Deseado	**100**								**100**									**100**							
		%Brecha	**10.4**								**11.11**									**43.75**							

Soporte											Operación											Evaluación del desempeño												Mejora			
1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4
Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	No	No	No	No	No	Si	Si	No	No	Si	Si	Si	Si	No	Si	No	Si	No	Si	No	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No	No	Si	Si	Si	Si	No	Si	Si	Si	Si
No	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No
Si	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No	No	No	Si	Si	Si	Si	Si	Si	Si	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No
Si	Si	No	Si	No	Si	No	No	No	Si	No	No	No	No	No	Si	No	No	No	No	Si	Si	No	No	No	No	No	No	No	No	No	No	No	No	Si	Si	Si	Si
5	**6**	**3**	**5**	**4**	**5**	**4**	**5**	**5**	**4**	**3**	**3**	**4**	**3**	**5**	**5**	**5**	**4**	**5**	**4**	**6**	**5**	**4**	**4**	**4**	**3**	**3**	**3**	**3**	**4**	**4**	**4**	**4**	**3**	**5**	**5**	**5**	**4**
6											**6**											**6**												**6**			
66											**66**											**72**												**24**			
49											**49**											**43**												**19**			
74.24											**74.24**											**59.72**												**79.17**			
100											**100**											**100**												**100**			
25.76											**25.8**											**40.28**												**20.83**			

ANEXO 5. RESULTADOS DE LA ENCUESTA TEST DE CUMPLIMIENTO DE CONTROLES ANEXO A ISO 27001-2022 EN SAN SERVICES S. DE R. L

	Controles Organizativos										
	Encuestados		A5.1	A5.2	A5.3	A5.4	A5.5	A5.6	A5.7	A5.8	A5.9	A5.10
1	DevOps	Sr. Site Reliability Engineer	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo
2	Bases de Datos	DBA	Totalmente en desacuerdo	Totalmente de acuerdo	Totalmente en desacuerdo	Totalmente de acuerdo	De acuerdo	En desacuerdo	Totalmente de acuerdo	En desacuerdo	De acuerdo	Neutral
3	Oracle Database Development	Senior Database Engineer	De acuerdo	De acuerdo	Neutral	Totalmente de acuerdo	De acuerdo	Neutral	De acuerdo	De acuerdo	En desacuerdo	De acuerdo
4	Business Systems (Databases)	Manager	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
5	Frontend development	Frontend lead	De acuerdo	De acuerdo	Neutral	Neutral	Neutral	En desacuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
6	Microservicios	Team Lead	En desacuerdo	De acuerdo	De acuerdo	En desacuerdo	De acuerdo	En desacuerdo	Totalmente en desacuerdo	Totalmente en desacuerdo	En desacuerdo	En desacuerdo

Totalmente de acuerdo	16.67	50.00	33.33	66.67	33.33	16.67	50.00	33.33	16.67	16.67
De acuerdo	50.00	50.00	16.67	0.00	50.00	16.67	33.33	33.33	50.00	50.00
Neutral	0.00	0.00	33.33	16.67	16.67	16.67	0.00	0.00	0.00	16.67
En desacuerdo	16.67	0.00	0.00	16.67	0.00	50.00	0.00	16.67	33.33	16.67
Totalmente en desacuerdo	16.67	0.00	16.67	0.00	0.00	0.00	16.67	16.67	0.00	0.00
TOTAL	100	100	100	100	100	100	100	100	100	100

A5.11	A5.12	A5.13	A5.14	A5.15	A5.16	A5.17	A5.18	A5.19	A5.20	A5.21
Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo
Totalmente de acuerdo	En desacuerdo	En desacuerdo	Totalmente en desacuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	En desacuerdo	Neutral	Neutral
En desacuerdo	Neutral	Neutral	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	Neutral	Neutral
Totalmente de acuerdo	Totalmente de acuerdo	Neutral	Totalmente de acuerdo	Neutral	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo
De acuerdo	Neutral	Neutral	De acuerdo	De acuerdo	De acuerdo	Neutral	Neutral	De acuerdo	Neutral	Neutral
Totalmente de acuerdo	En desacuerdo	En desacuerdo	De acuerdo	En desacuerdo	En desacuerdo	En desacuerdo	De acuerdo	En desacuerdo	De acuerdo	De acuerdo

66.67	16.67	16.67	33.33	0.00	50.00	33.33	50.00	33.33	16.67	16.67
16.67	16.67	0.00	50.00	66.67	33.33	33.33	33.33	33.33	33.33	33.33
0.00	33.33	50.00	0.00	16.67	0.00	16.67	16.67	0.00	50.00	50.00
16.67	33.33	33.33	0.00	16.67	16.67	16.67	0.00	33.33	0.00	0.00
0.00	0.00	0.00	16.67	0.00	0.00	0.00	0.00	0.00	0.00	0.00
100	100	100	100	100	100	100	100	100	100	100

A5.22	A5.23	A5.24	A5.25	A5.26	A5.27	A5.28	A5.29	A5.30	A5.31	A5.32	A5.33
Totalmente de acuerdo	Neutral	De acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo
Neutral	Neutral	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Neutral	De acuerdo	Totalmente de acuerdo
De acuerdo	De acuerdo	De acuerdo	Neutral	De acuerdo	De acuerdo	De acuerdo	Neutral	Neutral	De acuerdo	En desacuerdo	Neutral
Neutral	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Neutral	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
Neutral	En desacuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	Neutral	De acuerdo	De acuerdo	De acuerdo
En desacuerdo	Totalmente de a	De acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo

16.67	16.67	33.33	16.67	16.67	66.67	16.67	33.33	33.33	33.33	33.33	66.67
16.67	33.33	66.67	66.67	83.33	33.33	83.33	33.33	33.33	50.00	50.00	16.67
50.00	33.33	0.00	16.67	0.00	0.00	0.00	33.33	33.33	16.67	0.00	16.67
16.67	16.67	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	16.67	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
100	100	100	100	100	100	100	100	100	100	100	100

A5.34	A5.35	A5.36	A5.37	
Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	
Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	En desacuerdo	
De acuerdo	Neutral	En desacuerdo	De acuerdo	
Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	
Neutral	Neutral	Neutral	De acuerdo	
Totalmente de acuerdo	De acuerdo	De acuerdo	En desacuerdo	
				TOTAL
66.67	16.67	33.33	16.67	**31.98%**
16.67	50.00	33.33	50.00	**38.29%**
16.67	33.33	16.67	0.00	**16.22%**
0.00	0.00	16.67	33.33	**11.26%**
0.00	0.00	0.00	0.00	**2.25%**
100	100	100	100	100.00%

Global - Controles Organizativos		
Totalmente de acuerdo	71	31.98
De acuerdo	85	38.29
Neutral	36	16.22
En desacuerdo	25	11.26
Totalmente en desacuerdo	5	2.25
TOTAL	**222**	**100.00**

	Controles De Personas									
	Encuestados		A6.1	A6.2	A6.3	A6.4	A6.5	A6.6	A6.7	A6.8
1	DevOps	Sr. Site Reliability Engineer	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
2	Bases de Datos	DBA	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Neutral	En desacuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo
3	Oracle Database Development	Senior Database Engineer	Neutral	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
4	Business Systems (Databases)	Manager	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
5	Frontend development	Frontend lead	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
6	Microservicios	Team Lead	En desacuerdo	De acuerdo	Totalmente de acuerdo	En desacuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo

									TOTAL
Totalmente de acuerdo	50.00	16.67	50.00	33.33	33.33	50.00	50.00	50.00	**41.67%**
De acuerdo	16.67	83.33	50.00	33.33	50.00	50.00	50.00	50.00	**47.92%**
Neutral	16.67	0.00	0.00	16.67	0.00	0.00	0.00	0.00	**4.17%**
En desacuerdo	16.67	0.00	0.00	16.67	16.67	0.00	0.00	0.00	**6.25%**
Totalmente en desacuerdo	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	**0.00%**
TOTAL	100	100	100	100	100	100	100	100	100.00%

Global - Controles De Personas		
Totalmente de acuerdo	20	41.67
De acuerdo	23	47.92
Neutral	2	4.17
En desacuerdo	3	6.25
Totalmente en desacuerdo	0	0.00
TOTAL	**48**	**100.00**

	Controles Fisicos										
	Encuestados		A7.1	A7.2	A7.3	A7.4	A7.5	A7.6	A7.7	A7.8	A7.9	A7.10
1	DevOps	Sr. Site Reliability Engineer	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Neutral	Totalmente de acuerdo
2	Bases de Datos	DBA	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
3	Oracle Database Development	Senior Database Engineer	En desacuerdo	Neutral	Neutral	De acuerdo	En desacuerdo	Neutral	De acuerdo	Neutral	De acuerdo	Neutral
4	Business Systems (Databases)	Manager	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo
5	Frontend development	Frontend lead	Neutral	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	En desacuerdo	De acuerdo	De acuerdo	Neutral
6	Microservicios	Team Lead	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo

Totalmente de acuerdo	33.33	66.67	50.00	50.00	33.33	50.00	50.00	50.00	33.33	50.00
De acuerdo	33.33	16.67	33.33	50.00	50.00	33.33	33.33	33.33	50.00	16.67
Neutral	16.67	16.67	16.67	0.00	0.00	16.67	0.00	16.67	16.67	33.33
En desacuerdo	16.67	0.00	0.00	0.00	16.67	0.00	16.67	0.00	0.00	0.00
Totalmente en desacuerdo	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL	100	100	100	100	100	100	100	100	100	100

A7.11	A7.12	A7.13	A7.14
Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo
Totalmente de acuerdo	Neutral	Totalmente de acuerdo	Totalmente de acuerdo
De acuerdo	De acuerdo	De acuerdo	De acuerdo
Totalmente de acuerdo	Neutral	De acuerdo	Totalmente de acuerdo
De acuerdo	Neutral	De acuerdo	Neutral
Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo

66.67	33.33	33.33	50.00	**46.43%**
33.33	16.67	66.67	33.33	**35.71%**
0.00	50.00	0.00	16.67	**14.29%**
0.00	0.00	0.00	0.00	**3.57%**
0.00	0.00	0.00	0.00	**0.00%**
100	100	100	100	100.00%

Global - Controles Físicos		
Totalmente de acuerdo	39	46.43
De acuerdo	30	35.71
Neutral	12	14.29
En desacuerdo	3	3.57
Totalmente en desacuerdo	0	0.00
TOTAL	84	**100.00**

	Controles Tecnológicos										
	Encuestados		A8.1	A8.2	A8.3	A8.4	A8.5	A8.6	A8.7	A8.8	A8.9	A8.10
1	DevOps	Sr. Site Reliability Engineer	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
2	Bases de Datos	DBA	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Neutral	Totalmente de acuerdo	De acuerdo	De acuerdo	Neutral	De acuerdo	De acuerdo
3	Oracle Database Development	Senior Database Engineer	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
4	Business Systems (Databases)	Manager	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Neutral	De acuerdo	En desacuerdo
5	Frontend development	Frontend lead	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	Neutral
6	Microservicios	Team Lead	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	En desacuerdo	De acuerdo	De acuerdo

Totalmente de acuerdo	50.00	50.00	33.33	50.00	50.00	33.33	33.33	0.00	16.67	16.67
De acuerdo	50.00	50.00	66.67	33.33	50.00	66.67	66.67	50.00	83.33	50.00
Neutral	0.00	0.00	0.00	16.67	0.00	0.00	0.00	33.33	0.00	16.67
En desacuerdo	0.00	0.00	0.00	0.00	0.00	0.00	0.00	16.67	0.00	16.67
Totalmente en desacuerdo	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL	100	100	100	100	100	100	100	100	100	100

A8.11	A8.12	A8.13	A8.14	A8.15	A8.16	A8.17	A8.18	A8.19	A8.20	A8.21
Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
Neutral	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo
Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	Neutral	De acuerdo	De acuerdo	De acuerdo	De acuerdo
Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo
Neutral	Neutral	De acuerdo	De acuerdo	De acuerdo	De acuerdo	En desacuerdo	De acuerdo	De acuerdo	Neutral	Neutral
De acuerdo	Totalmente de acuerdo	De acuerdo	En desacuerdo	De acuerdo	De acuerdo	Neutral	De acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo

50.00	33.33	16.67	50.00	16.67	33.33	50.00	50.00	16.67	50.00	50.00
16.67	50.00	83.33	33.33	83.33	66.67	0.00	50.00	83.33	33.33	33.33
33.33	16.67	0.00	0.00	0.00	0.00	33.33	0.00	0.00	16.67	16.67
0.00	0.00	0.00	16.67	0.00	0.00	16.67	0.00	0.00	0.00	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
100	100	100	100	100	100	100	100	100	100	100

A8.22	A8.23	A8.24	A8.25	A8.26	A8.27	A8.28	A8.29	A8.30	A8.31
Totalmente de acuerdo	Totalmente de a	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo
Totalmente de acuerdo	De acuerdo	Neutral	En desacuerdo	En desacuerdo	En desacuerdo	En desacuerdo	En desacuerdo	Neutral	Totalmente de acuerdo
De acuerdo	De acuerdo	En desacuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	Neutral	De acuerdo
Totalmente de acuerdo	Totalmente de a	Neutral	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
Neutral	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo
Totalmente de acuerdo	Totalmente de a	En desacuerdo	En desacuerdo	En desacuerdo	En desacuerdo	Neutral	En desacuerdo	De acuerdo	Totalmente de acuerdo

66.67	50.00	16.67	0.00	33.33	33.33	16.67	16.67	0.00	50.00
16.67	50.00	16.67	66.67	33.33	33.33	50.00	50.00	66.67	50.00
16.67	0.00	33.33	0.00	0.00	0.00	16.67	0.00	33.33	0.00
0.00	0.00	33.33	33.33	33.33	33.33	16.67	33.33	0.00	0.00
0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
100	100	100	100	100	100	100	100	100	100

A8.32	A8.33	A8.34
Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo
Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo
Neutral	De acuerdo	Neutral
Totalmente de acuerdo	Neutral	De acuerdo
De acuerdo	De acuerdo	Neutral
Totalmente de acuerdo	De acuerdo	En desacuerdo

			TOTAL
66.67	16.67	33.33	**33.82%**
16.67	66.67	16.67	**48.04%**
16.67	16.67	33.33	**10.29%**
0.00	0.00	16.67	**7.84%**
0.00	0.00	0.00	**0.00%**
100	100	100	100.00%

Global - Controles Tecnológicos		
Totalmente de acuerdo	69	33.82
De acuerdo	98	48.04
Neutral	21	10.29
En desacuerdo	16	7.84
Totalmente en desacuerdo	0	0.00
TOTAL		**100.00**

ANEXO 6. DOCUMENTO DEL ALCANCE DEL SGSI EN SAN SERVICES

San Services S. de R.L.

DOCUMENTO SOBRE EL ALCANCE DEL SGSI

Código:	SANSERVICES-SGSI-DSA01
Versión:	V-0001
Fecha de Versión:	10 de junio del 2024
Creado por:	Alexander Bono Luis Tinoco
Aprobado por:	Gerencia TI
Nivel de confidencialidad:	10

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
08 de junio 2024	V-0001	Alexander Bono Luis Tinoco	Estructurar el documento inicial de acuerdo al objetivo del documento sobre el alcance del SGSI

Tabla de contenido

1. OBJETIVO Y ALCANCE

El objetivo del alcance del SGSI es definir los límites y la aplicabilidad del sistema dentro del área de TI en San Services S. de R.L., estableciendo las responsabilidades, procesos, activos y controles necesarios para proteger la información crítica de la empresa, socios, proveedores y clientes.

Este documento se aplica a toda la documentación y actividades dentro de SGSI.

2. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2022.

3. DEFINICIÓN DEL ALCANCE DEL SGSI

La organización necesita definir los limites del SGSI para decidir que información quiere proteger.

El SGSI se aplicará específicamente al área de TI de San Services, abarcando todos los sistemas, redes, aplicaciones, datos y personal involucrado en el desarrollo, mantenimiento y soporte de software. Esto incluye:

- Infraestructura de TI: Servidores, estaciones de trabajo, dispositivos de red (firewalls, switches, routers), almacenamiento y equipos de respaldo.
- Aplicaciones: Software en desarrollo, aplicaciones en producción, sistemas de control de versiones, herramientas de desarrollo y pruebas.
- Datos: Bases de datos, repositorios de código, documentos de diseño y especificaciones, información de clientes y proyectos.
- Comunicación: Sistemas de correo electrónico, mensajería interna, videoconferencias y otras formas de comunicación dentro del área de TI.
- Personal: Todos los empleados, contratistas y terceros que trabajen en el área de TI o manejen información crítica.

También se aplica para los activos de información críticos como:

- Código fuente: De todas las aplicaciones en desarrollo y en producción.
- Documentación: Proyectos, especificaciones técnicas, manuales de usuario y documentación administrativa.

- Configuraciones: De sistemas, redes y aplicaciones.
- Registros y logs: Actividades del sistema, accesos y eventos de seguridad.

4. EXCLUSIONES DEL ALCANCE

El SGSI se aplicará exclusivamente al área de TI, por lo tanto, queda excluido todo tipo de proceso, registro de sistema de gestión etc., de otras áreas ajenas a TI.

A su vez queda excluido todo equipo personal de los colaboradores como, laptops, teléfonos móviles, tabletas y otros dispositivos que nos son propiedad de la empresa y que no están registrados en la infraestructura de TI de San Services.

También serán excluidos todos los servicios que no estén bajo el control directo de San Services, tales como:

- Servicios en la nube gestionados por terceros.
- Sistemas que pertenecen a clientes o proveedores, que no son gestionados directamente por San Services.
- Software y herramientas que no hayan sido aprobadas por el área de TI de San Services y el cual no forme parte del inventario oficial de activos.

5. LÍMITES DEL SGSI

- Ubicaciones físicas: Oficinas y centros de datos donde el equipo de TI realiza sus actividades.
- Tecnologías: Hardware y software utilizados y administrados por el área de TI.
- Procesos de TI: Desarrollo de software, pruebas, implementación, mantenimiento, soporte técnico, gestión de cambios, gestión de incidentes y proyectos.

6. RESPONSABLES

- Jefe de operaciones de TI.
- Equipo de personas de seguridad de la información.

- Equipos de TI.

_____

Jefe de Operaciones de TI

ANEXO 7. VISTO BUENO ENTREGA PROYECTO FINAL

VISTO BUENO

CHIRINOS CHIRINOS JORGE RAUL
Para: LUIS ANTONIO TINOCO RIOS; ALEXANDER ENOC BONO RIVERA

Responder | Responder a todos | Reenviar | ...

Vie 28/06/2024 16:31

Estimados maestrantes, Alexander Enoc Bono Rivera y Luis Antonio Tinoco Ríos.

Luego de revisar el documento completo del Trabajo Final de Graduación titulado "**DISEÑO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN NORMA ISO 27001:2022 EN EMPRESA SAN SERVICES S. de R. L."** ". Tienen el **VISTO BUENO** para entregar a las autoridades correspondientes su proyecto final.

Les deseo el mayor de los éxitos, Dios les Bendiga.

Saludos.

M. Sc. Jorge Maradiaga
Docente e Investigador de Postgrado
Universidad Tecnológica Centroamericana (UNITEC)

*"**El precio de la educación solo se paga una vez, el precio de la ignorancia se paga toda la vida**"*

Responder | Responder a todos | Reenviar