

**Fortalecimiento y alineación de los
controles y procedimientos operativos
del proceso de Soporte en Tecnología
mediante su articulación y evaluación
continua dentro del Sistema de Gestión
de Seguridad de la Información (SGSI)
basado en riesgos de Skaphe Tecnología
S.A.S**

Trabajo final presentado por:	Dylan Esteban Casas Bayona, Jesús Andrés López Chirinos, Francisco Javier Ramos
Programa:	Especialización en Ciberseguridad
Docente:	Pedro Fabricio Echeverria Briones
Fecha:	2026-08-10

Índice de contenidos

Resumen	4
Abstract	4
1. Introducción	6
1.1. Objetivo General.....	6
1.2. Objetivos Específicos	6
1.3. Metodología	7
1.3.1. Identificación y Análisis del Problema.....	7
1.3.2. Planificación de la Solución	8
2. Identificación y descripción un problema al interior de la organización.....	10
2.1. Descripción de la empresa a intervenir.....	11
2.1.1. Misión	11
2.1.2. Visión	12
2.1.3. Mapa de procesos	13
2.1.4. Descripción del proceso a intervenir.....	15
2.1.5. Descripción del problema que presenta el proceso.....	17
3. Establecimiento de planes de acción para la solución del problema	20
3.1. Establecimiento de objetivos	22
3.2. Descripción de la solución	23
3.3. Secuencia de actividades para ejecución de la solución	29
3.4. Descripción de recursos necesarios para la ejecución de la solución.....	39
4. Definición del alcance de la solución, partes interesadas, cronograma y presupuestos. 46	
4.1. Alcance final de la solución	47
4.2. Identificación de responsables de las actividades para ejecución.....	50
4.3. Cronograma de ejecución.....	54

4.4.	Presupuesto.....	56
5.	Referencias bibliográficas	59

RESUMEN

El trabajo se centró en revisar cómo se están manejando hoy los temas de seguridad de la información dentro del proceso de Soporte en Tecnología de Skaphe Tecnología S.A.S. Al hacer la revisión se encontró que el área ya tiene varias cosas adelantadas: procedimientos para soporte, mantenimiento de equipos, gestión de respaldos y borrado de información, además de registros y controles que se usan en la operación diaria.

El problema aparece porque todo esto no está todavía organizado bajo una misma estructura. Algunos documentos son de años diferentes, otros se han actualizado recientemente y varios elementos del SGSI todavía están en construcción. Por eso fue necesario revisar qué se conserva, qué debe actualizarse y qué falta por completar.

A partir de ese análisis se tomó ISO/IEC 27001:2022 como referencia para ordenar el trabajo. Se planteó revisar los activos, identificar los riesgos más relevantes, relacionarlos con los controles existentes y definir acciones para los puntos que requieren mejora. También se incluyeron responsables, indicadores, cronograma, presupuesto y un plan de tratamiento.

La idea final es dejar una base organizada que permita continuar con la implementación del SGSI sin desconocer los controles y procedimientos que Skaphe ya viene utilizando.

Palabras clave: seguridad de la información, SGSI, ISO/IEC 27001:2022, gestión de riesgos, activos de información, soporte en tecnología.

ABSTRACT

The work focused on reviewing how information security is currently being managed within the Technology Support process at Skaphe Tecnología S.A.S. During the review, it was found that the area already has several elements in place, including procedures for technical support, equipment maintenance, backup management, and information deletion, as well as records and controls that are used as part of daily operations.

The main issue is that these elements are not yet organized under a single structure. Some documents were created in different years, others have been updated more recently, and

several ISMS components are still under development. For this reason, it was necessary to review what should be kept, what needs to be updated, and what still needs to be completed.

Based on this analysis, ISO/IEC 27001:2022 was taken as a reference to organize the work. The proposal includes reviewing the assets, identifying the most relevant risks, linking them to the existing controls, and defining actions for the areas that require improvement. It also includes assigned responsibilities, indicators, a schedule, a budget, and a risk treatment plan.

The final goal is to leave an organized foundation that allows Skaphe to continue with the implementation of the ISMS while taking advantage of the controls and procedures that the company already uses.

Keywords: information security, ISMS, ISO/IEC 27001:2022, risk management, information assets, technology support.

1. INTRODUCCIÓN

Este proyecto de aplicación en investigación-acción se centró en la identificación y resolución de la falta de actualización, articulación y evaluación de los controles y procedimientos operativos del proceso de Soporte en Tecnología dentro de un Sistema de Gestión de Seguridad de la Información basado en riesgos en Skaphe Tecnología S.A.S., permitiendo integrar teoría y práctica en un entorno real. Mediante un enfoque de investigación-acción, se desarrollaron habilidades de diagnóstico, análisis y planificación orientadas a mejorar la eficiencia y efectividad de un proceso crítico en la organización. La estructura del proyecto incluyó una revisión exhaustiva del contexto organizacional y la implementación de una solución factible que responde a las necesidades de la organización y optimiza su desempeño.

1.1. OBJETIVO GENERAL

El objetivo principal del proyecto fue desarrollar una solución operativa al problema relacionado con la falta de actualización, articulación y evaluación de los controles y procedimientos operativos del proceso de Soporte en Tecnología dentro de un Sistema de Gestión de Seguridad de la Información basado en riesgos en Skaphe Tecnología S.A.S. La intervención se orientó no solo a corregir el problema identificado, sino también a proporcionar una propuesta sostenible que pudiera integrarse a la estructura de la organización, elevando los niveles de eficiencia y alcanzando los estándares de desempeño requeridos en el proceso intervenido.

1.2. OBJETIVOS ESPECÍFICOS

Para cumplir con el objetivo general, se establecieron tres objetivos específicos:

1. Realizar una identificación detallada del problema en su contexto organizacional, determinando causas raíz y evaluando su impacto en el desempeño general del proceso.

2. Diseñar un plan de acción estructurado con objetivos claros, actividades específicas y recursos definidos para la ejecución de la solución.
3. Establecer el alcance de la intervención, definiendo responsables, cronograma y presupuesto, para asegurar que la implementación sea organizada y efectiva.

1.3. METODOLOGÍA

El proyecto se desarrolló mediante la metodología de investigación-acción, la cual facilitó la colaboración continua entre el equipo de estudiantes y docente asesor. Esta metodología permitió un enfoque sistemático para identificar problemas, formular hipótesis y aplicar soluciones en un contexto real, ajustando las estrategias conforme se avanzaba en el proyecto. La investigación-acción proporcionó un marco flexible y participativo para ejecutar el proyecto de manera estructurada, generando una intervención bien fundamentada y con alto potencial de impacto.

El diagnóstico se desarrolló mediante un análisis de brechas aplicado al proceso de Soporte en Tecnología y basado en los requisitos de la norma ISO/IEC 27001:2022. Para ello, se utilizó una lista de verificación orientada a evaluar el estado actual de la gestión de la seguridad de la información y se realizó una revisión documental de la caracterización del proceso, los procedimientos operativos, los registros, los controles técnicos y las evidencias disponibles en la organización. Esta información se complementó con la observación directa de la infraestructura tecnológica y con la consulta a los responsables de las actividades involucradas. Posteriormente, los hallazgos fueron clasificados de acuerdo con su nivel de cumplimiento, impacto y prioridad, lo que permitió identificar controles implementados, documentos desactualizados, actividades pendientes y riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información.

1.3.1. Identificación y Análisis del Problema

En la primera etapa, se realizó un análisis exhaustivo de la organización y del contexto en el cual se desarrolla el proceso afectado. Se documentó el problema identificando sus causas

raíz, efectos y puntos críticos que afectaban el desempeño del proceso. Este diagnóstico inicial fue esencial para estructurar la solución y asegurar que la intervención respondiera de manera precisa a las necesidades de la organización.

El diagnóstico se desarrolló mediante un análisis de brechas basado en los requisitos de la norma ISO/IEC 27001:2022. Para ello, se aplicó una lista de verificación orientada a evaluar el estado actual de la gestión de la seguridad de la información y se realizó una revisión documental de las políticas, procedimientos, inventarios, registros, controles técnicos y evidencias disponibles en la organización. Esta información se complementó con la observación directa de la infraestructura tecnológica y con la consulta a los responsables de los procesos involucrados. Posteriormente, los hallazgos fueron clasificados de acuerdo con su nivel de cumplimiento, impacto y prioridad, lo que permitió identificar debilidades, controles implementados, actividades pendientes y riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información.

1.3.2. Planificación de la Solución

En la segunda etapa, se desarrolló un plan de acción detallado que incluyó la definición de objetivos específicos y una secuencia de actividades que permitiría mitigar o resolver el problema identificado. Esta fase incluyó el diseño de una estrategia de ejecución organizada y estructurada que facilitara el logro de los objetivos propuestos y maximizara la eficiencia del proceso intervenido. La planificación detallada de actividades y recursos fue clave para asegurar una implementación precisa y efectiva.

1.3.2.1. Definición de Alcance y Recursos

La tercera etapa se enfocó en delimitar el alcance de la intervención y los recursos necesarios. Se establecieron responsables para cada actividad, y se elaboró un cronograma de ejecución para controlar el avance de la implementación. Asimismo, se desarrolló un presupuesto que

detalló los costos asociados a cada fase, permitiendo optimizar la asignación de recursos. Esta fase aseguró que todas las variables críticas estuvieran alineadas para una ejecución sin interrupciones.

2. IDENTIFICACIÓN Y DESCRIPCIÓN UN PROBLEMA AL INTERIOR DE LA ORGANIZACIÓN

Skaphe Tecnología S.A.S. es una organización colombiana dedicada a la prestación de servicios de gestión documental y tecnología de la información. Su modelo de negocio se orienta al desarrollo de soluciones que permiten a entidades públicas y privadas administrar, custodiar, organizar, digitalizar y recuperar información, así como implementar y mantener herramientas tecnológicas adaptadas a sus necesidades. La organización dispone de personal con experiencia en gestión documental, desarrollo de software y soporte tecnológico, áreas que requieren una adecuada coordinación para garantizar la calidad y continuidad de los servicios prestados.

Dentro de su portafolio se encuentran servicios de consultoría en gestión documental, custodia y administración de archivos, digitalización, elaboración de instrumentos archivísticos, inventarios documentales, intervención de acervos documentales, desarrollo de software, consultoría tecnológica, soporte y mantenimiento de aplicaciones. Estas actividades implican el tratamiento permanente de información física y digital perteneciente tanto a la empresa como a sus clientes.

La gestión documental constituye una de las principales líneas de operación de Skaphe Tecnología S.A.S. Los servicios relacionados con esta área comprenden la recepción, organización, clasificación, conservación, consulta, traslado, digitalización y disposición de documentos. Para desarrollar estas actividades, la empresa emplea infraestructura física, equipos de digitalización, sistemas de información, bases de datos, servidores, redes de comunicaciones y mecanismos de control que buscan preservar la integridad, disponibilidad, autenticidad y trazabilidad de la información.

El área de tecnología de la información cumple una función transversal, debido a que proporciona soporte a los sistemas, equipos, servidores, redes, aplicaciones y usuarios necesarios para la ejecución de los procesos organizacionales. Además de apoyar la operación interna, esta área participa en el diseño, desarrollo, implementación y mantenimiento de soluciones de software para los clientes. La empresa también dispone de una mesa de ayuda

para la gestión y organización de solicitudes de soporte, lo que evidencia la importancia de los servicios tecnológicos para la continuidad de sus operaciones.

Para el presente proyecto se intervendrá la gestión de la seguridad de la información asociada a los procesos de gestión documental y al soporte tecnológico que los respalda en la sede Montevideo. Esta delimitación se establece debido a que dichos procesos concentran información de clientes, documentos físicos y digitales, plataformas tecnológicas, infraestructura de almacenamiento y servicios esenciales para el cumplimiento de las obligaciones de la organización.

La información administrada por Skaphe Tecnología S.A.S. representa un activo crítico, puesto que una pérdida, alteración, divulgación no autorizada o indisponibilidad podría afectar la prestación de los servicios, el cumplimiento de los acuerdos con los clientes, la continuidad operativa y la reputación empresarial. En consecuencia, la organización requiere que sus controles técnicos, administrativos y documentales se encuentren articulados mediante un enfoque formal de gestión de riesgos.

2.1. DESCRIPCIÓN DE LA EMPRESA A INTERVENIR

2.1.1. Misión

La misión de Skaphe Tecnología S.A.S. consiste en consolidarse como un socio estratégico para sus clientes mediante la prestación de servicios de desarrollo de software y gestión documental que generen valor. Para lograrlo, la empresa promueve la innovación permanente de sus soluciones y procura que el crecimiento organizacional contribuya al bienestar y desarrollo de sus colaboradores, proveedores y comunidad.

Esta misión guarda relación directa con el proyecto propuesto, debido a que la generación de valor, la innovación y la confianza de los clientes dependen de la capacidad de la organización para proteger adecuadamente la información utilizada durante la prestación de sus servicios. La implementación inicial de un Sistema de Gestión de Seguridad de la Información permitirá

fortalecer esa relación de confianza, establecer criterios para gestionar los riesgos y asegurar que la innovación tecnológica se acompañe de medidas de seguridad apropiadas.

Asimismo, el SGSI contribuirá a que los servicios de desarrollo de software y gestión documental se ejecuten bajo lineamientos documentados, responsabilidades definidas y controles orientados a preservar la confidencialidad, integridad y disponibilidad de la información. De esta manera, la intervención propuesta se encuentra alineada con el propósito institucional y con la necesidad de mantener relaciones sostenibles con clientes, colaboradores, proveedores y demás partes interesadas.

2.1.2. Visión

La visión institucional de Skaphe Tecnología S.A.S. es: “Ser reconocidos a nivel nacional como una empresa líder en el suministro de soluciones de desarrollo de software y gestión documental”.

El cumplimiento de esta visión requiere que la organización no solamente ofrezca soluciones funcionales y de calidad, sino que también demuestre capacidad para proteger la información y administrar los riesgos asociados a sus operaciones. El liderazgo en los sectores de tecnología y gestión documental exige generar confianza, mantener la continuidad de los servicios, responder adecuadamente ante incidentes y cumplir los compromisos adquiridos con clientes y otras partes interesadas.

En este contexto, el diseño y la implementación inicial de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022 constituyen una iniciativa que apoya el crecimiento y posicionamiento de la organización. El SGSI permitirá integrar los controles existentes, fortalecer los procesos internos, establecer mecanismos de seguimiento y preparar a la empresa para una futura evaluación de conformidad o certificación.

La intervención también favorecerá la mejora continua de los servicios, al proporcionar una metodología para identificar vulnerabilidades, valorar riesgos, priorizar acciones y evaluar la eficacia de los controles. Esto permitirá que el crecimiento proyectado por Skaphe Tecnología S.A.S. se desarrolle sobre una base de seguridad, confiabilidad y sostenibilidad.

2.1.3. Mapa de procesos

El mapa de procesos de Skaphe Tecnología S.A.S., identificado con el código **MP-HSEQ-001, versión 6, de junio de 2026**, representa la interacción entre los procesos estratégicos, misionales, comerciales y de apoyo que permiten atender los requisitos de los clientes y demás partes interesadas. La estructura parte de las necesidades y expectativas recibidas por la organización y orienta sus actividades hacia la prestación de servicios que contribuyan a alcanzar la satisfacción del cliente.

En el nivel estratégico se encuentran los procesos de **Dirección Estratégica y Gestión Integral de Procesos**. Estos procesos establecen los lineamientos organizacionales, orientan la toma de decisiones y promueven la planificación, evaluación y mejora continua de las actividades desarrolladas por la empresa. Desde la perspectiva del presente proyecto, este nivel resulta fundamental, debido a que la implementación de un Sistema de Gestión de Seguridad de la Información requiere liderazgo, asignación de responsabilidades, aprobación de políticas, provisión de recursos y seguimiento por parte de la alta dirección.

El mapa identifica como procesos misionales principales la **Gestión de Proyectos de Gestión Documental** y la **Gestión de Proyectos de Tecnología de la Información**. La primera incluye los servicios de intervención de acervos documentales; traslado, custodia y administración de archivos; elaboración de instrumentos archivísticos; interventoría a proyectos de gestión documental; digitalización, y *outsourcing* de gestión documental. La segunda comprende el diseño y desarrollo de software, el soporte y mantenimiento de software, y la consultoría de software. Estos procesos constituyen el núcleo de la prestación de servicios de Skaphe Tecnología S.A.S. y dependen del tratamiento permanente de información física y digital perteneciente a la organización y a sus clientes.

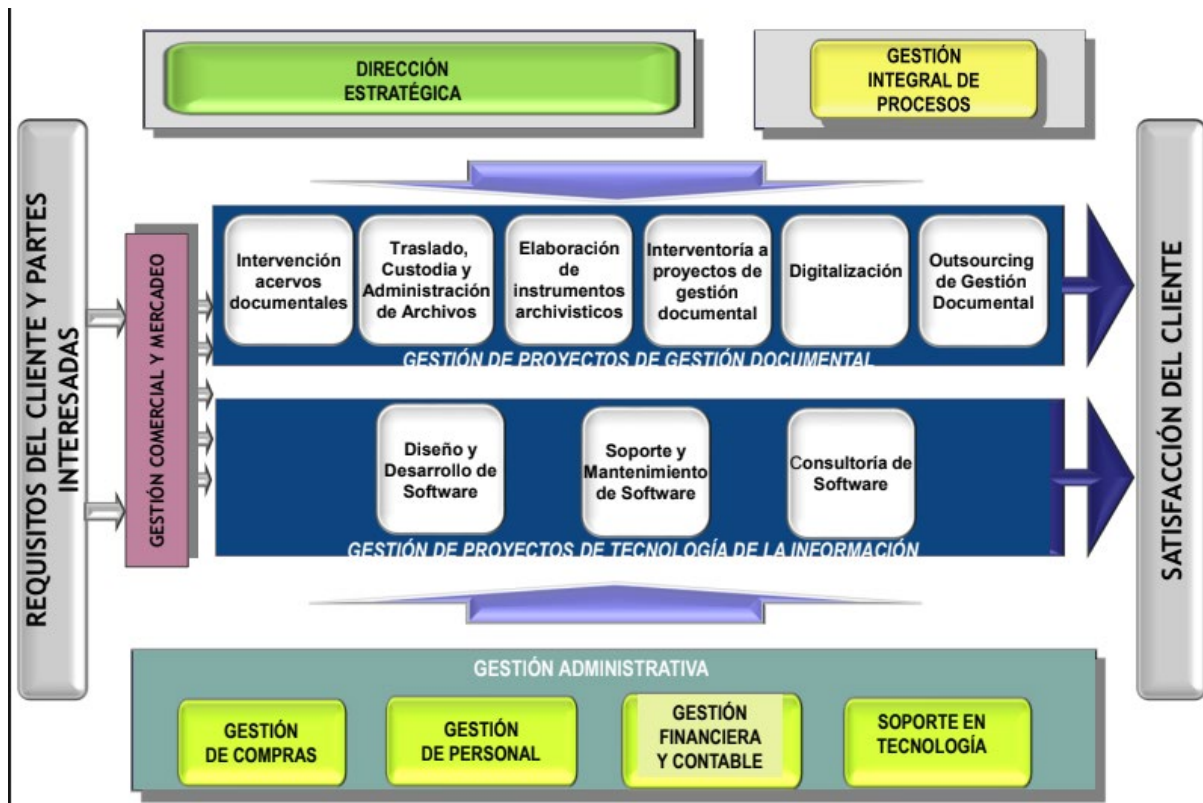
La **Gestión Comercial y Mercadeo** actúa como vínculo entre los requisitos de los clientes y la ejecución de los servicios. Este proceso recopila las necesidades comerciales, participa en la definición de las condiciones del servicio y facilita la comunicación con los procesos encargados de ejecutar los proyectos. Por esta razón, también interviene en el tratamiento de información comercial, contractual y de clientes que debe ser protegida frente a accesos no autorizados, pérdida, alteración o divulgación indebida.

Como procesos de apoyo, el mapa agrupa dentro de la **Gestión Administrativa** a la Gestión de Compras, Gestión de Personal, Gestión Financiera y Contable, y Soporte en Tecnología. Estos procesos proporcionan los recursos humanos, financieros, tecnológicos y contractuales necesarios para el funcionamiento de las actividades misionales. En particular, **Soporte en Tecnología** cumple una función transversal, debido a que administra y mantiene equipos, redes, servidores, sistemas de información, cuentas de usuario, plataformas, comunicaciones y servicios tecnológicos utilizados por las diferentes áreas.

El problema objeto de intervención se relaciona directamente con esta estructura, debido a que la seguridad de la información no corresponde exclusivamente al área de tecnología, sino que afecta a todos los procesos representados en el mapa. La ausencia de una integración formal de los controles, responsabilidades, procedimientos, riesgos y evidencias de seguridad puede generar impactos sobre la gestión documental, los proyectos de tecnología, los procesos administrativos y la relación con los clientes.

En consecuencia, el Sistema de Gestión de Seguridad de la Información propuesto deberá articularse principalmente desde **Dirección Estratégica y Gestión Integral de Procesos**, con el acompañamiento técnico de **Soporte en Tecnología** y la participación de los procesos misionales y administrativos. Esta integración permitirá establecer lineamientos comunes para proteger la confidencialidad, integridad y disponibilidad de la información, gestionar los riesgos y fortalecer la continuidad de los servicios prestados por la organización.

Figura 1. Mapa de procesos de Skaphe Tecnología S.A.S.



Fuente: Skaphe Tecnología S.A.S. (2026). *Estructura de procesos, MP-HSEQ-001, versión 6.*

2.1.4. Descripción del proceso a intervenir

El proceso seleccionado para la intervención es **Soporte en Tecnología**, ubicado dentro de los procesos de apoyo de Skaphe Tecnología S.A.S. Su objetivo consiste en gestionar y solucionar las necesidades relacionadas con los servicios tecnológicos de la organización. Debido a su naturaleza transversal, este proceso presta apoyo a las áreas administrativas, a los proyectos de gestión documental y a los proyectos de tecnología de la información, por lo que su funcionamiento influye directamente en la continuidad de las operaciones y en la prestación de los servicios a los clientes.

La caracterización del proceso establece como principales actividades el soporte de conectividad de la red de datos, el diagnóstico y mantenimiento de equipos de cómputo y servidores, la instalación y puesta en funcionamiento de software y aplicaciones, el traslado e instalación de equipos y periféricos, la ejecución de copias de seguridad en servidores y la

recepción o transferencia de información contenida en discos duros. Estas actividades tienen como resultados esperados la disponibilidad de los equipos, el funcionamiento adecuado del software, la conectividad de los usuarios y la protección de la información administrada por la organización.

La atención de los servicios tecnológicos se desarrolla principalmente mediante la Mesa de Ayuda, establecida como punto único para recibir, registrar y hacer seguimiento a los incidentes y requerimientos reportados por los usuarios. El procedimiento comprende desde el registro de la solicitud en la herramienta HelpDesk hasta la documentación de la solución, su validación con el usuario y el cierre del caso. Su alcance incluye equipos de cómputo, periféricos, redes de datos, acceso a internet, software, correo electrónico, aplicaciones, servicios compartidos, cuentas de usuario, inventario tecnológico y demás servicios administrados por el área.

El ciclo de atención inicia con el registro del ticket y continúa con la validación de la información, la clasificación del caso, la asignación de prioridad, el diagnóstico técnico, la ejecución de la solución o el escalamiento, la documentación de las actividades y la validación final con el usuario. Los casos son clasificados como incidentes o requerimientos y se priorizan de acuerdo con su impacto, urgencia y afectación operativa. Los eventos relacionados con la caída de la red, internet, servidores, energía o aplicaciones críticas pueden ser clasificados como prioridad crítica, debido a su capacidad para interrumpir servicios esenciales de la empresa.

Dentro del proceso también se ejecutan actividades preventivas dirigidas a preservar la disponibilidad, el desempeño, la seguridad y la vida útil de los activos tecnológicos. El mantenimiento preventivo comprende la programación periódica de los equipos, la revisión física del hardware, la actualización de sistemas y aplicaciones, la verificación del software autorizado, la revisión de soluciones antivirus, la identificación de privilegios administrativos injustificados y el registro de hallazgos que puedan requerir acciones correctivas. El procedimiento establece como referencia una frecuencia semestral para los equipos de cómputo, ajustable según su criticidad, condiciones de uso e historial de fallas.

Otra actividad relevante es el borrado seguro de información almacenada en computadores, servidores, discos, unidades de estado sólido, memorias extraíbles, dispositivos móviles, carpetas compartidas y repositorios. Este procedimiento contempla la autorización del

borrado, la clasificación previa de la información, la selección del método de eliminación, la verificación del resultado y la conservación de evidencias. También define responsabilidades para Soporte en Tecnología, los responsables de los procesos, los usuarios, Gestión Documental y las áreas encargadas de validar restricciones legales o contractuales de conservación.

Por lo anterior, Soporte en Tecnología no se limita a resolver fallas operativas. El proceso administra activos, accesos, redes, aplicaciones, respaldos, medios de almacenamiento y evidencias técnicas que contienen o permiten acceder a información de la organización y de sus clientes. En consecuencia, constituye un proceso crítico para proteger la confidencialidad, integridad y disponibilidad de la información, así como para mantener la continuidad de los procesos misionales de Skaphe Tecnología S.A.S.

La intervención propuesta se concentrará en fortalecer la gestión de la seguridad de la información dentro de este proceso, mediante la integración de las actividades existentes con un enfoque formal basado en riesgos y alineado con ISO/IEC 27001:2022. El proceso de Soporte en Tecnología funcionará como eje técnico y transversal de la implementación inicial del SGSI, con participación de la Dirección Estratégica, Gestión Integral de Procesos, Gestión Documental y demás áreas que administren o utilicen activos de información.

2.1.5. Descripción del problema que presenta el proceso

El problema es que el proceso de Soporte en Tecnología de Skaphe Tecnología S.A.S. tiene varios controles y procedimientos funcionando, pero todavía no están integrados dentro de un Sistema de Gestión de Seguridad de la Información basado en riesgos. Es decir, no se parte de una ausencia total de controles. El área ya atiende incidentes, realiza mantenimientos, administra equipos, genera respaldos y cuenta con un procedimiento para el borrado de información. Lo que hace falta es organizar estas actividades bajo una misma estructura y poder relacionarlas con los riesgos que realmente enfrenta la empresa.

Durante la revisión de los documentos del proceso se encontró que buena parte de ellos fueron creados para atender las necesidades del día a día. Esto es normal porque Soporte en Tecnología debe resolver fallas, atender usuarios y mantener disponibles los servicios. Sin

embargo, al revisar estos documentos desde el punto de vista de seguridad de la información, todavía quedan aspectos por integrar.

Un caso concreto es la caracterización del proceso C-ST-001. Este documento es de junio de 2023, mientras que otros procedimientos que hoy utiliza el área fueron actualizados en 2025 y 2026. Por esta razón, algunas actividades que actualmente se realizan pueden no estar reflejadas con el mismo nivel de detalle en la caracterización. También han cambiado herramientas, responsabilidades y formas de trabajo desde que se elaboró esa versión.

Algo similar ocurre con los riesgos. La caracterización menciona matrices de riesgos y oportunidades, planes de acción e indicadores, pero estos elementos pertenecen principalmente al sistema de gestión que ya tenía la empresa. Para el SGSI se necesita revisar los riesgos desde una perspectiva más específica: qué información se está protegiendo, qué activo la soporta, qué puede afectarlo y qué control existe actualmente para reducir ese riesgo.

Además, varios documentos del SGSI todavía se encuentran en elaboración. Entre ellos están el inventario integral de activos, la matriz de riesgos de seguridad de la información, el plan de tratamiento, la Declaración de Aplicabilidad y algunos indicadores. Esto hace parte del problema actual, pero también representa una oportunidad para organizar la información que la empresa ya tiene y evitar empezar nuevamente desde cero.

Por ejemplo, durante un mantenimiento preventivo ya se revisan actualizaciones, antivirus, programas instalados y privilegios de administrador. En la Mesa de Ayuda quedan registrados incidentes, fallas de acceso, problemas de conectividad y solicitudes relacionadas con aplicaciones. También existe un procedimiento para controlar el borrado de información cuando un equipo o medio deja de utilizarse. Por separado, cada una de estas actividades aporta a la seguridad.

La dificultad aparece cuando se intenta responder preguntas más generales. Por ejemplo: ¿qué riesgo está reduciendo cada control?, ¿qué equipos son realmente críticos?, ¿qué problemas se presentan con mayor frecuencia?, ¿quién debe hacer seguimiento a cada riesgo? o ¿cómo se puede demostrar que un control está funcionando? Hoy existe información para responder parte de estas preguntas, pero se encuentra distribuida entre diferentes documentos, herramientas y registros.

También ocurre con las evidencias. El área genera tickets, informes, formatos de mantenimiento, hojas de vida de equipos, fotografías y otros soportes técnicos. El reto consiste en aprovechar esa información y no dejarla solamente como evidencia de una actividad realizada. Si se organiza adecuadamente, puede servir para identificar fallas repetitivas, equipos con mayor número de incidentes o controles que necesitan ser reforzados.

Esta falta de integración puede hacer que algunos problemas se atiendan únicamente cuando ya se presentaron. Una falla en un servidor, un respaldo que no pudo recuperarse, un acceso incorrecto o una vulnerabilidad recurrente pueden convertirse en situaciones repetitivas si no se analizan como parte de un mismo esquema de riesgos.

Por lo tanto, la necesidad de Skaphe no es crear desde cero todos los controles de seguridad, porque muchos ya existen. El trabajo consiste principalmente en revisar lo que se tiene, actualizarlo cuando sea necesario y conectarlo dentro de un SGSI. De esta manera será más fácil conocer cuáles son los activos importantes, qué riesgos los afectan, qué controles ya están funcionando y qué acciones todavía deben realizarse.

3. ESTABLECIMIENTO DE PLANES DE ACCIÓN PARA LA SOLUCIÓN DEL PROBLEMA

En respuesta al problema identificado en el proceso de Soporte en Tecnología de Skaphe Tecnología S.A.S., se estableció un plan de acción orientado a actualizar, articular y evaluar los controles y procedimientos operativos existentes dentro de una estructura inicial de Sistema de Gestión de Seguridad de la Información basado en riesgos. La intervención parte del reconocimiento de que la organización ya dispone de mecanismos para atender incidentes y requerimientos, realizar mantenimientos preventivos, administrar activos tecnológicos y ejecutar el borrado controlado de información; sin embargo, estos elementos requieren relacionarse de manera sistemática con los activos, amenazas, vulnerabilidades, riesgos, responsables, evidencias e indicadores del proceso.

El procedimiento de servicios de soporte establece actividades para la recepción, registro, clasificación, atención, seguimiento y cierre de solicitudes tecnológicas mediante la Mesa de Ayuda, con el propósito de mantener trazabilidad, control operativo y oportunidad en la atención. Su alcance comprende equipos, periféricos, redes, internet, software, correo, aplicaciones, cuentas de usuario e inventario tecnológico, por lo que constituye una base relevante para integrar la gestión de incidentes y requerimientos con los objetivos de seguridad de la información.

De manera complementaria, el procedimiento de mantenimiento preventivo busca preservar la disponibilidad, el desempeño, la seguridad y la vida útil de los equipos, así como anticipar fallas, actualizar el inventario y conservar evidencias verificables de las intervenciones realizadas. El procedimiento de borrado de información, por su parte, define controles para la autorización, clasificación, eliminación, verificación y documentación del tratamiento realizado sobre equipos, dispositivos, servidores, repositorios y medios de almacenamiento. Estos procedimientos evidencian la existencia de controles operativos que pueden ser aprovechados y fortalecidos dentro del SGSI.

A partir de esta base, el plan de acción se estructuró en actividades progresivas que comprenden la validación del diagnóstico, la actualización de la caracterización del proceso,

la identificación y clasificación de activos, la definición de una metodología de riesgos, la elaboración de la matriz de riesgos, la evaluación de controles existentes, la construcción del plan de tratamiento y la preparación de una Declaración de Aplicabilidad preliminar. Posteriormente, se contempla la actualización de documentos, la implementación de controles prioritarios y el establecimiento de indicadores que permitan evaluar los resultados alcanzados.

Como parte del fortalecimiento de la postura de ciberseguridad, el plan de acción también contempla la implementación de controles técnicos alineados con los objetivos de seguridad del SGSI. Entre estos se incluyen la gestión de vulnerabilidades sobre los activos tecnológicos, el fortalecimiento de configuraciones seguras (hardening) de servidores y estaciones de trabajo, la revisión de la gestión de identidades y accesos bajo principios de mínimo privilegio y Zero Trust, el establecimiento de mecanismos de monitoreo continuo y gestión centralizada de registros (logs), así como la incorporación de buenas prácticas recomendadas por marcos de referencia como el **NIST Cybersecurity Framework (CSF 2.0)** y la matriz **MITRE ATT&CK** para fortalecer la identificación, protección, detección, respuesta y recuperación frente a incidentes de seguridad.

Cada actividad fue planteada para generar un producto verificable, como inventarios, matrices, procedimientos, informes, tickets, actas, registros técnicos, indicadores o evidencias de implementación. Este enfoque permitirá medir el avance mediante criterios como el porcentaje de activos identificados, riesgos evaluados, controles documentados, procedimientos actualizados y acciones de tratamiento ejecutadas. La utilización de resultados verificables contribuirá a que la evaluación del proceso no dependa únicamente de apreciaciones cualitativas, sino de información documentada y susceptible de seguimiento.

La ejecución de la solución requerirá la participación de la Dirección Estratégica, Gestión Integral de Procesos, Soporte en Tecnología, líderes de los procesos misionales, usuarios y proveedores, según la naturaleza de cada actividad. También será necesario utilizar recursos documentales, tecnológicos, físicos y financieros disponibles en la organización, procurando aprovechar la infraestructura, herramientas y procedimientos existentes antes de considerar nuevas adquisiciones.

Con este plan se busca abordar las causas raíz del problema, especialmente la desactualización documental, la administración separada de los controles, la ausencia de una metodología

consolidada de riesgos y la falta de indicadores integrados de seguridad. De esta manera, la intervención permitirá establecer una base sostenible para fortalecer la confidencialidad, integridad y disponibilidad de la información, mejorar la continuidad de las operaciones y facilitar que Skaphe Tecnología S.A.S. continúe posteriormente con la implementación progresiva de su Sistema de Gestión de Seguridad de la Información.

3.1. ESTABLECIMIENTO DE OBJETIVOS

En respuesta al problema identificado en el proceso de Soporte en Tecnología de Skaphe Tecnología S.A.S., el plan de acción se orienta a actualizar, articular y evaluar los controles y procedimientos existentes dentro de una estructura inicial de Sistema de Gestión de Seguridad de la Información basado en riesgos. Para facilitar su seguimiento, los objetivos fueron formulados mediante la metodología SMART, de manera que cada uno tenga un resultado concreto, una forma de verificación y un plazo de cumplimiento dentro del periodo del proyecto.

Objetivo 1. Actualizar la caracterización del proceso de Soporte en Tecnología, revisando las actividades, entradas, salidas, responsables, herramientas, documentos, riesgos y controles que actualmente forman parte de su operación, de forma que el documento refleje las condiciones reales del proceso.

Objetivo 2. Identificar y clasificar los activos de información y tecnológicos incluidos en el alcance de la sede Montevideo, registrando como mínimo su tipo, ubicación, responsable, propietario, servicio relacionado y nivel de criticidad, con el fin de disponer de una base confiable para la posterior valoración de riesgos.

Objetivo 3. Diseñar y aplicar una metodología de gestión de riesgos de seguridad de la información, estableciendo criterios de probabilidad, impacto, nivel de riesgo y aceptación, y utilizándola para valorar los riesgos asociados a los activos identificados dentro del alcance.

Objetivo 4. Elaborar un plan de tratamiento para el 100 % de los riesgos clasificados como altos o no aceptables, asignando para cada uno una acción de tratamiento, responsable, prioridad, recurso requerido, evidencia esperada y estado de ejecución.

Objetivo 5. Elaborar una Declaración de Aplicabilidad preliminar relacionando los controles considerados para el alcance del proyecto, su justificación, estado de implementación y las evidencias o documentos que los respaldan.

Objetivo 6. Implementar o fortalecer al menos cinco controles prioritarios de seguridad de la información, seleccionados de acuerdo con los riesgos identificados y la viabilidad del proyecto, generando evidencias verificables de su aplicación.

Objetivo 7. Definir un conjunto mínimo de cinco indicadores de seguimiento, relacionados con activos, riesgos, incidentes, controles, vulnerabilidades, respaldos o cumplimiento documental, especificando para cada uno su fórmula, fuente de información, responsable y frecuencia de medición.

Objetivo 8. Evaluar el avance de la intervención comparando los resultados obtenidos con el diagnóstico inicial y documentando los controles implementados, las actividades pendientes, las limitaciones encontradas y las recomendaciones para continuar con la implementación progresiva del SGSI.

Estos objetivos permiten que el plan de acción pueda ser evaluado mediante entregables y evidencias concretas. Su cumplimiento no implica finalizar la implementación completa del SGSI ni alcanzar una certificación ISO/IEC 27001:2022 a corto plazo, sino establecer una primera base funcional, documentada y medible que pueda continuar desarrollándose.

3.2. DESCRIPCIÓN DE LA SOLUCIÓN

La solución parte de los procedimientos, herramientas y prácticas que actualmente utiliza el proceso de Soporte en Tecnología de Skaphe Tecnología S.A.S. para atender solicitudes, realizar mantenimientos, administrar equipos y ejecutar actividades relacionadas con la protección de la información. El diagnóstico evidenció que estos elementos fueron desarrollados en momentos diferentes y aún requieren una integración metodológica dentro del SGSI.

Por esta razón, la solución planteada consiste en iniciar la implementación de un Sistema de Gestión de Seguridad de la Información tomando como referencia la norma ISO/IEC

27001:2022. El trabajo se concentrará en el proceso de Soporte en Tecnología de la sede Montevideo, ya que desde allí se administran buena parte de los equipos, usuarios, redes, servidores, aplicaciones, respaldos y servicios que utilizan los demás procesos de la empresa.

El objetivo es conservar los elementos que resulten vigentes, actualizar aquellos que no reflejen la operación actual y relacionar las actividades existentes con los riesgos identificados en la organización. De esta manera, los procedimientos podrán integrarse como controles documentados dentro del SGSI, evitando duplicidades y aprovechando la gestión ya desarrollada por el proceso.

Uno de los primeros documentos que debe revisarse es la caracterización del proceso de Soporte en Tecnología. En ella aparecen actividades como el soporte de conectividad, el mantenimiento de equipos y servidores, la instalación de programas, el traslado de periféricos, la realización de copias de seguridad y la recepción de discos duros. Sin embargo, su versión es anterior a varios de los procedimientos que hoy utiliza el área. Esto hace necesario compararla con la operación actual y agregar las actividades, herramientas y responsabilidades que se han incorporado con el tiempo.

La Mesa de Ayuda también tendrá un papel importante en la solución. Actualmente, el HelpDesk permite registrar los incidentes y requerimientos reportados por los usuarios. Cada caso puede ser clasificado, asignado, atendido y cerrado, dejando evidencia de las acciones realizadas. La información almacenada en los tickets será útil para conocer cuáles son las fallas más frecuentes, qué equipos o servicios presentan mayores inconvenientes y cuánto tiempo toma atender cada solicitud.

Estos datos no deberían utilizarse únicamente para demostrar que un ticket fue cerrado. Al analizarlos en conjunto, pueden ayudar a detectar problemas repetitivos y a tomar decisiones preventivas. Por ejemplo, si varios usuarios reportan fallas sobre un mismo servicio, equipo o aplicación, el caso puede dejar de tratarse como una novedad aislada y convertirse en un riesgo que requiere una acción de mejora.

El mantenimiento preventivo será otro de los elementos que se incorporará al SGSI. Esta actividad permite revisar el estado físico y lógico de los equipos, verificar actualizaciones, comprobar el funcionamiento del antivirus, detectar programas no autorizados y revisar si

existen usuarios con privilegios que no necesitan. También ayuda a identificar equipos deteriorados u obsoletos antes de que una falla afecte el trabajo de un área.

Actualmente existe un procedimiento para realizar estas tareas, pero será necesario relacionar sus resultados con el inventario de activos y con la matriz de riesgos. Así, un hallazgo encontrado durante un mantenimiento no quedará únicamente registrado en un formato, sino que podrá dar origen a una acción correctiva o a un tratamiento específico.

También se revisará el procedimiento de borrado de información. Este documento define cómo eliminar datos almacenados en computadores, servidores, discos, memorias, dispositivos móviles y carpetas compartidas. Su aplicación es importante porque los equipos pueden ser reasignados, retirados del servicio, enviados a mantenimiento o entregados a terceros.

Antes de borrar información se debe confirmar quién autoriza la actividad, qué tipo de datos contiene el medio y si existe alguna obligación de conservación. Después del borrado debe verificarse que la información no pueda recuperarse fácilmente y conservarse una evidencia de lo realizado. Estas actividades se relacionarán con la protección de la confidencialidad y con el manejo de los activos durante todo su ciclo de vida.

Para organizar el trabajo, la solución se estructurará en siete componentes claramente relacionados con las actividades descritas en la sección 3.3.

Componente 1. Revisión y actualización del proceso

En esta etapa se comparará la caracterización de Soporte en Tecnología con las actividades que actualmente realiza el área. Se revisarán sus entradas, salidas, responsables, herramientas, registros y relación con los demás procesos.

También se identificarán los documentos vigentes y aquellos que todavía se encuentran en construcción. El resultado será una propuesta de caracterización actualizada que represente mejor el funcionamiento actual de Soporte en Tecnología.

Componente 2. Identificación de activos y riesgos

Se realizará el inventario de los activos que hacen parte del alcance. Allí se incluirán, entre otros, servidores, computadores, equipos de red, aplicaciones, bases de datos, cuentas de usuario, respaldos, documentos y servicios contratados.

Para cada activo se registrará quién es su responsable, dónde se encuentra, qué servicio soporta y qué tan importante es para la operación. Después se analizarán las amenazas y debilidades que podrían afectarlo.

La valoración tendrá en cuenta tanto la posibilidad de ocurrencia como las consecuencias para la empresa. No tendrá la misma prioridad una falla en un equipo de uso ocasional que la caída de un servidor, la pérdida de un respaldo o el acceso no autorizado a información de clientes.

Componente 3. Revisión y tratamiento de controles

Una vez identificados los riesgos, se revisará qué controles ya existen y cuáles necesitan ajustes. Algunos estarán contenidos en los procedimientos actuales; otros dependerán de configuraciones técnicas, herramientas de monitoreo, prácticas de los usuarios o decisiones de la dirección.

Con esta información se elaborará un plan de tratamiento. Allí se indicará qué debe hacerse, quién será responsable, qué recursos se necesitan, qué evidencia debe quedar y cuál es la prioridad de la actividad.

También se preparará una Declaración de Aplicabilidad preliminar. Este documento permitirá identificar los controles tomados como referencia, justificar su aplicación y señalar si están implementados, en proceso o pendientes.

Componente 4. Aplicación de controles prioritarios

Debido al tiempo disponible para el proyecto, no será posible implementar todos los controles de un SGSI. Por ello, se seleccionarán aquellos que puedan generar un avance comprobable y que respondan a los riesgos más relevantes.

Entre las acciones previstas se encuentran la actualización del inventario de activos, la mejora del registro de incidentes, la verificación de respaldos, el seguimiento a equipos críticos y la aplicación de controles documentales u operativos priorizados. Las actividades técnicas de vulnerabilidades, Hardening, gestión de identidades y accesos, y monitoreo de logs se desarrollarán específicamente en el Componente 5.

También se revisarán las evidencias de mantenimiento, el borrado seguro de medios y los documentos que requieran actualización. Cada actividad deberá dejar un soporte, por ejemplo, un ticket, un informe, una captura, una matriz, un acta o un formato diligenciado.

Componente 5. Fortalecimiento de la postura de ciberseguridad

Este componente busca reforzar algunos controles técnicos que ya existen en Skaphe Tecnología S.A.S. y que son importantes para reducir riesgos sobre los activos tecnológicos. El trabajo se concentrará en tres frentes: revisar las configuraciones de seguridad de los equipos y servidores, controlar mejor los accesos de los usuarios y aprovechar los registros generados por los sistemas para detectar situaciones que requieran atención.

La gestión de vulnerabilidades se aborda previamente en el Componente 2. Identificación de activos y riesgos, mediante la Actividad 8. Evaluación técnica de vulnerabilidades. Los resultados obtenidos en esa revisión servirán para definir qué equipos, servicios o configuraciones necesitan mayor atención dentro de este componente.

Para organizar mejor el trabajo, el Componente 5 se divide en tres subcomponentes.

Subcomponente 5.1. Fortalecimiento de configuraciones seguras

En esta parte se revisarán servidores, estaciones de trabajo y dispositivos de red que hayan sido considerados importantes dentro del alcance. La revisión permitirá detectar configuraciones que puedan representar un riesgo, como servicios que no se utilizan, parámetros que conservan valores por defecto, permisos innecesarios o ajustes de seguridad que todavía no hayan sido aplicados.

Subcomponente 5.2. Gestión de identidades y accesos

Se revisarán las cuentas, grupos y permisos utilizados dentro del proceso, prestando especial atención a los usuarios con privilegios administrativos. La finalidad es comprobar que cada persona conserve únicamente los accesos que necesita para realizar sus funciones y que puedan retirarse aquellos que hayan dejado de ser necesarios.

Subcomponente 5.3. Monitoreo y gestión de registros

También se revisará la manera en que se generan y almacenan los registros de servidores, aplicaciones, estaciones de trabajo, dispositivos de red y herramientas de seguridad. Estos registros pueden ser útiles para conocer qué ocurrió antes, durante o después de una falla o incidente, por lo que se establecerán criterios básicos para definir cuáles deben revisarse, dónde se conservarán y quién estará a cargo de su seguimiento.

Estas actividades tomarán como referencia los controles aplicables de ISO/IEC 27001:2022 y podrán complementarse con buenas prácticas del NIST Cybersecurity Framework y MITRE ATT&CK, especialmente en los temas relacionados con protección, detección y respuesta frente a eventos de seguridad.

Componente 6. Integración de Inteligencia Artificial

Durante la revisión del proceso se evidenció que Soporte en Tecnología genera información en varios espacios: tickets de la Mesa de Ayuda, reportes técnicos, registros de eventos y evidencias de mantenimiento. Todos estos datos pueden ser útiles, pero al estar separados no siempre resulta sencillo analizarlos en conjunto o detectar situaciones que se repiten.

Por esta razón, se plantea realizar una prueba piloto con una herramienta de Inteligencia Artificial. La intención es comprobar si puede ayudar a organizar parte de esa información y facilitar algunas tareas que actualmente requieren revisión manual.

La prueba se enfocará en actividades puntuales, como clasificar tickets, agrupar casos parecidos, revisar registros de eventos o apoyar la organización de información para los reportes. No se pretende reemplazar el trabajo del personal de Soporte en Tecnología ni dejar decisiones importantes en manos de una herramienta.

Los resultados siempre deberán ser revisados por una persona antes de ser utilizados. Al finalizar la prueba se documentará qué funcionó, qué dificultades se encontraron y si realmente se obtuvo algún beneficio para el proceso.

Con esto se busca determinar, de una manera controlada, si la Inteligencia Artificial puede servir como apoyo para aprovechar mejor la información que ya genera el área. Si los resultados no muestran una mejora clara, su uso no se considerará necesario para las siguientes etapas del SGSI.

Componente 7. Seguimiento de los resultados

La última parte consistirá en revisar qué tanto se avanzó frente al diagnóstico inicial. Para ello se definirán indicadores sencillos, como el porcentaje de activos inventariados, los riesgos evaluados, los controles documentados y las acciones ejecutadas.

Esta comparación permitirá mostrar los avances alcanzados, pero también las actividades que deberán continuar después de terminar el trabajo académico. La implementación de un SGSI requiere seguimiento permanente, por lo que el proyecto dejará una base inicial y una ruta para las siguientes etapas.

Con esta propuesta, el proceso de Soporte en Tecnología podrá organizar mejor la información que ya genera, relacionar sus procedimientos con los riesgos de la empresa y conservar evidencias más claras de los controles aplicados. Esto facilitará la priorización de recursos, la toma de decisiones y el fortalecimiento gradual de la continuidad de las operaciones.

3.3. SECUENCIA DE ACTIVIDADES PARA EJECUCIÓN DE LA SOLUCIÓN

La ejecución de la solución se organizó de manera progresiva, procurando que cada actividad entregue un resultado que sirva de base para la siguiente. Para mantener la relación con la solución planteada en el apartado 3.2, cada actividad se asocia con uno de los cinco

componentes definidos: actualización del proceso, gestión de activos y riesgos, tratamiento y selección de controles, implementación inicial, y seguimiento y mejora.

De esta forma, es posible identificar con claridad qué parte de la solución se está desarrollando en cada momento y cómo las actividades contribuyen a resolver el problema identificado en el proceso de Soporte en Tecnología.

Actividad 1. Validación del diagnóstico inicial

Componente que cubre: Componente 1. Actualización del proceso.

Se revisarán los resultados obtenidos durante la identificación del problema para confirmar las condiciones actuales del proceso, los documentos existentes, las actividades realizadas y las principales brechas relacionadas con la seguridad de la información.

Resultado esperado: diagnóstico validado y listado de brechas priorizadas.

Indicador: porcentaje de documentos y actividades del proceso revisados.

Actividad 2. Revisión y actualización de la caracterización del proceso

Componente que cubre: Componente 1. Actualización del proceso.

Se comparará la caracterización C-ST-001 con los procedimientos, herramientas y responsabilidades actualmente utilizadas. A partir de esta revisión se actualizarán las entradas, actividades, salidas, responsables, recursos, riesgos, documentos e indicadores que correspondan.

Resultado esperado: propuesta de caracterización actualizada de Soporte en Tecnología.

Indicador: caracterización revisada y presentada para validación.

Actividad 3. Identificación de partes interesadas y requisitos

Componente que cubre: Componente 1. Actualización del proceso.

Se identificarán las áreas, responsables, usuarios, clientes internos, proveedores y demás partes que intervienen o dependen del proceso. También se revisarán requisitos

organizacionales, contractuales, legales y normativos relacionados con la protección de la información.

Resultado esperado: matriz preliminar de partes interesadas y requisitos.

Indicador: número de partes interesadas y requisitos identificados.

Actividad 4. Levantamiento del inventario de activos

Componente que cubre: Componente 2. Gestión de activos y riesgos.

Se identificarán los activos de información y tecnológicos incluidos dentro del alcance, entre ellos servidores, computadores, equipos de red, sistemas, aplicaciones, bases de datos, cuentas, repositorios, respaldos, documentos y servicios externos.

Resultado esperado: inventario de activos actualizado.

Indicador: porcentaje de activos identificados frente al universo definido para el alcance.

Actividad 5. Clasificación y valoración de activos

Componente que cubre: Componente 2. Gestión de activos y riesgos.

Los activos se clasificarán teniendo en cuenta su tipo, propietario, custodio, ubicación, criticidad y necesidad de confidencialidad, integridad y disponibilidad.

Resultado esperado: inventario clasificado y activos críticos identificados.

Indicador: porcentaje de activos clasificados y con responsable asignado.

Actividad 6. Definición de la metodología de riesgos

Componente que cubre: Componente 2. Gestión de activos y riesgos.

Se definirán las escalas de probabilidad e impacto, la forma de calcular el nivel de riesgo y los criterios que permitan determinar cuándo un riesgo puede ser aceptado, mitigado, evitado o transferido.

Resultado esperado: metodología documentada para gestionar riesgos de seguridad de la información.

Indicador: metodología elaborada y validada.

Actividad 7. Identificación de amenazas y vulnerabilidades

Componente que cubre: Componente 2. Gestión de activos y riesgos.

Para los activos identificados se analizarán situaciones que puedan afectar su funcionamiento o la información que contienen, como fallas de hardware, errores humanos, accesos no autorizados, malware, pérdida de información, problemas de conectividad o configuraciones inadecuadas.

Resultado esperado: escenarios de riesgo asociados a los activos.

Indicador: número de activos críticos con amenazas y vulnerabilidades identificadas.

Actividad 8. Evaluación técnica de vulnerabilidades

Componente que cubre: Componente 2. Gestión de activos y riesgos.

Se realizará una evaluación de vulnerabilidades sobre los activos tecnológicos incluidos en el alcance, con el propósito de complementar el análisis documental con información técnica sobre las debilidades presentes en servidores, estaciones de trabajo y otros sistemas.

Resultado esperado: inventario de vulnerabilidades clasificadas según su criticidad.

Indicador: porcentaje de activos evaluados y número de vulnerabilidades críticas identificadas.

Actividad 9. Análisis y evaluación de riesgos

Componente que cubre: Componente 2. Gestión de activos y riesgos.

Los escenarios identificados serán valorados mediante la metodología definida. Esto permitirá establecer qué riesgos pueden aceptarse y cuáles requieren intervención prioritaria.

Resultado esperado: matriz de riesgos de seguridad de la información.

Indicador: porcentaje de riesgos evaluados y priorizados.

Actividad 10. Identificación y evaluación de controles existentes

Componente que cubre: Componente 3. Tratamiento y selección de controles.

Se revisarán los controles que actualmente se aplican mediante los procedimientos de soporte, mantenimiento, respaldos, administración de cuentas, monitoreo, borrado de información y demás actividades del proceso. Cada control será relacionado con los riesgos que ayuda a reducir.

Resultado esperado: matriz de controles existentes y análisis de su suficiencia.

Indicador: porcentaje de riesgos con controles existentes identificados.

Actividad 11. Elaboración del plan de tratamiento

Componente que cubre: Componente 3. Tratamiento y selección de controles.

Una vez identificados los riesgos más importantes, se definirá qué se debe hacer con cada uno. No todos los riesgos necesitarán la misma respuesta; algunos podrán aceptarse, mientras que otros requerirán acciones para reducirlos.

Para los riesgos que requieran tratamiento se documentará la acción propuesta, el responsable de ejecutarla, los recursos necesarios y la evidencia requerida para verificar su cumplimiento. El plan funcionará como un instrumento de seguimiento para controlar el avance de las acciones definidas y el estado de cada riesgo.

Resultado esperado: plan de tratamiento de riesgos con acciones, responsables y prioridades definidas.

Indicador: porcentaje de riesgos no aceptables que cuentan con una acción de tratamiento asignada.

Actividad 12. Elaboración de la Declaración de Aplicabilidad preliminar

Componente que cubre: Componente 3. Tratamiento y selección de controles.

Después de revisar los riesgos y los controles que ya existen en la empresa, se preparará una primera versión de la Declaración de Aplicabilidad. En este documento se indicará qué

controles se consideran necesarios para el alcance del proyecto, cuáles ya están implementados y cuáles todavía necesitan trabajo.

También se dejará una justificación sencilla de por qué cada control aplica o no aplica. Cuando exista un procedimiento, registro, configuración o evidencia que respalde un control, se relacionará dentro del documento.

Resultado esperado: primera versión de la Declaración de Aplicabilidad.

Indicador: porcentaje de controles revisados y con estado identificado.

Actividad 13. Revisión y actualización de documentos

Componente que cubre: Componente 3. Tratamiento y selección de controles.

Durante esta etapa se revisarán los documentos que actualmente utiliza Soporte en Tecnología para determinar cuáles siguen siendo adecuados y cuáles necesitan ajustes.

El propósito no es rehacer el proceso ni la documentación existente. Por el contrario, el objetivo es aprovechar los documentos, registros y evidencias ya disponibles, actualizando únicamente aquellos aspectos que no reflejen la operación actual, se encuentren desactualizados o requieran la incorporación de elementos asociados al Sistema de Gestión de Seguridad de la Información (SGSI).

También se identificarán los documentos que todavía hacen falta, de manera que la empresa pueda continuar desarrollándolos después del periodo académico.

Resultado esperado: documentos prioritarios revisados y relación de documentos pendientes.

Indicador: porcentaje de documentos priorizados que fueron revisados o actualizados.

Actividad 14. Fortalecimiento de configuraciones —Hardening—

Componente que cubre: Componente 5. Fortalecimiento de la postura de ciberseguridad.

Subcomponente: 5.1. Fortalecimiento de configuraciones seguras.

Se revisarán las configuraciones de algunos servidores, estaciones de trabajo y dispositivos de red incluidos dentro del alcance. La revisión estará enfocada en encontrar ajustes que puedan

mejorar su seguridad, como deshabilitar servicios que no se utilicen, corregir configuraciones por defecto o revisar permisos que no sean necesarios.

Los cambios que puedan aplicarse sin afectar la operación se realizarán durante el proyecto. Cuando un ajuste necesite una ventana de mantenimiento, una autorización adicional o represente algún riesgo para la continuidad del servicio, quedará registrado para ejecutarse posteriormente.

Resultado esperado: activos priorizados revisados, ajustes aplicados cuando sea posible y acciones pendientes documentadas.

Indicador: porcentaje de activos priorizados revisados y con acciones de mejora definidas.

Actividad 15. Revisión de identidades y accesos

Componente que cubre: Componente 5. Fortalecimiento de la postura de ciberseguridad.

Subcomponente: 5.2. Gestión de identidades y accesos.

En esta actividad se revisarán las cuentas de usuario, los grupos, los permisos y los accesos administrativos relacionados con los sistemas incluidos en el alcance.

La revisión permitirá identificar cuentas que ya no se utilicen, accesos que dejaron de ser necesarios o usuarios que tengan más privilegios de los requeridos para su trabajo. Cuando sea posible, estos ajustes se realizarán durante el proyecto. Los casos que dependan de la aprobación de otro responsable quedarán registrados para su posterior gestión.

Resultado esperado: cuentas y accesos revisados, con los ajustes realizados y las acciones pendientes identificadas.

Indicador: porcentaje de cuentas priorizadas revisadas y número de accesos que requieran ajuste.

Actividad 16. Monitoreo y gestión de registros de seguridad

Componente que cubre: Componente 5. Fortalecimiento de la postura de ciberseguridad.

Subcomponente: 5.3. Monitoreo y gestión de registros.

Se revisará cómo se están generando y almacenando los registros de los servidores, estaciones de trabajo, aplicaciones y dispositivos de red que hacen parte del alcance.

La finalidad es conocer qué registros pueden ser útiles cuando se presenta una falla, una alerta o un incidente de seguridad. También se revisará dónde se están almacenando, quién tiene acceso a ellos y qué herramientas disponibles en la empresa pueden facilitar su consulta y seguimiento.

A partir de esta revisión se definirán criterios básicos para organizar los registros y aprovechar mejor la información que ya generan los sistemas.

Resultado esperado: esquema inicial para la gestión de registros de seguridad, con fuentes y responsables definidos.

Indicador: porcentaje de activos críticos que generan registros disponibles para revisión y seguimiento.

Actividad 17. Aplicación de controles prioritarios

Componente que cubre: Componente 4. Implementación inicial.

Con base en los riesgos identificados, se seleccionarán algunos controles que puedan fortalecerse o implementarse dentro del tiempo disponible.

La prioridad será trabajar sobre acciones que generen un resultado visible y que realmente ayuden a reducir riesgos. Dependiendo de los hallazgos, estas acciones podrán estar relacionadas con respaldos, accesos, mantenimiento, vulnerabilidades, monitoreo o actualización documental.

Cada control aplicado deberá dejar una evidencia que permita comprobar qué se hizo y cuál fue el resultado.

Resultado esperado: controles prioritarios aplicados y soportados con evidencias.

Indicador: número de controles implementados o fortalecidos durante el proyecto.

Actividad 18. Prueba piloto con herramientas de Inteligencia Artificial

Componente que cubre: Componente 6. Prueba piloto de Inteligencia Artificial como apoyo al proceso.

En esta actividad se tomará una muestra de la información que ya genera Soporte en Tecnología, como tickets, registros de eventos o reportes técnicos, para revisar si una herramienta de Inteligencia Artificial puede ayudar a organizarla y facilitar su análisis.

La prueba se concentrará en tareas puntuales, por ejemplo, clasificar tickets, agrupar casos similares, revisar algunos registros o apoyar la preparación de reportes. La herramienta se utilizará únicamente como apoyo y los resultados deberán ser revisados por el personal responsable antes de ser considerados válidos.

Durante la prueba se comparará el resultado obtenido con la forma actual de realizar estas tareas. Con esto se podrá identificar si realmente aporta alguna mejora, si presenta limitaciones o si su uso no resulta conveniente para el proceso.

Al finalizar, se dejará un registro de lo realizado, los resultados obtenidos y una conclusión sobre la conveniencia de continuar o no con este tipo de apoyo en etapas posteriores del SGSI.

Resultado esperado: prueba piloto documentada con los resultados obtenidos, las limitaciones encontradas y una conclusión sobre su utilidad para el proceso.

Indicador: porcentaje de resultados considerados útiles o correctos después de la revisión realizada por el personal responsable.

Actividad 19. Definición de indicadores de seguimiento

Componente que cubre: Componente 5. Seguimiento y mejora.

Para saber si las acciones realizadas están generando algún avance, se definirán indicadores sencillos que puedan mantenerse después de finalizar el proyecto.

No se pretende crear una gran cantidad de indicadores, sino seleccionar aquellos que realmente ayuden a entender cómo está funcionando el proceso.

Se podrán revisar aspectos como los activos inventariados, los riesgos tratados, los incidentes atendidos, los respaldos verificados, las vulnerabilidades pendientes y el avance de las acciones definidas.

Entre los indicadores que pueden utilizarse se encuentran:

- porcentaje de activos identificados y clasificados;
- porcentaje de riesgos que cuentan con tratamiento;
- número de incidentes registrados por tipo;
- porcentaje de respaldos verificados;
- vulnerabilidades críticas identificadas y corregidas;
- porcentaje de controles que cuentan con evidencia;
- avance del plan de tratamiento.

Cada indicador deberá tener una fuente de información clara y un responsable encargado de su seguimiento.

Resultado esperado: conjunto inicial de indicadores para el seguimiento del SGSI.

Indicador: número de indicadores definidos con fuente, responsable y periodicidad.

Actividad 20. Revisión de resultados y recomendaciones

Componente que cubre: Componente 5. Seguimiento y mejora.

Al terminar el periodo del proyecto se revisará qué cambió frente al diagnóstico inicial. La intención será identificar qué actividades se alcanzaron a completar, cuáles tuvieron avances parciales y cuáles deberán continuar después.

También se revisarán las dificultades encontradas durante la ejecución, ya que estas pueden mostrar necesidades de recursos, apoyo de otras áreas o decisiones que dependen de la Dirección.

A partir de esta revisión se elaborarán recomendaciones para continuar con la implementación del SGSI. De esta manera, el cierre del trabajo académico no significará que el proceso termina, sino que quedará una ruta definida para seguir avanzando.

Resultado esperado: informe de resultados, actividades pendientes y recomendaciones de continuidad.

Indicador: porcentaje de actividades ejecutadas y número de acciones que quedan programadas para una siguiente etapa.

La secuencia de actividades permite pasar de la revisión del proceso a la identificación de riesgos y, posteriormente, a la aplicación de mejoras concretas. Los primeros componentes se concentran en entender cómo se encuentra actualmente Soporte en Tecnología; los siguientes permiten decidir qué riesgos necesitan mayor atención y qué controles pueden utilizarse para tratarlos.

Finalmente, las actividades de seguimiento permiten comparar lo planeado con lo que realmente se logró. Esto ayudará a que Skaphe Tecnología S.A.S. no vea el SGSI únicamente como un conjunto de documentos, sino como una forma de organizar y mejorar progresivamente la manera en que se protege la información y se administran los servicios tecnológicos.

3.4. DESCRIPCIÓN DE RECURSOS NECESARIOS PARA LA EJECUCIÓN DE LA SOLUCIÓN

La ejecución del plan requiere recursos humanos, documentales, tecnológicos, físicos y financieros. La mayor parte de estos recursos ya se encuentran disponibles en Skaphe Tecnología S.A.S., por lo que el proyecto se apoyará principalmente en la infraestructura, las herramientas y el personal que actualmente participa en el proceso de Soporte en Tecnología.

De acuerdo con el alcance definido para el proyecto, **los recursos utilizados y las actividades técnicas desarrolladas estarán limitados a la sede Montevideo**. La sede Calle 64 no será intervenida directa y únicamente se tendrá en cuenta cuando exista alguna relación con servicios, usuarios, aplicaciones o infraestructura administrada desde Montevideo. Esta delimitación también aplica para el acceso a servidores, estaciones de trabajo, dispositivos de red, sistemas de almacenamiento y demás activos tecnológicos.

Recursos humanos

La participación del personal será necesaria para obtener información, validar los resultados y apoyar la aplicación de los controles seleccionados.

Responsable del proyecto: estará a cargo de organizar las actividades, revisar la documentación, consolidar las evidencias y presentar los resultados obtenidos.

Personal de Soporte en Tecnología: proporcionará información sobre los activos, servicios, incidentes, mantenimientos, respaldos, accesos y configuraciones que hacen parte de la sede Montevideo.

Dirección Estratégica: participará en la aprobación de lineamientos, asignación de recursos y decisiones relacionadas con los riesgos que requieran aceptación o tratamiento.

Gestión Integral de Procesos: apoyará la actualización de documentos, el control de versiones y la integración del SGSI con el Sistema de Gestión Integral existente.

Líderes de Gestión Documental y Tecnología de la Información: apoyarán la identificación de activos, necesidades y requisitos que tengan relación con los servicios tecnológicos administrados desde la sede Montevideo.

Directores, coordinadores y responsables de procesos: colaborarán en la validación de responsables de activos, niveles de criticidad, accesos y acciones de tratamiento cuando corresponda.

Usuarios finales: podrán aportar información sobre los activos que utilizan, reportar incidentes y participar en la validación de algunos controles.

Proveedores y terceros: intervendrán únicamente cuando sea necesario atender actividades relacionadas con garantías, licenciamiento, conectividad, mantenimiento especializado o servicios contratados incluidos dentro del alcance.

Recursos documentales

Para desarrollar el proyecto será necesario consultar los documentos y registros que actualmente respaldan la operación de Soporte en Tecnología. Entre ellos se encuentran:

- Mapa de procesos de Skaphe Tecnología S.A.S.
- Caracterización de Soporte en Tecnología.
- Procedimiento de Servicios de Soporte en Tecnología.
- Procedimiento de Mantenimiento Preventivo.
- Procedimiento de Borrado de Información.

- Manual de usuario de la Mesa de Ayuda.
- Inventarios tecnológicos.
- Hojas de vida de los equipos.
- Cronogramas y registros de mantenimiento.
- Registros de copias de seguridad.
- Tickets de incidentes y requerimientos.
- Informes técnicos y evidencias.
- Políticas y procedimientos institucionales.
- Matrices de riesgos existentes.
- Requisitos contractuales y de clientes.
- Documentación del Sistema de Gestión Integral.
- ISO/IEC 27001:2022 y demás documentos de referencia utilizados en el proyecto.

La revisión de estos documentos permitirá conocer qué controles ya existen, cuáles necesitan ajustes y qué información puede utilizarse como evidencia para el SGSI.

Recursos tecnológicos

Para desarrollar las actividades del proyecto se utilizarán principalmente herramientas e infraestructura que Skaphe Tecnología S.A.S. ya tiene disponibles para su operación. Su uso estará relacionado únicamente con los activos y servicios incluidos dentro del alcance de la sede Montevideo.

Entre los recursos tecnológicos que podrán ser consultados o utilizados se encuentran:

- GLPI o la plataforma de Mesa de Ayuda, para consultar incidentes, requerimientos, activos y evidencias.
- Active Directory, para revisar usuarios, grupos, cuentas y privilegios relacionados con el alcance.
- Zabbix, como fuente de información sobre disponibilidad y estado de los servicios tecnológicos.

- Wazuh, para consultar eventos de seguridad relacionados con los activos seleccionados.
- Greenbone/OpenVAS, como apoyo para la identificación y revisión de vulnerabilidades sobre activos previamente autorizados.
- FortiGate, para revisar aspectos relacionados con conectividad, segmentación y controles perimetrales.
- RustDesk, para realizar actividades de soporte remoto cuando se encuentren autorizadas.
- Servidores y máquinas virtuales incluidos dentro del alcance.
- Sistemas de almacenamiento y respaldo utilizados por los servicios de la sede Montevideo.
- Herramientas ofimáticas para elaborar matrices, procedimientos, informes y demás productos del proyecto.
- Repositorios documentales para conservar versiones y evidencias.
- Equipos de cómputo utilizados durante el desarrollo de las actividades.

Estas herramientas **no serán implementadas ni administradas desde cero como parte del proyecto**, debido a que ya forman parte de la infraestructura tecnológica y de las actividades habituales de Soporte en Tecnología. La administración diaria, actualización, mantenimiento y atención de fallas asociadas con ellas continuará haciendo parte de la operación normal del área y, por lo tanto, no se considera un costo adicional atribuible al proyecto.

Las horas de Soporte en Tecnología incluidas en el presupuesto corresponden únicamente al tiempo adicional requerido para apoyar actividades específicas del proyecto, como consultar información, levantar inventarios, validar configuraciones, proporcionar evidencias, apoyar evaluaciones técnicas y aplicar ajustes previamente definidos.

Si durante la ejecución se identifica un cambio que requiera una dedicación técnica considerable, una nueva implementación o una intervención diferente a la operación habitual, este deberá ser evaluado por separado antes de ser incorporado al proyecto.

El uso de estos recursos se limitará a los activos autorizados de la sede Montevideo. No se realizarán pruebas, cambios de configuración, evaluaciones de vulnerabilidades ni intervenciones directas sobre equipos pertenecientes a la sede Calle 64. Cuando exista alguna dependencia con servicios administrados desde Montevideo, esta se documentará únicamente como una interfaz, sin ampliar el alcance definido.

Recursos físicos y materiales

Se requerirán espacios para reuniones, revisión documental, validación de resultados y actividades de socialización. También podrán utilizarse herramientas de mantenimiento, medios de almacenamiento controlados, material de capacitación y formatos para registrar las actividades realizadas.

Cuando sea necesario acceder físicamente o de manera remota a un servidor, computador, dispositivo de red u otro activo, **el acceso deberá estar previamente autorizado y corresponder a infraestructura incluida dentro del alcance de la sede Montevideo.**

Las intervenciones técnicas deberán realizarse procurando no afectar la continuidad de los servicios y respetando los procedimientos internos de la organización. Los cambios que puedan generar interrupciones deberán ser programados y aprobados antes de su ejecución.

Recursos financieros

Aunque varias de las herramientas utilizadas ya están disponibles en la organización o corresponden a soluciones de código abierto, la ejecución del proyecto requiere tiempo del personal y algunos recursos complementarios.

Los principales costos pueden estar relacionados con:

- Horas de trabajo del responsable del proyecto.
- Tiempo dedicado por Soporte en Tecnología y demás participantes.
- Configuración o ajuste de herramientas.
- Capacitación y actividades de sensibilización.
- Almacenamiento adicional para registros o respaldos.
- Reposición de equipos cuando se identifique una necesidad dentro del alcance.

- Renovación de licencias cuando corresponda.
- Servicios especializados de proveedores.
- Auditorías o pruebas externas que sean aprobadas.
- Materiales necesarios para la implementación de controles.
- Contingencias asociadas con las actividades del proyecto.

Las necesidades que involucren infraestructura o activos ubicados exclusivamente en la sede Calle 64 no serán incluidas como costos directos de esta intervención. En caso de identificarse alguna dependencia que pueda afectar los servicios administrados desde Montevideo, se registrará como recomendación para una etapa posterior.

Recursos de tiempo

El proyecto académico tiene una duración limitada, por lo que será necesario priorizar las actividades que puedan generar resultados verificables durante el periodo disponible.

El tiempo se concentrará principalmente en:

- Actualizar la información del proceso.
- Consolidar el inventario de activos del alcance.
- Definir la metodología y matriz de riesgos.
- Elaborar el plan de tratamiento.
- Preparar la Declaración de Aplicabilidad preliminar.
- Actualizar documentos prioritarios.
- Aplicar los controles seleccionados.
- Establecer indicadores y recomendaciones.

Las actividades que no puedan finalizarse durante el periodo académico quedarán registradas para continuar su ejecución posteriormente. De esta manera, los recursos disponibles se utilizarán sobre un alcance claramente definido y sin extender la intervención hacia activos o infraestructura que no forman parte de la sede Montevideo.

4. DEFINICIÓN DEL ALCANCE DE LA SOLUCIÓN, PARTES INTERESADAS, CRONOGRAMA Y PRESUPUESTOS.

En esta etapa se definieron las condiciones necesarias para llevar el plan de acción a una ejecución controlada. Para ello se establecieron los límites de la intervención, los resultados que se espera obtener, las personas y áreas que participarán, el tiempo requerido y los recursos económicos asociados.

La propuesta se concentra en el proceso de Soporte en Tecnología de la sede Montevideo de Skaphe Tecnología S.A.S. Este proceso fue seleccionado porque presta apoyo transversal a las áreas administrativas y misionales, y porque tiene a su cargo actividades relacionadas con equipos, usuarios, conectividad, aplicaciones, servidores, respaldos, mantenimiento y atención de incidentes tecnológicos.

Los procedimientos revisados muestran que Soporte en Tecnología ya cuenta con responsabilidades para recibir, clasificar, atender, documentar y cerrar solicitudes; además, los usuarios, líderes de proceso y proveedores intervienen en diferentes momentos de la atención. Esta distribución de funciones servirá como punto de partida para asignar las responsabilidades del proyecto.

La intervención académica se ejecutará durante agosto de 2026. En este periodo se elaborarán los principales documentos del SGSI, se revisarán los controles existentes y se implementarán las acciones que puedan completarse dentro del tiempo disponible. Las actividades que requieran mayor inversión, cambios de infraestructura, aprobación directiva o participación de proveedores quedarán incorporadas en un plan de continuidad de ocho meses.

El presupuesto fue calculado considerando principalmente el tiempo del personal, el uso de la infraestructura actual, la capacitación y algunos recursos complementarios. Debido a que

varias de las herramientas utilizadas por la organización son de código abierto o ya se encuentran implementadas, el proyecto no contempla inicialmente costos elevados de licenciamiento. Sin embargo, las horas dedicadas por los colaboradores representan un costo interno y deben incluirse para reflejar el valor real de la intervención.

4.1.ALCANCE FINAL DE LA SOLUCIÓN

El alcance final de la solución comprende el diseño y la implementación inicial de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001:2022 para fortalecer el proceso de Soporte en Tecnología de la sede Montevideo de Skaphe Tecnología S.A.S.

La intervención incluirá las actividades, personas, documentos, activos y servicios tecnológicos administrados directamente por este proceso y que apoyan el funcionamiento de las demás áreas de la organización. Aunque el SGSI tiene una naturaleza transversal, el proyecto académico no pretende intervenir de manera completa todos los procesos de la empresa, sino establecer una primera base que pueda ampliarse posteriormente.

Dentro del alcance se incluirán los equipos de cómputo, servidores físicos y virtuales, dispositivos de red, sistemas de almacenamiento, herramientas de monitoreo, plataformas de soporte, cuentas de usuario, aplicaciones, respaldos, medios de almacenamiento y documentos asociados con la operación tecnológica de la sede Montevideo. También se considerarán los servicios administrados por terceros cuando su disponibilidad o seguridad pueda afectar el proceso intervenido.

El procedimiento de servicios de soporte ya incluye equipos, periféricos, red de datos, acceso a internet, software, correo electrónico, aplicaciones, servicios compartidos, cuentas de usuario e inventario tecnológico. Por esta razón, estos elementos serán tomados como referencia para determinar los activos que deben identificarse y protegerse dentro del proyecto.

La solución comprenderá las siguientes actividades:

- Revisión del diagnóstico inicial del proceso de Soporte en Tecnología.
- Actualización de la caracterización del proceso para reflejar sus actividades, herramientas, responsables, entradas, salidas, riesgos y controles actuales.
- Identificación y clasificación de los activos de información y tecnológicos incluidos en el alcance.
- Definición de una metodología para identificar, analizar, evaluar y tratar riesgos de seguridad de la información.
- Elaboración de una matriz de riesgos que relacione activos, amenazas, vulnerabilidades, impactos y controles existentes.
- Elaboración de un plan de tratamiento para los riesgos que no puedan ser aceptados.
- Preparación de una Declaración de Aplicabilidad preliminar.
- Revisión y actualización de políticas, procedimientos, instructivos, formatos y registros prioritarios.
- Implementación inicial de controles relacionados con inventario, accesos, respaldos, incidentes, mantenimiento, monitoreo, vulnerabilidades y borrado seguro.
- Definición de indicadores y evidencias para realizar seguimiento a los controles.
- Elaboración de recomendaciones y un plan de continuidad para las actividades que deban ejecutarse después de finalizar el proyecto académico.

El mantenimiento preventivo será considerado dentro del alcance porque permite reducir fallas, anticipar deterioros, actualizar el inventario y generar evidencias sobre los activos tecnológicos. El procedimiento vigente también establece que los hallazgos deben registrarse y escalarse cuando puedan afectar el funcionamiento de los equipos.

El borrado seguro de información también hará parte de la intervención. Este control aplica a computadores, servidores, discos, memorias, dispositivos móviles, carpetas compartidas y

otros repositorios. Su incorporación permitirá relacionar la eliminación de información con su clasificación, ciclo de vida, responsable y evidencia de ejecución.

Límites de la intervención

La sede Calle 64 no hará parte del alcance formal. Sin embargo, será considerada como una interfaz cuando utilice infraestructura, servicios, aplicaciones, usuarios o recursos administrados desde la sede Montevideo.

El proyecto no contempla:

- La certificación de Skaphe Tecnología S.A.S. bajo ISO/IEC 27001:2022.
- La implementación completa de todos los controles de la norma.
- La ejecución de pruebas invasivas que puedan afectar los sistemas en producción.
- La renovación total de servidores, equipos de red o estaciones de trabajo.
- La compra de herramientas comerciales que no hayan sido aprobadas previamente.
- La realización de una auditoría de certificación.
- La intervención completa de procesos diferentes a Soporte en Tecnología.
- La solución definitiva de riesgos que requieran inversiones superiores al presupuesto del proyecto.

Cuando se identifiquen necesidades relacionadas con reposición de equipos, licencias, infraestructura adicional, contratación de personal o servicios especializados, estas se documentarán dentro del plan de tratamiento para que la Dirección pueda evaluarlas posteriormente.

Resultados esperados

Al finalizar la intervención se espera contar con:

- Caracterización actualizada de Soporte en Tecnología.
- Inventario inicial de activos del alcance.
- Clasificación de activos según su criticidad.
- Metodología de riesgos documentada.
- Matriz de riesgos de seguridad de la información.
- Relación de controles existentes.
- Plan de tratamiento de riesgos.
- Declaración de Aplicabilidad preliminar.
- Documentos prioritarios revisados o actualizados.
- Evidencias de controles implementados.
- Indicadores de seguimiento.
- Informe de resultados y recomendaciones.
- Plan de continuidad para los meses posteriores.

La solución se considerará cumplida cuando los productos definidos hayan sido elaborados, revisados y presentados a los responsables del proceso, y cuando exista evidencia de la implementación de los controles seleccionados para el periodo académico.

4.2.IDENTIFICACIÓN DE RESPONSABLES DE LAS ACTIVIDADES PARA EJECUCIÓN

La ejecución del proyecto requiere la participación coordinada de la Dirección, Soporte en Tecnología, Gestión Integral de Procesos, líderes de las áreas y usuarios. Cada participante tendrá responsabilidades diferentes según su conocimiento, autoridad y relación con los activos de información.

Los documentos actuales ya asignan funciones a Soporte en Tecnología, usuarios, directores, coordinadores y proveedores. Por ejemplo, Soporte debe documentar las actividades

realizadas; los usuarios deben reportar las fallas y validar las soluciones; los líderes deben priorizar necesidades y autorizar requerimientos, y los proveedores deben atender casos especializados cuando corresponda.

Partes interesadas internas

Dirección Estratégica: autoriza el proyecto, proporciona orientación, aprueba recursos y toma decisiones sobre los riesgos que requieran inversión o aceptación formal.

Responsable del proyecto o responsable inicial del SGSI: coordina las actividades, consolida los documentos, organiza las evidencias, realiza el seguimiento y presenta los resultados.

Soporte en Tecnología: aporta la información técnica, participa en la identificación de activos, revisa los riesgos, implementa controles y conserva las evidencias correspondientes.

Gestión Integral de Procesos o HSEQ: apoya el control documental, la actualización de la caracterización, la integración con los sistemas de gestión existentes y la revisión de indicadores.

Líderes de Gestión Documental y Tecnología de la Información: identifican los activos y servicios críticos utilizados por los procesos misionales.

Gestión de Personal: apoya actividades relacionadas con usuarios, responsabilidades, ingreso, retiro, formación y sensibilización.

Gestión de Compras: participa cuando el tratamiento de un riesgo requiere adquisición de equipos, licencias, repuestos o servicios.

Gestión Financiera y Contable: revisa la disponibilidad presupuestal y realiza seguimiento a los costos aprobados.

Usuarios finales: informan sobre los activos que utilizan, reportan incidentes, cumplen los controles definidos y validan las soluciones aplicadas.

Partes interesadas externas

Clientes: esperan que la información entregada a la organización sea tratada de manera segura y que los servicios se mantengan disponibles.

Proveedores tecnológicos: intervienen en servicios de conectividad, licenciamiento, garantías, mantenimiento especializado, infraestructura y soporte.

Auditores: verifican la existencia, aplicación y eficacia de los controles y las evidencias.

Entidades regulatorias y autoridades: establecen requisitos legales relacionados con protección de datos, conservación documental, seguridad y cumplimiento contractual.

Tabla 1

Asignación de responsabilidades

Actividad	Responsable principal	Apoyo requerido	Resultado evidencia
Validar el diagnóstico	Responsable del proyecto	Soporte y Gestión Integral	Diagnóstico aprobado
Actualizar la caracterización	Gestión Integral de Procesos	Soporte en Tecnología	Caracterización actualizada
Identificar partes interesadas	Responsable del proyecto	Dirección y líderes de proceso	Matriz de partes interesadas
Levantar el inventario de activos	Soporte en Tecnología	Usuarios y líderes	Inventario actualizado
Clasificar los activos	Responsable del proyecto	Propietarios de activos	Activos valorados
Definir la metodología de riesgos	Responsable del proyecto	Gestión Integral y Dirección	Metodología documentada
Identificar amenazas y vulnerabilidades	Soporte en Tecnología	Líderes y proveedores	Escenarios de riesgo

Actividad	Responsable principal	Apoyo requerido	Resultado o evidencia
Evaluar los riesgos	Responsable del proyecto	Soporte y propietarios	Matriz de riesgos
Revisar controles existentes	Soporte en Tecnología	Gestión Integral	Matriz de controles
Elaborar el plan de tratamiento	Responsable del proyecto	Dirección y responsables	Plan de tratamiento
Elaborar la Declaración de Aplicabilidad	Responsable del proyecto	Gestión Integral y Dirección	SoA preliminar
Actualizar documentos	Gestión Integral de Procesos	Soporte y líderes	Documentos controlados
Implementar controles prioritarios	Soporte en Tecnología	Proveedores y usuarios	Evidencias técnicas
Definir indicadores	Responsable del proyecto	Gestión Integral	Matriz de indicadores
Evaluar resultados	Responsable del proyecto	Dirección y Soporte	Informe final
Aprobar continuidad	Dirección Estratégica	Responsables de proceso	Plan aprobado

En las actividades relacionadas con mantenimiento, el área de Soporte deberá programar y registrar las intervenciones, mientras que los usuarios deberán facilitar los equipos y validar

su funcionamiento. Los líderes de proceso deberán priorizar los activos críticos y autorizar los cambios o reposiciones que se requieran.

Para el borrado de información, Soporte en Tecnología será responsable de ejecutar o coordinar la actividad, mientras que el propietario del proceso deberá autorizarla. Gestión Documental, HSEQ o el área competente revisará las obligaciones de conservación cuando corresponda.

4.3. CRONOGRAMA DE EJECUCIÓN

La fase académica se desarrollará durante agosto de 2026. Sin embargo, teniendo en cuenta que la implementación completa de un SGSI no puede realizarse en un solo mes, se propone un cronograma de nueve meses que combina la ejecución inicial con un plan de continuidad.

Los meses del cronograma corresponden a:

- **Mes 1:** agosto de 2026.
- **Mes 2:** septiembre de 2026.
- **Mes 3:** octubre de 2026.
- **Mes 4:** noviembre de 2026.
- **Mes 5:** diciembre de 2026.
- **Mes 6:** enero de 2027.
- **Mes 7:** febrero de 2027.
- **Mes 8:** marzo de 2027.
- **Mes 9:** abril de 2027.

Tabla 2*Cronograma de actividades*

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9
Validación del diagnóstico y actualización del proceso	X								
Inventario y clasificación de activos	X	X							
Metodología y matriz de riesgos	X	X							
Plan de tratamiento y Declaración de Aplicabilidad	X	X	X						
Actualización de políticas, procedimientos y formatos	X	X	X	X					
Implementación de controles prioritarios	X	X	X	X	X	X			
Capacitación y sensibilización	X	X		X		X		X	
Seguimiento de indicadores y evidencias	X	X	X	X	X	X	X	X	X
Revisión interna y plan de mejora			X			X			X

Los principales hitos serán la aprobación del diagnóstico, la consolidación del inventario, la elaboración de la matriz de riesgos, la preparación del plan de tratamiento, la implementación de controles prioritarios y la presentación del informe final.

Durante los meses posteriores se realizará el seguimiento a las acciones que no puedan cerrarse durante agosto. Esto incluye los controles que dependan de compras, proveedores, cambios de infraestructura, capacitación continua, aprobaciones directivas o ajustes operativos.

4.4.PRESUPUESTO

El presupuesto presenta una estimación de los recursos necesarios para desarrollar la fase inicial del proyecto. Los valores están expresados en pesos colombianos y corresponden principalmente al tiempo que deberá destinar el personal a actividades directamente relacionadas con la intervención.

Para realizar esta estimación se tuvieron en cuenta las horas del responsable del proyecto, el acompañamiento de Soporte en Tecnología, la participación de Gestión Integral de Procesos y el apoyo de los líderes que deberán intervenir en las revisiones y validaciones. También se contemplaron algunos recursos para capacitación, almacenamiento de evidencias, materiales y contingencias.

En el caso de Soporte en Tecnología se estimaron **32 horas de participación directa en el proyecto**. Este tiempo no corresponde a la administración completa de las plataformas tecnológicas de la empresa. Está destinado únicamente a actividades adicionales generadas por el proyecto, como el levantamiento y validación de activos, consulta de registros, revisión de configuraciones, apoyo en la evaluación de vulnerabilidades, generación de evidencias y aplicación de algunos controles priorizados.

Herramientas como GLPI, Active Directory, Zabbix, Wazuh, Greenbone/OpenVAS, FortiGate y RustDesk ya son utilizadas dentro de la operación tecnológica de la organización. Por esta razón, las actividades habituales de administración, soporte, actualización y mantenimiento de estas plataformas no se cargan como un costo adicional al proyecto. Solo se contabiliza el

tiempo que el personal deberá dedicar específicamente a las actividades definidas en el plan de trabajo.

De esta manera, las 32 horas asignadas a Soporte en Tecnología corresponden a una participación puntual y complementaria, mientras que la operación regular de las herramientas continúa desarrollándose dentro de las funciones habituales del área.

Tabla 3

Presupuesto

Rubro	Valor
Responsable del proyecto: 80 horas estimadas	\$3.200.000
Participación adicional de Soporte en Tecnología para actividades del proyecto: 32 horas	\$1.120.000
Participación de Gestión Integral y líderes de procesos	\$960.000
Actividad de capacitación y sensibilización	\$300.000
Almacenamiento, respaldos y conservación de evidencias	\$500.000
Materiales, formatos y comunicaciones	\$100.000
Licenciamiento adicional de herramientas utilizadas en el proyecto	\$0
Contingencia del 10 %	\$618.000
Total estimado	\$6.798.000

El valor asignado al responsable del proyecto contempla el tiempo utilizado para revisar documentos, elaborar matrices, coordinar reuniones, analizar riesgos, preparar el plan de tratamiento y consolidar los resultados.

Las 32 horas destinadas a Soporte en Tecnología cubren exclusivamente su participación adicional en las actividades del proyecto. No incluyen la administración cotidiana de GLPI, Zabbix, Wazuh, Greenbone/OpenVAS, FortiGate, Active Directory o RustDesk, debido a que estas tareas forman parte de las funciones habituales del área.

La participación de Gestión Integral y de los líderes de proceso contempla el tiempo necesario para revisar documentos, validar responsables, confirmar requisitos y aprobar los resultados relacionados con sus procesos. El presupuesto también considera una actividad de sensibilización y la preparación del material requerido para su desarrollo.

El valor destinado a almacenamiento busca cubrir posibles necesidades adicionales para conservar reportes, registros, eventos, respaldos y demás evidencias generadas durante la intervención. La contingencia se mantiene para cubrir variaciones menores que puedan presentarse durante la ejecución.

No se incluyen dentro de este presupuesto:

- Compra o renovación de servidores.
- Reemplazo masivo de computadores.
- Adquisición de antivirus o EDR comercial.
- Contratación de una auditoría de certificación.
- Compra de equipos de red o sistemas de almacenamiento de gran capacidad.
- Servicios especializados que no hayan sido previamente cotizados.
- Costos asociados con la certificación ISO/IEC 27001:2022.
- Administración ordinaria de las plataformas tecnológicas que ya forman parte de la operación de Skaphe Tecnología S.A.S.

Si durante la evaluación de riesgos se determina que alguno de estos recursos es necesario, deberá elaborarse una solicitud independiente con su respectiva justificación técnica y financiera. Esto permite que el presupuesto del proyecto se concentre en las actividades directamente relacionadas con la intervención y no incluya costos que actualmente hacen parte de la operación normal de la organización.

5. REFERENCIAS BIBLIOGRÁFICAS

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

Skaphe Tecnología S.A.S. (2023). *Caracterización de procesos: Soporte en Tecnología* (C-ST-001, versión 4) [Documento interno no publicado].

Skaphe Tecnología S.A.S. (2024). *Procedimiento de borrado de información* (P-ST-004, versión 0) [Documento interno no publicado].

Skaphe Tecnología S.A.S. (2025). *Procedimiento de mantenimiento preventivo* (P-ST-002, versión 6) [Documento interno no publicado].

Skaphe Tecnología S.A.S. (2026a). *Estructura de procesos de Skaphe Tecnología S.A.S.* (MP-HSEQ-001, versión 6) [Documento interno no publicado].

Skaphe Tecnología S.A.S. (2026b). *Procedimiento de servicios de soporte en tecnología* (P-ST-001, versión 6) [Documento interno no publicado].

Skaphe Tecnología S.A.S. (s. f.-a). *Custodia y administración documental*.

<https://www.skaphe.com/servicios/gestion-documental/custodia-y-administracion-documental>

Skaphe Tecnología S.A.S. (s. f.-b). *Quiénes somos*.

<https://www.skaphe.com/nosotros/quienes-somos>