

Propuesta de Fortalecimiento de Ciberseguridad y Gestión de Riesgos de TI para la Empresa Novatech Logistics S.A.S.

Trabajo final presentado por:	Oscar Paul Martinez Camelo Sebastian Tabarquino Noreña Jonny Alejandro Padilla Salinas
Programa:	Especialización en Ciberseguridad
Docente:	Fabricio Echeverría Briones
Fecha:	26-08-2026

Índice de contenidos

Resumen	4
Abstract	4
1. Introducción	6
1.1. Objetivo General	6
1.2. Objetivos Específicos	6
1.3. Metodología	6
1.3.1. Identificación y Análisis del Problema	7
1.3.2. Planificación de la Solución	7
2. Identificación y descripción un problema al interior de la organización	9
2.1. Descripción de la empresa a intervenir	9
2.1.1. Misión	9
2.1.2. Visión	10
2.1.3. Mapa de procesos	10
2.1.4. Descripción del proceso a intervenir	11
2.1.5. Descripción del problema que presenta el proceso	12
3. Establecimiento de planes de acción para la solución del problema	13
3.1. Establecimiento de objetivos	13
3.2. Descripción de la solución	14
3.3. Secuencia de actividades para ejecución de la solución	14
3.4. Descripción de recursos necesarios para la ejecución de la solución	15
4. Definición del alcance de la solución, partes interesadas, cronograma y presupuestos.	16
4.1. Alcance final de la solución	16
4.2. Identificación de responsables de las actividades para ejecución	17
4.3. Cronograma de ejecución	17

4.4.	Presupuesto	18
5.	Referencias bibliográficas	20

RESUMEN

El presente proyecto propone el fortalecimiento de la ciberseguridad y la gestión de riesgos de TI en la empresa ficticia Novatech Logistics S.A.S., a partir de la identificación de vulnerabilidades tecnológicas, físicas y operacionales que afectan la seguridad de la información. El problema principal se relaciona con la ausencia de un Sistema de Gestión de Seguridad de la información (SGSI) formal, situación que ha generado debilidades de la gestión de accesos, protección de activos, infraestructura física, tratamiento de datos personales y monitoreo de eventos de seguridad. Para abordar esta situación se empleó una metodología de investigación-acción, complementada con un análisis de brechas frente a los controles del Anexo A de ISO/IEC 27001:2022. Como resultado del análisis se priorizaron 34 controles de seguridad, distribuidos en controles organizacionales, de personas, físicos y tecnológicos. La propuesta contempla su implementación progresiva durante nueve meses, incluyendo políticas de seguridad, gestión de identidades y accesos, MFA, segmentación de redes, NGFW, EDR, copias de seguridad, monitoreo de eventos, adecuaciones físicas y actividades de concientización. Con la ejecución de la propuesta se espera reducir la exposición a riesgos, fortalecer la protección de los activos de información y establecer una base para la mejora continua de la seguridad de la información en Novatech Logistics S.A.S.

Palabras clave: Ciberseguridad, SGSI, ISO/IEC 27001:2022, gestión de riesgos, seguridad de la información, controles de seguridad

ABSTRACT

This project proposes strengthening cybersecurity and IT risk management at the fictitious company Novatech Logistics S.A.S. by identifying the technological, physical, and operational vulnerabilities that affect information security. The primary issue stems from the absence of a formal Information Security Management System (ISMS), a situation that has led to weaknesses in access management, asset protection, physical infrastructure, personal data handling, and security event monitoring. To address this, an action-research methodology was employed, complemented by a gap analysis against the controls listed in Annex A of ISO/IEC 27001:2022. The analysis resulted in the prioritization of 34 security controls, categorized into organizational, people-related, physical, and technological controls. The proposal outlines a phased nine-month implementation plan covering security policies,

identity and access management, MFA, network segmentation, NGFW, EDR, backups, event monitoring, physical facility upgrades, and awareness-raising activities. Implementing this proposal is expected to reduce risk exposure, strengthen the protection of information assets, and establish a foundation for the continuous improvement of information security at Novatech Logistics S.A.S.

Keywords: Cybersecurity, ISMS, ISO/IEC 27001:2022, risk management, information security, security controls

1. INTRODUCCIÓN

Este proyecto de aplicación en investigación-acción se centró en la identificación y resolución de la seguridad de la información en el departamento de tecnología de la información y operaciones de Novatech Logistics S.A.S., proponiendo una solución estructurada bajo el estándar ISO/IEC 27001:2022, permitiendo integrar teoría y práctica en un entorno ficticio. 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 optimice su desempeño.

1.1.OBJETIVO GENERAL

El objetivo principal del proyecto fue desarrollar una solución operativa al problema de postura de ciberseguridad corporativa, en la empresa Novatech Logistics S.A.S. Para esto hemos decidido diseñar un plan de solución integral basado en la norma ISO/IEC 27001:2022 para poder abordar los problemas tecnológicos de la organización. La intervención se orientó no sólo 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 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 afectan 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 método utilizado fue un análisis GAP o de brecha normativa entre el estado actual de la infraestructura informática de Novatech Logistics S.A.S y las recomendaciones del Anexo A de ISO/IEC 27001:2022. Para la recolección de los datos se realizaron entrevistas a personal clave, se verificaron políticas actuales del sistema de seguridad de la información, se

revisaron registros de auditoría como logs del sistema ERP y se verificaron los cuartos de los servidores y sus zonas de almacenamiento.

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 maximizará la eficiencia del proceso intervenido. La planificación detallada de actividades y recursos fue clave para asegurar una implementación precisa y efectiva.

Este proceso llevó a la identificación de 34 posibles controles de implementación progresiva para suplir el problema evidenciado en Novatech Logistics S.A.S., teniendo en cuenta las limitaciones organizacionales y controles críticos y prioritarios para mitigar los riesgos y falencias evidenciadas en el sistema.

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

La organización Novatech Logistics S.A.S., presenta un problema estructural derivado de no contar con un Sistema de Gestión de Seguridad de la Información. Esta ausencia ha generado fallas que afectan de manera transversal a toda la compañía, evidenciando debilidades que comprometen la protección, disponibilidad y confiabilidad de la información. Entre las principales falencias se encuentra la inexistencia de un inventario de activos, lo que dificulta la identificación de recursos críticos y la asignación de controles adecuados. Asimismo, la organización carece de políticas de seguridad claras, actualizadas y aplicadas, situación que incrementa la exposición a amenazas y riesgos que pudieron haberse mitigado si la seguridad de la información se hubiera abordado de manera integral desde el inicio.

La falta de lineamientos, controles y procedimientos alineados con estándares internacionales ha generado un entorno vulnerable, donde los riesgos asociados a la infraestructura tecnológica, el control de accesos y la gestión documental no se encuentran adecuadamente gestionados. Sin embargo, esta situación permitió al equipo realizar una evaluación completa y plantear una solución integral basada en los lineamientos de la norma ISO/IEC 27001, incorporando el ciclo PHVA para establecer controles, fortalecer la postura de seguridad y mitigar los riesgos más relevantes. Este diagnóstico constituye el punto de partida para comprender el problema interno de la organización y orientar la implementación de medidas que garanticen la protección de la información y la continuidad operativa.

2.1. DESCRIPCIÓN DE LA EMPRESA A INTERVENIR

2.1.1. Misión

Ofrecer soluciones logísticas integrales, seguras e innovadoras que optimicen la cadena de suministro de nuestros clientes, garantizando la trazabilidad, eficiencia y puntualidad en la entrega de mercancías a través de tecnología de vanguardia y un equipo humano altamente capacitado.

2.1.2. Visión

Para el año 2030, posicionarnos como el operador logístico líder en la región, reconocido por la transformación digital, la resiliencia operativa y el cumplimiento de altos estándares internacionales y la protección de datos corporativos.

2.1.3. Mapa de procesos

La estructura procesal de Novatech Logistics S.A.S., se organiza en tres niveles fundamentales:

Procesos Estratégicos: Dirección general, gestión de la calidad, gestión de riesgos y cumplimiento.

Procesos Misionales / Operativos: Recepción de mercancía, gestión de inventario y almacenamiento, despacho y transporte, servicio al cliente.

Procesos de apoyo: Gestión de tecnología de la información (TI), recursos humanos, compras y proveedores, gestión financiera y mantenimiento físico.

Figura 1 Mapa de procesos de Novatech Logistics S.A.S.



2.1.4. Descripción del proceso a intervenir

El proceso objeto de intervención es la **Gestión de Tecnología de la Información (TI)**. Este proceso es de carácter transversal y se encarga de administrar, asegurar y mantener la infraestructura tecnológica de Novatech Logistics S.A.S., garantizando la disponibilidad, confidencialidad e integridad de las plataformas operativas (ERP, bases de datos de clientes, redes locales e inalámbricas en bodegas).

Dada su naturaleza crítica, cualquier falla en la seguridad de este proceso afecta directamente la operación misional: caídas del sistema ERP paralizan el despacho de mercancía, la manipulación no autorizada de datos afecta el inventario y una fuga de información vulnera la privacidad de los datos personales (protegidos por la Ley 1581 de 2012). Por ello, el proceso se interviene mediante la alineación con los controles de la norma ISO/IEC 27001:2022 (Organizacionales, de Personas, Físicos y Tecnológicos).

Tabla I

Componentes y elementos alineados a la estrategia de controles del SGSI

Componente	Descripción / Elementos alineados a la estrategia de controles
Entradas (inputs)	Requerimientos y políticas: Política General del SGSI (Control 5.1), Política de uso aceptable de credenciales/equipos (Control 5.10) y directrices de protección de datos personales - Ley 1581 (Control 5.34). Solicitudes operativas: Solicitudes de cuentas nominales únicas y asignación de accesos basados en roles - RBAC (Controles 5.15, 5.16).

	Información de infraestructura: Inventario actualizado de activos críticos como servidores, ERP y base de datos (Control 5.9). Gestión de personas y terceros: Verificación de antecedentes (Control 6.1), NDA firmados (Control 6.6) y acuerdos de seguridad con transportadoras/contratistas (Control 5.19).
Actividades principales	Seguridad Física e Infraestructura: Control de acceso biométrico/tarjeta al centro de datos (Control 7.2), cierre del cuarto de servidores (Control 7.3), monitoreo con CCTV por 90 días (Control 7.4) y climatización de precisión (Control 7.5). Gestión de Redes y Tecnológica: Segmentación de red mediante VLANs para operación, cámaras e IoT (Control 8.22), implementación de Next-Generation Firewall - NGFW (Control 8.20) y <i>hardening</i> de servidores (Control 8.9). Gestión de Accesos e Identidades: Asignación de accesos privilegiados diferenciados (Control 8.2), autenticación MFA para accesos remotos (Control 8.5) y revisión/revocación periódica de accesos (Control 5.18). Protección Operativa y Datos: Despliegue de EDR en estaciones críticas (Control 8.7), escaneo periódico de vulnerabilidades/parches (Control 8.8), respaldo de base de datos con pruebas de restauración (Control 8.13) y cifrado de base de datos en reposo y tránsito (Control 8.24). Monitoreo, Incidentes y Personas: Centralización de <i>logs</i> en un SIEM básico (Controles 8.15, 8.16), ejecución del procedimiento de incidentes (Control 5.24), programa de concientización y simulación de <i>phishing</i> (Control 6.3), y desvinculación con revocación de accesos en <24 h (Control 6.5).

Salidas (outputs)	Infraestructura de red y centro de datos protegido, climatizado y monitoreado. Cuentas nominales y accesos RBAC/MFA configurados y auditados. Base de datos del ERP e inventarios cifrados y respaldados. Registros de eventos de seguridad (<i>logs</i>) y alertas monitoreadas vía SIEM/EDR. Informes de vulnerabilidades remediadas y evidencias de simulacros de <i>phishing</i>. Procedimientos formales de respuesta ante incidentes de seguridad ejecutados.
Clientes / destinatarios	Internos: Procesos misionales (Recepción de mercancía, Gestión de inventario/almacenamiento, Despacho/transporte y Servicio al cliente). Externos: Transportadoras, contratistas, proveedores y clientes cuyos datos personales están resguardados por la organización.

2.1.5. Descripción del problema que presenta el proceso

El problema es el alto nivel de vulnerabilidad tecnológica, física y operacional en el proceso de Gestión de Tecnología de la Información (TI), originado principalmente por la ausencia de un sistema de Gestión de Seguridad de la información (SGSI) formal que permita gestionar los riesgos y establecer controles de seguridad de manera estructurada. Esta situación ha generado incidentes de seguridad de la información, incongruencias en los registros de inventario, filtración de listas de precios y datos de clientes, así como un impacto negativo en la reputación y atención al cliente de Novatech Logistics S.A.S.

La ausencia de un SGSI ha ocasionado que diferentes aspectos relacionados con la seguridad sean gestionados de manera independiente y sin lineamientos claramente establecidos, generando debilidades en la gestión de accesos, protección de la infraestructura, administración de activos y protección de la información. De esta manera, las vulnerabilidades identificadas representan una consecuencia directa de la falta de una gestión integral y organizada de la seguridad de la información.

Tras la investigación interna realizada en el último año, se evidenció que la causa raíz del problema obedece a deficiencias críticas estructuradas en tres frentes:

Deficiencias organizacionales y de personal: Empleados compartiendo credenciales de acceso al ERP, excolaboradores con accesos activos meses después de su salida, y proveedores externos conectados a la red sin acuerdos de confidencialidad o revisión de seguridad.

Deficiencias físicas: el centro de datos (cuartos de servidores) permanece con la puerta abierta para ventilación improvisada, carece de control de acceso biométrico o por tarjeta, y no cuenta con registros de ingreso de personal no autorizado.

Deficiencias Tecnológicas: Falla de segmentación de red en bodegas, servidores con sistemas operativos obsoletos sin parches de seguridad actualizados y ausencia de autenticación multifactor (MFA) para conexiones remotas.

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

En esta sección se realiza el plan de acción propuesto para abordar las vulnerabilidades identificadas en el proceso de Gestión de Tecnología de la Información (TI) de Novatech Logistics S.A.S. Se definen los objetivos teniendo como base las causas raíz identificadas y los riesgos asociados a la seguridad de la información.

Se presenta la solución propuesta mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con la norma ISO/IEC 27001:2022 y sustentado en la aplicación de los 34 controles del Anexo A previamente seleccionados de acuerdo con las necesidades y el contexto de la organización.

Se establece una secuencia organizada de actividades para la ejecución del plan, contemplando los recursos humanos, materiales, tecnológicos y financieros necesarios, así como mecanismos de seguimiento y medición que permitan evaluar el cumplimiento de los objetivos y contribuir al fortalecimiento continuo de la seguridad de la información en Novatech Logistics S.A.S.

3.1. ESTABLECIMIENTO DE OBJETIVOS

-Implementar, en un plazo máximo de nueve meses, los 34 controles de seguridad de la información seleccionados como aplicables para Novatech Logistics S.A.S., de los 93 establecidos en el Anexo A de la norma ISO/IEC 27001:2022. Esta implementación se realizará conforme a las necesidades, los riesgos identificados y el contexto operativo de la organización, garantizando que los controles adoptados respondan de manera efectiva a las brechas actuales y fortalezcan la gestión integral de la seguridad de la información.

-Reducir en un alto índice con respecto a la situación actual los accesos no autorizados identificados y los eventos de fuga de información asociados al sistema de inventarios WMS/ERP, mediante la implementación de controles de gestión de identidades, control de acceso, autenticación segura, monitoreo y protección de la información.

-Garantizar una cobertura del 80% en las actividades de capacitación y concienciación en seguridad de la información dirigidas a los colaboradores de la organización, mediante un programa formal de formación y sensibilización.

3.2.DESCRIPCIÓN DE LA SOLUCIÓN

La solución consiste en el diseño y despliegue de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los requisitos de ISO/IEC 27001:2022. De acuerdo con el análisis del contexto, las necesidades de seguridad y los riesgos identificados en Novatech Logistics S.A.S., la solución prioriza la implementación de 34 de los 93 controles establecidos en el Anexo A de ISO/IEC 27001:2022, distribuidos en las categorías de controles organizacionales, de personas, físicos y tecnológicos.

Los 34 controles fueron seleccionados considerando las necesidades específicas de la organización y aquellos aspectos que generan mayor impacto sobre la confidencialidad, integridad y disponibilidad de la información así como sobre la operación de sus servicios críticos.

La distribución de los 34 controles priorizados es la siguiente:

Tabla II
Distribución de los controles priorizados según las categorías de ISO/IEC 27001:2022

Categoría ISO/IEC 27001:2022	Controles del Anexo A	Controles priorizados	Principales acciones en Novatech Logistics S.A.S
5. Controles organizacionales	37	11	roles y responsabilidades, inventario de activos, uso aceptable de activos, control de acceso, gestión de identidades, información de autenticación, derechos de acceso, seguridad con proveedores, gestión de incidentes y protección de datos personales.
6. Controles de	8	5	Verificación de

personas			antecedentes, concienciación y formación en seguridad de la información, proceso disciplinario, responsabilidades durante la desvinculación y acuerdos de confidencialidad.
7. Controles físicos	14	6	Protección del perímetro físico, control de entrada, seguridad de oficinas e instalaciones, monitoreo mediante CCTV, protección frente a amenazas físicas y ambientales y gestión segura de medios de almacenamiento.
8. Controles tecnológicos	34	12	Gestión de accesos privilegiados, restricción de acceso a la información, autenticación segura mediante MFA, protección contra código malicioso, gestión de vulnerabilidades, gestión de configuraciones, copias de seguridad, registro de eventos, monitoreo, seguridad y segregación de redes y uso de criptografía.
Total	93	34	Implementación de 34 controles priorizados dentro del alcance del proyecto.

La implementación de estos 34 controles permitirá establecer una línea base de seguridad dirigida a fortalecer la gestión de accesos, la protección de activos de información, la seguridad física, la gestión de incidentes, la protección de datos personales, la seguridad de la infraestructura tecnológica y la capacidad de prevención, detección y respuesta ante eventos de seguridad.

3.3.SECUENCIA DE ACTIVIDADES PARA EJECUCIÓN DE LA SOLUCIÓN

La solución propuesta para Novatech Logistics S.A.S., se desarrollará durante una secuencia de seis fases, orientadas a la implementación progresiva de los 34 controles de seguridad de la información priorizados de acuerdo con el contexto, los riesgos y las necesidades de la empresa. Estas fases comprenden desde la evaluación inicial, el análisis de riesgos, el diseño documental, la implementación de controles de personas, físicos y tecnológicos, hasta el fortalecimiento de los procesos de gestión de seguridad y la posterior auditoría interna revisada por la dirección. Este método permite establecer, implementar, verificar y mejorar de manera continua el sistema de gestión de seguridad de la información (SGSI), y así poder garantizar que las actividades propuestas se desarrollan de una forma organizada y alineada con los principales objetivos de seguridad de la organización.

Fase 1:

Evaluación inicial, análisis de riesgos y declaración de aplicabilidad (SoA).

Identificación y valoración de riesgos de seguridad de la información, análisis de brechas y definición de los 34 controles priorizados de acuerdo con el contexto de Novatech Logistics S.A.S.

Fase 2:

Diseño, redacción y aprobación del marco documental del SGSI.

Elaboración y aprobación de la Política General de Seguridad de la Información, políticas y

procedimientos asociados a los controles priorizados, incluyendo roles y responsabilidades, gestión de activos, control de acceso, gestión de incidentes y protección de datos personales.

Fase 3:

Implementación de controles de personas y físicos.

Ejecución de actividades relacionadas con verificación de antecedentes, capacitación y concienciación, acuerdos de confidencialidad, procesos de desvinculación, adecuación del perímetro físico, control de acceso al centro de datos, CCTV y protección frente a amenazas físicas y ambientales.

Fase 4:

Implementación de controles tecnológicos y fortalecimiento de la infraestructura de seguridad.

Implementación de MFA, gestión de cuentas privilegiadas, segmentación de redes mediante VLAN, firewall de nueva generación, protección contra código malicioso, gestión de vulnerabilidades, hardening, copias de seguridad, registro y monitoreo de eventos, y cifrado de la información.

Fase 5:

Implementación y fortalecimiento de los procesos de gestión de seguridad.

Puesta en operación de los procedimientos de gestión de incidentes, control de accesos, gestión de proveedores, protección de datos personales, gestión de activos y demás procesos asociados a los 34 controles priorizados.

Fase 6:

Auditoría interna, evaluación de resultados y revisión por la dirección.

Verificación del cumplimiento y eficacia de los controles implementados, identificación de no conformidades y oportunidades de mejora, establecimiento de acciones correctivas y revisión por la dirección del desempeño del SGSI.

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

Para implementar los 34 controles de seguridad de la información que se priorizaron para la empresa Novatech Logistics S.A.S, se requiere la disponibilidad de diferentes recursos que nos permitan desarrollar todas las actividades propuestas y garantizar la operación indicada del sistema de gestión de seguridad de la información (SGSI). Para esto, se consideran recursos humanos, tecnológicos, materiales físicos, documentales y financieros, los cuales cumplen funciones que complementan las diferentes fases de implementación. Una adecuada asignación y gestión de estos recursos nos va a permitir contar con el personal responsable, las herramientas tecnológicas, la infraestructura, la documentación y el presupuesto necesario para implementar, mantener y mejorar los controles de seguridad definidos.

- **Recursos humanos:** Oficial de Seguridad de la Información (CISO) o responsable del SGSI, personal del área de Tecnología y administradores de infraestructura, responsables de Recursos Humanos para los controles relacionados con el personal, responsables de seguridad física y apoyo de asesoría legal para aspectos relacionados con protección de datos personales, acuerdos de confidencialidad y relaciones con proveedores.
- **Recursos tecnológicos:** Soluciones de autenticación multifactor (MFA), firewall de nueva generación (NGFW), herramientas de protección contra código malicioso/EDR, herramientas para gestión y análisis de vulnerabilidades, mecanismos de registro y monitoreo de eventos de seguridad, infraestructura para copias de seguridad, herramientas de gestión de identidades y accesos, segmentación de redes mediante VLAN y mecanismos de cifrado de información.
- **Recursos materiales y físicos:** Sistemas de control de acceso físico mediante tarjeta o biometría, cerraduras y mecanismos de protección del centro de datos, sistema de videovigilancia (CCTV), señalización y delimitación del perímetro de seguridad, condiciones adecuadas de climatización para los equipos críticos y medios seguros para el almacenamiento y transporte de información.

- **Recursos documentales:** Políticas, procedimientos, instructivos, registros y demás documentación necesaria para soportar la implementación y operación de los controles priorizados, incluyendo la Política General de Seguridad de la Información, procedimientos de control de acceso, gestión de incidentes, gestión de activos, copias de seguridad, gestión de vulnerabilidades, gestión de proveedores y protección de datos personales.
- **Recursos financieros:** Presupuesto destinado a la adquisición o renovación de licencias de seguridad, implementación y adecuación de controles físicos y tecnológicos, servicios de asesoría especializada, actividades de capacitación y concienciación, auditoría interna y demás costos asociados a la implementación y mantenimiento de los 34 controles priorizados.

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

El alcance de la solución propuesta para Novatech Logistics S.A.S., abarca la totalidad de la operación de Novatech Logistics S.A.S., tanto en sede principal como bodegas y sedes operativas, teniendo en cuenta un cronograma operativo de nueve (9) meses para la implementación del SGSI, el cual busca proteger toda la información almacenada y procesada en los sistemas de Novatech Logistics S.A.S., así como bases de datos de los clientes, adicionalmente queda excluida del alcance del proyecto, la continuidad del negocio en un sitio alternativo, la implementación de controles asociados a la gestión de activos en la nube ya que la compañía cuenta con sus activos de manera local (infraestructura propia), la acreditación y certificación de la ISO 27001 ante un ente certificador y los controles restantes no priorizados para el proyecto, dando como resultado una implementación de un sistema de seguridad de la información con los controles priorizados indicados en la tabla 2 que se alinean con la situación actual de la compañía y que busca mejorar y fortalecer los diferentes procesos relacionados a la gestión de la información .

4.1.ALCANCE FINAL DE LA SOLUCIÓN

El alcance final para la propuesta de fortalecer la seguridad de la organización es implementar un SGSI basado en la norma ISO/IEC 27001:2022 para la empresa Novatech Logistics S.A.S. Este alcance busca abarcar los activos de información, procesos tecnológicos, infraestructura física y personal operativo de la sede principal, así como de todas las bodegas y sedes de la organización.

Inclusiones del alcance

Implementar progresivamente los 34 controles de seguridad priorizados del Anexo A de ISO/IEC 27001:2022 (11 organizacionales, 5 de personas, 6 físicos, y 12 tecnológicos) teniendo en cuenta el core del negocio en un tiempo determinado de nueve meses.

La cobertura del proceso de gestión de tecnología de la información y su interacción con gestión de inventario y almacenamiento ERP en la organización teniendo en cuenta la normativa vigente.

La protección de datos personales, bases de datos de clientes, listas de precios e inventarios y activos de información bajo la ley 1581 de 2012 de Colombia y demás leyes regulatorias aplicables según el tipo de información.

La evaluación y adecuación física de la infraestructura del data center local para que corresponda con los controles priorizados para el proyecto.

Exclusiones del alcance:

Se excluyen del alcance del proyecto los siguientes ítems:

Certificación y acreditación externa: Se excluye del alcance del proyecto la auditoría de certificación y acreditación formal del sistema de Gestión de Seguridad de la Información ante un organismo certificador externo. La auditoría contemplada dentro del proyecto corresponde exclusivamente a una auditoría interna del SGSI, destinada a evaluar el cumplimiento y la eficacia de los controles implementados e identificar oportunidades de mejora. Por lo tanto, el valor presupuestado para la auditoría interna no contempla costos asociados a procesos de certificación externa.

4.2. IDENTIFICACIÓN DE RESPONSABLES DE LAS ACTIVIDADES PARA EJECUCIÓN

Para organizar la ejecución vamos a asignar las responsabilidades mediante la matriz de responsabilidades (Matriz RACI) Con esta herramienta se permitirá identificar

R : Responsable , quien ejecuta la actividad

A: Aprobar, quien autoriza o rinde cuentas sobre el entregable

C: Consultado, quien proporciona información

I: Informado, quien recibe actualización del avance.

Roles participantes:

1. AD: Alta dirección
2. CISO: Oficial de seguridad de la información
3. TI: Área de tecnología y administradores de tecnología.

4. RH: Recursos humanos.
5. LEG: Asesoría legal y cumplimiento
6. SF: Seguridad física y mantenimiento.

Tabla III. Matriz RACI para la implementación del SGSI en Novatech Logistics S.A.S

Fase o actividad principal	Alta Dirección (AD)	CISO	Tecnología (TI)	Recursos Humanos (RH)	Legal (LEG)	Seguridad (SF)
Fase 1: Evaluación inicial, análisis de riesgos y SoA (34 controles)	A	R	C	I	C	I
Fase 2: diseño, redacción y aprobación del marco documental del SGSI.	A	R	C	C	C	I
Fase 3: implementación de controles de personas (NDA, antecedentes, capacitación).	A	C	I	R	C	I
Fase 4: Implementación de controles tecnológicos (MFA, NGFW, EDR, Hardening, VLANs)	A	C	R	I	I	I
Fase 5: Puesta en operación de procesos (Incidentes, Proveedores, Ley 1581)	A	R	C	C	R	I
Fase 6: Auditoría interna, evaluación de resultados y evaluación por la dirección	A	R	C	I	I	I

4.3. CRONOGRAMA DE EJECUCIÓN

A continuación se presenta la distribución temporal de actividades durante los nueve meses de implementación ajustada a las seis fases definidas en la sección 3.3

Tabla IV. Cronograma de implementación del SGSI

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9
Fase 1: Evaluación inicial y riesgos (- Diagnóstico GAP y SoA (34 controles).)	X								
Fase 2: Marco documental SGSI (Redacción y aprobación de políticas.)		X	X						
Fase 3: controles físicos y de personas (Selección/NDA/Capacitación (Personas)), (Control acceso/CCTV/Climatización (Físico).)			X	X	X				

Fase 4: Controles tecnológicos (NGFW, VLANs, MFA, EDR, Hardening), (Backups, Cifrado y Monitoreo SIEM.)					X	X	X		
Fase 5: Operación de procesos (Gestión de incidentes y proveedores)							X	X	
Fase 6: Auditoría y revisión directa (Auditoría interna y revisión directiva.)								X	X

4.4. PRESUPUESTO

El presupuesto estimado para la implementación del SGSI en Novatech Logistics S.A.S., se resume en la siguiente tabla teniendo en cuenta los diferentes elementos definidos en la sección 3.4 con un presupuesto en pesos colombianos y de manera más específica cada elemento usado y su justificación.

Tabla V. Presupuesto estimado para la implementación del SGSI

Rubro	Justificación	Valor Estimado
Diagnóstico, análisis GAP, riesgos y SoA	Evaluación inicial, identificación de activos, análisis de riesgos y selección documentada de controles.	\$12.000.000 COP

Diseño documental y asesoría para el SGSI	Elaboración de políticas, procedimientos, matrices, registros e indicadores.	\$16.000.000 COP
Capacitación y simulaciones de phishing	Formación de colaboradores, material educativo y ejecución de campañas de sensibilización.	\$8.000.000 COP
Autenticación multifactor y gestión de accesos	Licencias, configuración de MFA y fortalecimiento de cuentas privilegiadas	\$12.000.000 COP
NGFW y segmentación de redes	Adquisición o fortalecimiento del firewall, configuración de VLANs y segregación de redes	\$25.000.000 COP
EDR, gestión de vulnerabilidades y hardening	Protección de equipos críticos, análisis de vulnerabilidades y configuración segura	\$18.000.000 COP
Copias de seguridad y mecanismos de cifrado	Infraestructura de respaldo, pruebas de restauración y protección criptográficas	\$15.000.000 COP
SIEM y centralización de registros	Recolección, almacenamiento, correlación y monitoreo básico de eventos	\$18.000.000 COP
Adecuaciones físicas del centro de datos	Control de acceso, CCTV, cerraduras, monitoreo y protección ambiental.	\$20.000.000 COP
Auditoría interna y evaluación final	Auditoría independiente, elaboración del informe de hallazgos y verificación de acciones correctivas. Esta actividad se realiza internamente, no sustituye una auditoría externa de certificación y su costo es independiente de los costos correspondientes al proceso de certificación.	\$7.000.000 COP

Subtotal		\$151.000.000 COP
Reserva de contingencia del 10%	Atención de variaciones de precio y requerimientos no previstos	\$15.100.000 COP
Total estimado		\$166.100.000

5. REFERENCIAS BIBLIOGRÁFICAS

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. **Diario Oficial n.º 47.223**.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales*. **Diario Oficial n.º 48.587**.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Departamento Nacional de Planeación [DNP]. (2016). *Documento CONPES 3854: Política nacional de seguridad digital. Consejo Nacional de Política Económica y Social*.

<https://bibliotecadigital.ccb.org.co/server/api/core/bitstreams/d2ea30e4-2079-41fd-b913-2b1c8f23b76e/content>

Departamento Nacional de Planeación [DNP]. (2020). *Documento CONPES 3995: Política nacional de confianza y seguridad digital. Consejo Nacional de Política Económica y Social*.

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf>

Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2022). *Norma Técnica Colombiana NTC-ISO-IEC 27001:2022, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos*. ICONTEC.

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2021). *Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital*.

https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_0500_2021.htm

Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2025). *Resolución 02277 de 2025, por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia*.

https://normograma.mintic.gov.co/mintic/compilacion/docs/resolucion_mintic_2277_2025.htm

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley 1581 de 2012. Compilado en el Decreto 1074 de 2015, Título 2.2.2.25.* <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646>

Presidencia de la República de Colombia. (2015). *Decreto 1074 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.* <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608>

Superintendencia de Industria y Comercio [SIC]. (s.f.). *Registro Nacional de Bases de Datos (RNBD).* Recuperado el 1 de agosto de 2026, de <https://www.sic.gov.co/tema/proteccion-de-datospersonales/registro-nacional-de-bases-de-datos>