Estudio de Vulnerabilidades y Propuesta de Implementación Norma ISO 27001. Mejora De La Seguridad Informática Para La Empresa Security S.A.S.

Trabajo final presentado por:	Cristian David López Arenas Clara Inés Silva Jiménez
Programa:	Especialización en Ciberseguridad
Docente:	Fabricio Echeverría Briones
Fecha:	Julio/2026

Índice de contenidos

RESUMEN

Actualmente, la seguridad de la información es un proceso minucioso y de gran importancia para una organización, ya que permite proteger su activo más valioso: *la información*. Por ello, las empresas buscan certificarse con la norma ISO 27001, pues esta les permite proyectarse ante sus clientes como organizaciones seguras, fortaleciendo los lazos de confianza mediante una certificación reconocida internacionalmente.

Esta norma busca mejorar la integridad, la confidencialidad y la disponibilidad de los datos. Asimismo, la ISO 27001 contribuye a garantizar que todo trámite, servicio, sistema de información, infraestructura y activo de información sea resguardado de manera segura, que sea accesible únicamente para las personas autorizadas y que mantenga su integridad al momento de ser consultado o utilizado.

Palabras clave: Sistema de Gestión de Seguridad de la Información, confidencialidad, integridad, disponibilidad, ciberseguridad.

Confidencialidad: Propiedad de la información que garantiza que esta no esté disponible ni sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de la información que busca preservar su exactitud, consistencia y completitud durante todo su ciclo de vida.

Disponibilidad: Propiedad de la información que garantiza que sea accesible y utilizable cuando una parte interesada autorizada la requiera.

***Sistema de Gestión de Seguridad de la Información (SGSI*)**: Conjunto de políticas, manuales, procedimientos, controles y técnicas utilizados para gestionar y proteger los activos de información de una organización, de acuerdo con los requisitos establecidos en la norma ISO 27001.

Ciberseguridad: Proceso de proteger los activos de información mediante la gestión y el tratamiento de las amenazas que afectan la información procesada, almacenada y/o transmitida a través de sistemas de información interconectados.

ABSTRACT

Currently, information security is a meticulous and crucial process for any organization, as it protects its most valuable asset: information. Therefore, companies seek ISO 27001 certification, which allows them to project a secure image to their clients, strengthening trust through an internationally recognized certification.

This standard aims to improve data integrity, confidentiality, and availability. Furthermore, ISO 27001 helps ensure that every process, service, information system, infrastructure, and information asset is securely protected, accessible only to authorized personnel, and maintains its integrity when consulted or used.

Keywords: Information Security Management System, confidentiality, integrity, availability, cybersecurity.

Confidentiality: The property of information that guarantees it is not available or disclosed to unauthorized individuals, entities, or processes.

Integrity: The property of information that seeks to preserve its accuracy, consistency, and completeness throughout its lifecycle.

Availability: The property of information that ensures it is accessible and usable when required by an authorized stakeholder.

Information Security Management System: A set of policies, manuals, procedures, controls, and techniques used to manage and protect an organization's information assets, in accordance with the requirements established in ISO 27001.

Cybersecurity: The process of protecting information assets by managing and addressing threats that affect information processed, stored, and/or transmitted through interconnected information systems.

1. INTRODUCCIÓN

Este proyecto de aplicación, desarrollado bajo la metodología de investigación-acción, se centró en la identificación y resolución de los hallazgos de una auditoría vigente, así como en la implementación de políticas de seguridad. Además, buscó fortalecer la infraestructura tecnológica y mejorar los protocolos de seguridad existentes, con el fin de preparar a la empresa para obtener la certificación bajo los estándares de la norma ISO 27001, integrando la teoría y la práctica en un entorno organizacional real.

Mediante este enfoque de investigación-acción, se desarrollaron habilidades de diagnóstico, análisis y planificación orientadas a mejorar la eficiencia y la efectividad de un proceso crítico dentro de la organización. La estructura del proyecto incluyó una revisión exhaustiva del contexto organizacional, la identificación de oportunidades de mejora y la implementación de una solución viable que respondiera a las necesidades de la empresa, optimizando su desempeño y fortaleciendo su Sistema de Gestión de Seguridad de la Información.

1.1. OBJETIVO GENERAL

El objetivo principal del proyecto es desarrollar una solución operativa para abordar la actualización, mejora e implementación de las políticas de seguridad de la información basadas en la norma ISO 27001 en una compañía que ha experimentado incidentes y problemas de seguridad. Para ello, se identificará la información sensible, se fortalecerá la seguridad de las aplicaciones desde su etapa de desarrollo y se controlará el acceso a los recursos críticos por parte de la empresa implementadora Security S.A.S.

La intervención no solo consistió en corregir las deficiencias identificadas, sino también en proponer una solución sostenible que pudiera integrarse a la estructura organizacional. De esta manera, se busca elevar los niveles de eficiencia, fortalecer el Sistema de Gestión de Seguridad de la Información y alcanzar los estándares de desempeño requeridos para el proceso intervenido, garantizando la protección de los activos de información de la organización.

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 desarrollo del proyecto se estructuró en tres etapas secuenciales, cada una de las cuales abordó un aspecto específico de la intervención. En la primera etapa, se identificó y analizó el problema organizacional, incluyendo una descripción detallada de la organización, su misión, visión y el proceso específico afectado. La segunda etapa se centró en la planificación de la solución, estableciendo objetivos y actividades concretas para abordar el problema. En la tercera fase, se definieron aspectos operativos como el cronograma, el presupuesto y la asignación de roles.

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.

Para el diagnóstico del problema se empleó la metodología de Gestión de Riesgos de Seguridad de la Información, estructurada de acuerdo con los lineamientos establecidos por la norma ISO/IEC 27001. Como punto de partida, se analizaron las políticas de seguridad vigentes de la organización con el propósito de identificar oportunidades de mejora, actualizar los controles existentes y fortalecer el nivel de seguridad de la información, contribuyendo así a la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los requisitos de la norma.

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

El problema identificado para este proyecto es una gran falta de seguridad en todos sus procesos de información. Esta situación se presenta en una empresa la cual la parte encargada de la prestación de servicios de auditoría de seguridad de la información ha presentado fallas constantes en la implementación de políticas y controles de seguridad enfatizados en la norma ISO/IEC 27001. La organización anteriormente mencionada, ha tenido un crecimiento acelerado, ya que integró nuevas sedes y empresas a sus servicios, priorizando la parte operativa y su crecimiento organizativo, sin tener en cuenta una planificación estratégica en materia de seguridad de los procesos de gestión de la información y la infraestructura tecnológica.

Esta falta de seguridad se ve reflejada en: (una inexistencia de políticas corporativas de seguridad de la información, la ausencia de procedimientos estandarizados para la protección de activos de información, la falta de clasificación de la información, el escaso control en los accesos a los sistemas, inexistencia de mecanismos de monitoreo y registro de eventos, la falta capacitaciones y sensibilizaciones al personal, que dificultan la identificación de vulnerabilidades y aumentan el riesgo de incidentes que afectan a la confidencialidad, integridad y disponibilidad de información).

Adicionalmente, la organización carece de una metodología para gestionar los riesgos de seguridad de la información, lo que dificulta su capacidad para identificar, evaluar y mitigar las amenazas a procesos institucionales de carácter crítico. La falta de auditorías periódicas y salvaguardias técnicas, incluidos sistemas de detección y prevención de intrusiones, vigilancia continua y capacidad de respuesta a incidentes, dificulta la capacidad de la organización para prevenir ciberataques y detectar rápidamente actividades anómalas dentro de su red corporativa.

En efecto de estas deficiencias de seguridad, la organización ha tenido incidentes de fuga de información cuya causa no se ha determinado con precisión, debido a la falta de evidencia

técnica y registros que permitan realizar un análisis forense. Esta situación incrementa el riesgo de pérdida de información confidencial, afectación de la propiedad intelectual, incumplimiento de requisitos legales y contractuales, deterioro de la confianza de clientes y socios comerciales, así como posibles pérdidas económicas derivadas de incidentes de seguridad.

En consecuencia de estos efectos, la organización requiere implementar un Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001, con el propósito de establecer controles organizacionales, físicos y tecnológicos que permitan gestionar los riesgos, fortalecer la protección de los activos de información, mejorar la capacidad de respuesta ante incidentes y garantizar la confidencialidad, integridad y disponibilidad de la información en todas las empresas que conforman el grupo empresarial.

2.1. DESCRIPCIÓN DE LA EMPRESA A INTERVENIR

2.1.1. Misión

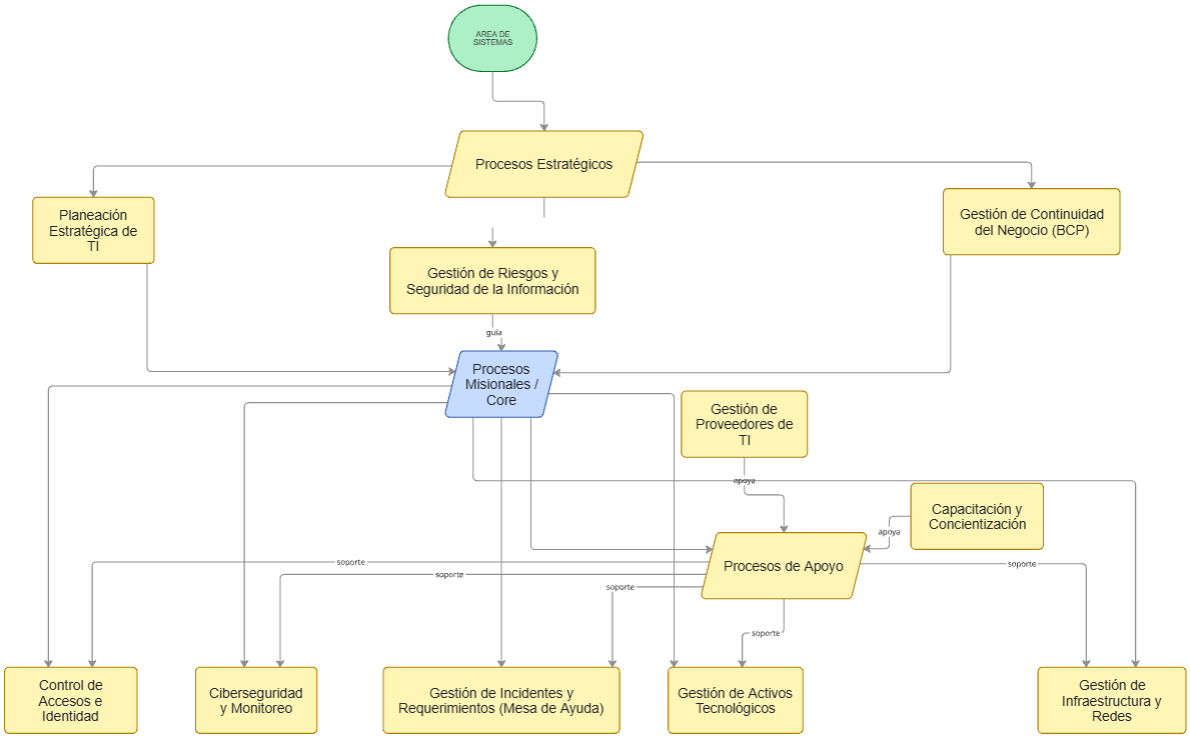
Impulsar el crecimiento de las personas mediante oportunidades de aprendizaje, capacitación y acompañamiento profesional en las áreas de tecnología y ciberseguridad. Nuestro propósito es fortalecer sus habilidades para que puedan enfrentar los desafíos del entorno digital, acceder a mejores oportunidades laborales y contribuir a la construcción de organizaciones y comunidades más seguras, preparadas e innovadoras.

2.1.2. Visión

Para 2030 la Empresa Security S.A.S, se visiona como una organización líder en ciberseguridad inteligente, con la incorporación de la Inteligencia artificial y la inteligencia de amenazas, podrá anticipar, detectar y mitigar amenazas y fraudes digitales mediante el uso ético, responsable e innovador de intelligent systems, fortaleciendo la confianza, la resiliencia y la protección de los entornos digitales.

2.1.3. Mapa de procesos

Figura 1 *Mapa de procesos empresa área de sistemas*



Nota. Elaboración propia.

Descripción de mapa de procesos

Procesos Estratégicos

Planeación Estratégica de TI: Proceso mediante el cual se alinean los objetivos tecnológicos con las metas estratégicas de la organización, asegurando que las iniciativas de tecnologías de la información apoyen el cumplimiento de los objetivos del negocio, optimicen el uso de los recursos y aporten valor a la empresa.

Gestión de Riesgos y Seguridad de la Información: Proceso encargado de identificar, analizar y gestionar los riesgos asociados a los activos de tecnología de la información, con el propósito de establecer controles y medidas de protección que permitan fortalecer la confidencialidad, integridad y disponibilidad de la información, de acuerdo con los lineamientos establecidos en la norma ISO/IEC 27001.

Gestión de Continuidad del Negocio: Proceso encargado de establecer estrategias, procedimientos y controles que permitan garantizar la operación continua de la organización ante incidentes, fallas críticas o situaciones disruptivas. Incluye la gestión de copias de seguridad (*backups*), la elaboración de planes de recuperación ante desastres y la implementación de mecanismos que faciliten la restauración de los servicios y la información en el menor tiempo posible.

Procesos Misionales

Gestión de Infraestructura y Redes: Proceso encargado de la administración, configuración, monitoreo y mantenimiento de los componentes tecnológicos de una organización, incluyendo servidores, equipos activos de red, redes LAN/WAN, conexiones VPN, servicios de telecomunicaciones y bases de datos. Su objetivo es garantizar la disponibilidad, rendimiento, seguridad y funcionamiento adecuado de la infraestructura tecnológica que soporta los sistemas de información de la empresa.

Gestión de Incidentes y Requerimientos (Mesa de Ayuda): Área encargada de brindar soporte técnico a los usuarios mediante canales de atención telefónicos, presenciales y virtuales. Gestiona las solicitudes e incidentes a través de un sistema de tickets (*software de gestión de tickets*), donde se registran, clasifican, categorizan, priorizan y dan seguimiento a los casos reportados, con el fin de resolver fallas operativas relacionadas con hardware, software y servicios tecnológicos. Su objetivo es garantizar una atención eficiente, mejorar la experiencia del usuario y mantener la continuidad de los servicios de TI.

Gestión de Activos Tecnológicos: Es el área encargada de llevar el control del inventario actual de los activos informáticos y documentar detalladamente aspectos como el ciclo de vida, las actualizaciones, los costos y las características del hardware y software. Este proceso inicia

desde la adquisición del activo, continúa con su asignación a un usuario y finaliza con su respectiva baja, manteniendo registrada toda la hoja de vida del equipo.

Ciberseguridad y Monitoreo: Su función es detectar vulnerabilidades mediante el uso de software especializado, realizando actividades de monitoreo continuo y análisis de correlación de eventos de seguridad a través de un sistema SIEM (sistema de información y eventos de seguridad). Además, permite gestionar la respuesta ante incidentes de seguridad dentro de la red corporativa, con el propósito de identificar, analizar y mitigar posibles amenazas que puedan afectar los activos de información de la organización.

Control de Accesos e Identidad: Es el área encargada de la administración y gestión de identidades mediante un gestor de directorio activo, permitiendo controlar los usuarios, credenciales de acceso, cuentas de correo electrónico y permisos asociados a los recursos tecnológicos de la organización. Asimismo, se encarga de la sincronización con sistemas de control de acceso físico, como relojes de control de asistencia y plataformas biométricas, con el fin de garantizar una adecuada gestión del acceso del personal y fortalecer la seguridad de los recursos de la empresa.

Gestión de Proveedores de TI: Es el área encargada de administrar y controlar la información relacionada con los proveedores tecnológicos de la organización, incluyendo contratos de licenciamiento de software, acuerdos de servicio, datos de contacto y documentación asociada. Asimismo, gestiona la relación con proveedores de servicios de internet, soporte de aplicaciones, mantenimiento de equipos tecnológicos y demás servicios externos necesarios para garantizar la operación eficiente de la infraestructura tecnológica.

Capacitación y Concientización: Es el área encargada de capacitar y orientar a los usuarios finales en el uso adecuado de las herramientas ofimáticas, los sistemas de gestión de tickets y las plataformas tecnológicas utilizadas por la organización. Asimismo, promueve las buenas prácticas de seguridad informática, fortaleciendo la cultura de seguridad y concientizando al personal sobre la importancia de proteger los activos de información de la empresa.

Para nuestro proceso actual, el proceso inicia con una planeación estratégica con la gestión comercial, donde se realiza la prospección de clientes, el diagnóstico inicial y la formalización

contractual. Posteriormente, se desarrolla el análisis y valoración de riesgos, que sirve como base para el diseño de políticas, procedimientos y controles del SGSI. Paralelamente, se adecuan las herramientas tecnológicas y se capacita al personal para garantizar la correcta implementación del sistema. Una vez implementado, se ejecutan auditorías internas y actividades de seguimiento para verificar la eficacia de los controles establecidos. Finalmente, se coordina la auditoría externa con el organismo certificador, se obtiene la certificación correspondiente y se realiza la entrega de resultados y el cierre formal del proyecto, promoviendo la mejora continua del sistema.

2.1.4. Descripción del proceso a intervenir

Vamos a intervenir el proceso de sistemas en el área de Gestión de Riesgos y Seguridad de la Información, debido a las falencias identificadas durante la implementación de la certificación ISO 27001 en la compañía. Por esta razón, el proyecto se fundamentará en la gestión de la seguridad de la información, tomando como referencia la actualización de las políticas y procesos actuales establecidos por la organización.

Posteriormente, se realizará la implementación y evaluación de las políticas vigentes relacionadas con la seguridad de los datos, con el fin de actualizar los procedimientos existentes y modificar las políticas actuales cuando sea necesario. De esta manera, se busca alinear a la empresa con los requisitos establecidos por la norma ISO/IEC 27001.

2.1.5. Descripción del problema que presenta el proceso

El problema identificado es que actualmente nuestro cliente ha intentado certificarse de manera constante bajo la norma ISO 27001; sin embargo, ha implementado diversas políticas de seguridad sin contar con una evaluación adecuada que permita determinar su efectividad, debido a que estas han sido desarrolladas por personal que no cuenta con la calificación necesaria para este tipo de actividades. Además, no se ha realizado un énfasis suficiente en la definición, documentación y fortalecimiento de los procesos internos basados en dichas políticas.

Por esta razón, la organización presenta algunas brechas de seguridad y oportunidades de mejora en la gestión de la seguridad de la información. En consecuencia, con el objetivo de fortalecer su gestión e incrementar la confianza con sus clientes, busca adoptar mejores prácticas de seguridad alineadas con los estándares internacionales, así como avanzar en el proceso de obtención de la certificación ISO 27001.

La implementación de esta norma permitirá establecer controles y protocolos más robustos para la protección de la información, optimizar los procesos internos, gestionar adecuadamente los riesgos asociados a la seguridad de la información y demostrar el compromiso de la organización con la confidencialidad, integridad y disponibilidad de sus activos de información.

Adicionalmente, la certificación contribuirá a mejorar la credibilidad de la empresa frente a sus clientes, socios y demás partes interesadas, fortaleciendo su posición competitiva en el mercado y garantizando una mejora continua en los servicios ofrecidos.

Por lo anterior, se busca fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI), mejorar los controles y procedimientos existentes, aumentar la confianza de los clientes y asegurar la adopción de buenas prácticas alineadas con estándares internacionales.

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

En base en el diagnóstico realizado de la situación que se presenta y se busca a dar solución según lo siguiente:

Se busca realizar un examen inicial de seguridad de la información con el fin de poder dar a conocer y dar un dictamen actual de la seguridad de la información actual con la que se encuentra la empresa.

se plantea el siguiente plan de acción con el propósito de corregir las debilidades encontradas en la empresa y mejorar la protección de la información.

Las actividades propuestas buscan disminuir los riesgos de seguridad y servir como base para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001.

TABLA1. Matriz de riesgos

Objetivo Especifico	Actividad Propuesta	Meta	Indicador	Medio de Verificación	Responsable	Tiempo
Identificar el estado actual de la seguridad de la información.	Revisar los procesos, entrevistar a los responsables de cada área e identificar las principales debilidades relacionadas con la seguridad de la información.	Contar con un diagnóstico completo de la organización.	Diagnóstico elaborado y aprobado.	Informe de diagnóstico.	Alta dirección y área de TI.	1 mes.

Definir normas para el manejo seguro de la información.	Elaborar las políticas, procedimientos y lineamientos de seguridad, socializarlos con los colaboradores y dejar evidencia de su aprobación.	Disponer de políticas de seguridad implementadas en toda la organización.	Porcentaje de políticas aprobadas y divulgadas.	Manual de políticas, actas y registros de socialización.	Comité de Seguridad de la Información.	2 meses.
Organizar y proteger los activos de información	Identificar los activos de información, clasificarlos según su importancia y asignar controles para su protección.	Tener todos los activos inventariados y clasificados	Porcentaje de activos clasificados.	Inventario de activos y matriz de clasificación.	Área de TI y líderes de proceso	2 meses.
Mejorar el control de acceso a la información.	Revisar los permisos de los usuarios, eliminar accesos innecesarios, fortalecer las contraseñas y aplicar el principio de mínimo privilegio.	Garantizar que cada usuario acceda únicamente a la información que necesita para realizar su trabajo.	Número de accesos revisados y actualizados.	Registro de usuarios y permisos.	Área de TI.	2 meses.

Implementar un proceso para gestionar los riesgos.	Identificar las amenazas, evaluar los riesgos y definir acciones para reducir su impacto.	Contar con una matriz de riesgos y un plan de tratamiento.	Riesgos identificados y tratados.	Matriz de riesgos y plan de tratamiento.	Comité de Seguridad.	2 meses.
Fortalecer el monitoreo de la infraestructura tecnológica.	Configurar registros de eventos, monitorear los sistemas y generar alertas cuando se detecten actividades inusuales.	Mejorar la capacidad de detectar incidentes de seguridad.	Porcentaje de equipos y servidores monitoreados	Registros de eventos e informes de monitoreo.	Área de TI.	3 meses.
Promover una cultura de seguridad entre los colaboradores.	Realizar capacitaciones, campañas de sensibilización y actividades sobre buenas prácticas en seguridad de la información.	Capacitar a la mayor parte del personal.	Porcentaje de colaboradores capacitados.	Listas de asistencia y evaluaciones.	Talento Humano y responsable del SGSI.	Actividad permanente.
Evaluar el funcionamiento de los controles implementados.	Programar auditorías internas para verificar el cumplimiento de las políticas y detectar oportunidades de mejora.	Ejecutar auditorías de forma periódica.	Número de auditorías realizadas.	Informes de auditoría y planes de mejora.	Auditor interno.	Cada 6 meses.

Establecer un proceso para atender incidentes de seguridad.	Crear un procedimiento que indique cómo reportar, analizar y responder a los incidentes de seguridad.	Reducir el tiempo de respuesta frente a incidentes.	Tiempo promedio de atención de incidentes.	Registro de incidentes y reportes de seguimiento.	Área de TI y Comité de Seguridad.	2 meses.
Implementar y mantener el SGSI.	Integrar todas las actividades anteriores, realizar seguimiento a los indicadores y aplicar acciones de mejora continua.	Contar con un SGSI funcionando de acuerdo con la norma ISO/IEC 27001.	Nivel de cumplimiento del plan de implementación.	Informes de seguimiento, indicadores y actas del comité.	Alta Dirección y Comité de Seguridad.	12 meses.

Nota. Elaboración propia.

3.1. ESTABLECIMIENTO DE OBJETIVOS

- *Identificar las principales debilidades que presenta la empresa en la gestión de la seguridad de la información, con el fin de conocer la situación actual de la organización.*
- *Diseñar una propuesta de Sistema de Gestión de Seguridad de la Información (SGSI), tomando como guía la norma ISO/IEC 27001.*
- *Elaborar un plan de implementación del SGSI que establezca las actividades, los responsables, los recursos y los tiempos necesarios para fortalecer la seguridad de la información.*

3.2. DESCRIPCIÓN DE LA SOLUCIÓN

Actualmente, la empresa necesita corregir las debilidades encontradas, por lo cual nos basamos en la norma internacional ISO 27001, ya que esta representa una forma estandarizada y efectiva de hacerlo mediante el ciclo de mejora continua (Planificar, Hacer, Verificar y Actuar).

Planificar: Se busca planificar y definir el terreno. Para ello, se va a identificar la cantidad de activos que existen en la empresa; posteriormente, se procederá a verificar cada uno de los equipos y cuáles pueden ser sus posibles vulnerabilidades. Para ello, se evaluará el estado actual de las normas y procesos de seguridad existentes, de acuerdo con los requisitos de la norma ISO 27001. Esto permitirá verificar el estado actual de la empresa y generar un diagnóstico de los aspectos que hacen falta por construir, permitiendo determinar qué elementos se van a intervenir y cuáles están dentro del SGSI que se va a implementar.

Hacer: En esta etapa se identifican cada una de las variables, se observan los procesos y se busca concientizar sobre qué puede salir mal y cómo evitarlo. Para ello, se realiza un proceso de gestión de riesgos; asimismo, se va a asignar un valor actual a cada uno de los riesgos que componen los activos de la organización, determinando cuánto pueden afectar a la empresa. Para esto, se utiliza una matriz de riesgos en la cual son valorizados, por lo que es fundamental estructurar en detalle cómo se van a identificar y evaluar, para posteriormente tomar decisiones sobre cómo mitigar y tratar dichos riesgos.

Esto se realiza bajo la Declaración de Aplicabilidad (SoA), la cual es un documento que justifica cuáles de los controles de seguridad del Anexo A de la norma ISO 27001 serán implementados.

Implementar (Despliegue de Controles): Con base en el Anexo A de la norma ISO 27001, se procede a implementar políticas y controles de seguridad. En esta etapa se busca abarcar un plan de tratamiento de riesgos en el cual se vean involucrados aspectos de tecnología, hardware o software (donde se desplegarán soluciones tecnológicas para proteger la red). Es vital integrar plataformas de monitoreo continuo y detección de vulnerabilidades.

Asimismo, se trabajará con las personas mediante capacitaciones, donde se guiará al personal sobre cómo protegerse al navegar en la red, qué tipos de riesgos existen y cómo generar conciencia con base en las políticas que serán implementadas. Finalmente, se abordarán los

procesos actuales de la empresa, los cuales serán ajustados mediante políticas de seguridad de la información.

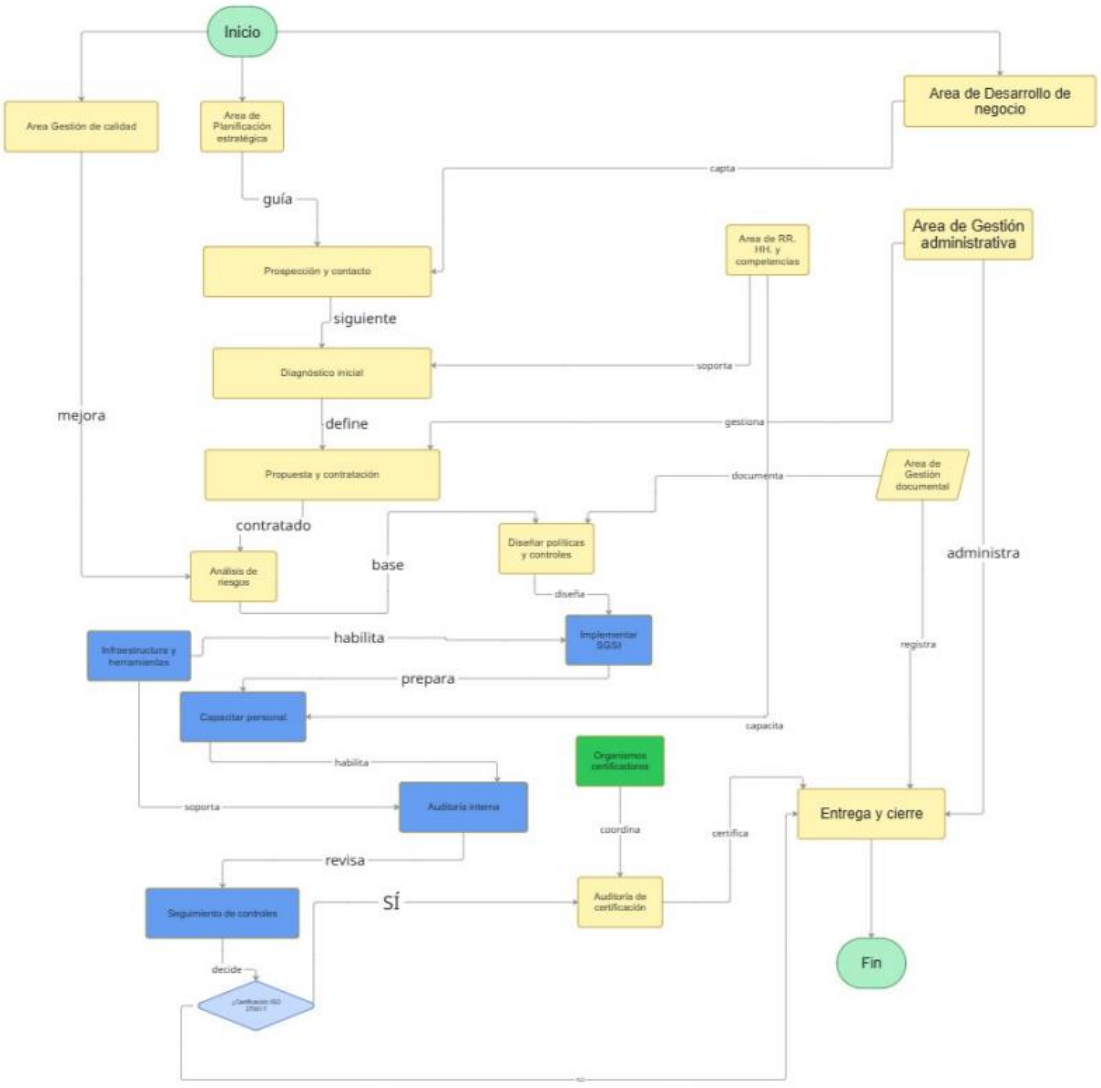
Verificar y Actuar (Monitoreo y Mejora):

Buscando una mejora continua en el SGSI, se pretende mantener un proceso constante de evaluación y optimización. Por ello, se debe implementar una auditoría interna en la empresa, con el fin de identificar futuras falencias o vulnerabilidades que puedan surgir, realizando una retroalimentación y corrección de los hallazgos encontrados, ya que se busca mejorar la protección de la información.

Las actividades propuestas buscan disminuir los riesgos de seguridad y servir como base para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO/IEC 27001. Posteriormente, los resultados obtenidos en las auditorías serán entregados al área de gerencia, donde se tomarán decisiones respecto a los posibles riesgos encontrados, con el fin de evaluar las acciones de mejora correspondientes.

3.3. SECUENCIA DE ACTIVIDADES PARA EJECUCIÓN DE LA SOLUCIÓN

Figura 2. Actividades Para Ejecución De La Solución



Nota. Elaboración propia.

Para dar inicio al proyecto de implementación en la empresa de nuestro cliente, relacionado con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), nos proponemos asignar responsables y objetivos clave frente a la ejecución del proyecto.

Área de Gestión de Calidad:

El área de gestión de calidad nos va a servir para realizar la integración entre los sistemas de gestión que actualmente maneja la empresa y el Sistema de Gestión de Seguridad de la Información.

Área de Planificación Estratégica:

Esta área es fundamental para el proyecto, ya que nos permite definir el direccionamiento estratégico, estableciendo objetivos, alcances, recursos y una planeación por fechas en la que se estima el tiempo de ejecución del proyecto. Además, permite identificar y priorizar tareas, gestionándolas como actividades a realizar por el grupo encargado. Esto tiene como finalidad administrar mejor el tiempo de desarrollo del proyecto y crear un periodo de amortiguación para los imprevistos que puedan surgir.

Prospección y contacto:

Es el área encargada de establecer contacto con nuestro cliente e identificar oportunidades comerciales, con el fin de determinar las necesidades actuales que tiene la organización en temas de seguridad de la información.

Para iniciar el proyecto, se procede a realizar, por parte de nuestro grupo de ingeniería, un diagnóstico inicial, evaluando el estado actual en el que se encuentra la organización frente a los requisitos establecidos.

Con nuestro grupo de ingeniería buscamos identificar y valorar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información.

Diseño de políticas y controles:

Una vez analizados e identificados cada uno de los riesgos, se les asigna un valor porcentual para poder clasificarlos y presentarlos ante la junta directiva. Esto con el fin de realizar una valoración en caso de asumir el riesgo o determinar las acciones necesarias para disminuirlo frente a las vulnerabilidades actuales.

Asimismo, según el riesgo identificado, se procede a definir políticas, procedimientos y controles de seguridad, basándonos en los controles establecidos conforme a los riesgos identificados y al Anexo A de la norma ISO 27001.

Implementación del SGSI:

Es el despliegue de la propuesta realizada para nuestro cliente, en donde se inicia la implementación y operación de los controles, procedimientos y actividades necesarias para gestionar adecuadamente la seguridad de la información exigida por la norma ISO 27001.

Esto tiene como finalidad evitar reprocesos, identificar posibles vulnerabilidades y brechas de seguridad, y generar mejores oportunidades de mejora. Una vez obtenidos los datos iniciales, se procede a realizar una propuesta económica frente al proyecto para la implementación del SGSI y la formalización de los compromisos contractuales.

Análisis de riesgos, infraestructura y herramientas:

Es la etapa donde se verifican las aplicaciones y mecanismos de seguridad existentes, se evalúan y se realizan las correcciones necesarias. Mediante aplicativos y políticas de seguridad se busca generar mejoras y realizar seguimiento a los lineamientos establecidos en el Anexo A de la norma ISO 27001.

Esto permitirá verificar cada uno de los controles a implementar, determinar su efectividad y realizar monitoreo mediante pruebas, con el fin de validar si estos controles funcionan correctamente y soportan el funcionamiento del SGSI.

Capacitar al personal:

Según las políticas de la norma ISO 27001, los controles y políticas que serán implementados deben estar acompañados de capacitaciones al personal, con el objetivo de explicar qué actividades pueden realizar en la red, qué riesgos pueden presentarse y qué aspectos pueden mejorarse para evitar incidentes de seguridad.

Para ello, se desarrollarán competencias, actividades de concientización y entrenamientos al personal sobre los requisitos y responsabilidades relacionados con el SGSI.

Auditoría interna:

Evaluación independiente del SGSI para verificar el cumplimiento de los requisitos establecidos y detectar no conformidades u oportunidades de mejora.

Seguimiento de controles:

El monitoreo y la evaluación continua permiten verificar los controles implementados, con el fin de asegurar el cumplimiento de los objetivos de seguridad y generar retroalimentación sobre el trabajo realizado.

Controles constantes:

Punto de decisión donde se determina si los controles implementados cumplen con los resultados esperados y gestionan adecuadamente los riesgos identificados.

Área de RR. HH. y Competencias:

Garantiza la asignación de roles, responsabilidades y competencias necesarias para mantener la eficacia del SGSI.

Área de Gestión Administrativa:

Gestiona los recursos financieros, físicos y administrativos requeridos para la implementación y sostenibilidad del sistema.

Área de Gestión Documental:

Área encargada de llevar la gestión documental, las bitácoras y los controles de revisión y aprobación, además de resguardar el almacenamiento y conservación de la información documentada del SGSI.

Organismos certificadores:

Son las entidades acreditadas legalmente encargadas de evaluar la conformidad del proyecto del SGSI frente a los requisitos establecidos en la norma ISO/IEC 27001.

Auditoría de certificación:

Proceso formal de auditoría externa mediante el cual se verifica la conformidad y eficacia del SGSI para la obtención de la certificación.

Entrega y cierre:

Es la entrega del SGSI y la formalización de los resultados obtenidos, incluyendo la documentación generada, conclusiones, lecciones aprendidas, cierre administrativo y técnico

del proyecto. Finalizando con la culminación del proceso, la certificación obtenida y la finalización de las actividades definidas dentro del alcance del proyecto.

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

Para llevar a cabo la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), la organización deberá contar con recursos humanos, tecnológicos, financieros y organizacionales.

En relación con los recursos humanos, será necesaria la participación de la alta dirección, el área de tecnologías de la información, los líderes de proceso y los demás colaboradores, quienes apoyarán las actividades de diagnóstico, implementación y seguimiento.

Los recursos tecnológicos incluyen equipos de cómputo, servidores, software para la gestión de la seguridad, herramientas de monitoreo, sistemas de respaldo y equipos de red necesarios para proteger la información.

Respecto a los recursos financieros, se deberá disponer de un presupuesto para la adquisición de herramientas tecnológicas, capacitación del personal, posibles asesorías especializadas y demás gastos relacionados con la implementación del SGSI.

Finalmente, serán necesarios recursos organizacionales, como el tiempo para desarrollar las actividades, espacios para reuniones y capacitaciones, así como el compromiso de la dirección para apoyar la ejecución del proyecto y promover la mejora continua en la seguridad de la información.

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

El alcance de la solución propuesta es implementar la certificación de la norma ISO 27001 para la mejora de la seguridad informática de la empresa Security S.A.S., verificando posibles vulnerabilidades de acuerdo con los estándares y controles indicados en el Anexo A de la norma ISO 27001.

La intervención estará enfocada principalmente en el proceso de gestión de riesgos y seguridad de la información, incluyendo los procedimientos, las políticas, los recursos humanos y los controles tecnológicos.

4.1. ALCANCE FINAL DE LA SOLUCIÓN

El alcance final de la solución está enfocado en la obtención del certificado del SGSI. En este se comprende todo el diseño, implementación y seguimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), buscando estar alineado con los requisitos de la norma ISO/IEC 27001 y, como resultado, poder implementar nuevos protocolos de seguridad.

La solución estará orientada a realizar un diagnóstico inicial y, con base en los resultados obtenidos, dar a conocer la situación actual de seguridad en la que se encuentra la empresa. A partir de este análisis, se realizarán las correcciones necesarias y se establecerán los protocolos de seguridad, así como las modificaciones requeridas para alinearlos con la norma.

Dentro de la solución se busca realizar la identificación actual de los activos de información y su posterior clasificación, implementar controles de acceso a la información, mejorar la gestión de controles de seguridad y fortalecer los mecanismos de monitoreo. Adicionalmente, se busca educar y capacitar a los usuarios con el propósito de dar a conocer los riesgos latentes a los que pueden estar expuestos al administrar información.

Como parte del proceso de mejora continua, se busca ejecutar auditorías internas y establecer procedimientos para la gestión de incidentes de seguridad.

4.2. IDENTIFICACIÓN DE RESPONSABLES DE LAS ACTIVIDADES PARA EJECUCIÓN

Tabla 3. tabla de identificación de responsabilidades.

PROCESO	Responsable	Apoyo a grupo
Diagnóstico inicial de seguridad	Comité de Seguridad de la Información	Alta Dirección y Área TI
Elaboración de políticas y procedimientos	Comité de Seguridad	Gestión de Calidad
Inventario y clasificación de activos	Área TI	Líderes de proceso y Área TI
Gestión de riesgos	Comité de Seguridad	Alta Dirección y Área TI
Implementación de controles de acceso	Área TI	Recursos Humanos
Implementación de herramientas de monitoreo	Área TI	Proveedores tecnológicos
Capacitación y sensibilización	Recursos Humanos	Responsable SGSI
Auditorías internas	Auditor Interno	Comité de Seguridad
Gestión de incidentes de seguridad	Área TI	Comité de Seguridad, Área TI
Seguimiento y mejora continua	Alta Dirección	Comité de Seguridad, auditoría interna

Nota. Elaboración propia.

La asignación de las actividades y procesos para cada una de las áreas involucradas es fundamental para poder dar mejora y sostenibilidad al proyecto. Por lo tanto, es importante su cumplimiento y apoyo para gestionar el proyecto de manera correcta.

4.3. CRONOGRAMA DE EJECUCIÓN

Tabla 4. Cronograma de actividades.

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7 al 12
Diagnóstico Inicial.	X						
Elaboración de Políticas	X	X					
Inventario y Clasificación de activos.		X	X				
Control de Accesos.		X	X				
Gestión de Riesgos.		X	X				
Implementación de Monitoreo.			X	X			
Capacitación al Personal.			X	X	X	X	X
Auditorías Internas.					X	X	X
Gestión de Incidentes.			X	X			
Seguimiento y mejora continua.						X	X

Nota. Elaboración propia.

4.4. PRESUPUESTO

Actividad	Recurso Requerido	Cantidad	Valor Unitario	Valor Total
Diagnóstico inicial	Horas de análisis y recopilación de la información	20 horas	$35.000	$700.000
Elaboración de políticas	Diseño y documentación de políticas de seguridad	30 horas	$40.000	$1.200.000
Inventario y clasificación de activos	Papelería, formatos y herramientas de oficina	1 paquete	$350.000	$350.000
Control de accesos	Configuración y revisión de permisos	25 horas	$40.000	$1.000.000
Gestión de riesgos	Identificación, análisis y valoración de riesgos	30 horas	$40.000	$1.200.000
Implementación de monitoreo	Herramientas de monitoreo y configuración	1 implementación	$1.500.000	$1.500.000
Capacitación al personal	Material de apoyo y dos jornadas de capacitación	2 jornadas	$400.000	$800.000

Auditorías internas	Revisión de controles y elaboración de informe	20 horas	$40.000	$800.000
Gestión de incidentes	Elaboración de procedimientos y simulación	15 horas	$40.000	$600.000
Seguimiento y mejora continua	Evaluación de indicadores y actualización documental	20 horas	$35.000	$700.000

Tabla 6. Resumen

Concepto	**Valor**
Recursos humanos	$7.000.000
Materiales y herramientas	$1.850.000
Total, estimado del proyecto	$8.850.000

5. REFERENCIAS BIBLIOGRÁFICAS

- R, A. (2021). Implementación de la seguridad de la información basada en ISO 27001/ISO 27002 (8.ª ed.). IT Governance Publishing.

- Hernández-Sampieri, R., & Mendoza, C. P. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. McGraw-Hill.

- International Organization for Standardization. (2018). ISO 31000:2018 Gestión del riesgo: Directrices. ISO.

- International Organization for Standardization. (2022). ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de seguridad de la información – Requisitos. ISO.

- Stallings, W., & Brown, L. (2018). Seguridad informática: Principios y prácticas (4.ª ed.). Pearson.

- Whitman, M. E., & Mattord, H. J. (2021). Principios de seguridad de la información (7.ª ed.). Cengage Learning.

- Ministerio de Tecnologías de la Información y las Comunicaciones. (2026, 6 de mayo). Modelo de Seguridad y Privacidad de la Información (MSPI). Gobierno Digital. https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/