UNIVERSIDAD INTERNACIONAL DE LAS AMÉRICAS

ESCUELA DE INGENIERÍA INFORMÁTICA

Propuesta para la implementación de la seguridad física y del entorno basada en la norma ISO/IEC 27001:2022 e ISO/IEC 27002:2022, para la empresa Sauter Infomax S.A, ubicada en San José

MODALIDAD PROYECTO PARA OPTAR POR EL GRADO DE BACHILLER EN INGENIERÍA DE SOFTWARE

Mariana de los Ángeles Chinchilla Murillo.

Enero, 2026

Dedicatoria

Primeramente, dedico este logro a Dios, quien ha sido mi guía, mi fortaleza y el centro de mi vida durante todo este camino. Gracias por acompañarme en cada desafío, por brindarme la sabiduría, la paciencia y la fuerza necesaria para continuar cuando las circunstancias parecían difíciles. Hoy reconozco que cada paso recorrido fue posible gracias a Su voluntad y amor.

A mis padres, Magaly y Manuel, quienes han sido mi mayor inspiración y el pilar fundamental de este sueño. Gracias por cada sacrificio, por su amor incondicional, por creer en mí y por enseñarme con su ejemplo el valor del esfuerzo, la perseverancia y la dedicación. Este logro lleva una parte de ustedes, porque sin su apoyo y acompañamiento no habría llegado hasta este momento tan importante de mi vida.

A mi hermano Matías, dedico también este logro con mucho amor, con la esperanza de que sea un recordatorio de que los sueños se alcanzan con esfuerzo, disciplina y fe. Deseo que este sea un ejemplo para ti y que muy pronto puedas celebrar tus propias metas y ver cumplidos todos tus sueños.

Hoy cierro una etapa que representa años de esfuerzo, aprendizajes y crecimiento, pero también el inicio de nuevos caminos. Este logro no solo representa una meta alcanzada, sino la historia de quienes estuvieron conmigo, me sostuvieron y me motivaron a seguir adelante.

Con todo mi amor y gratitud, dedico este logro a Dios y a mi familia, quienes han sido mi razón para perseverar y llegar hasta aquí.

Agradecimientos

Primeramente, agradezco a Dios por haberme acompañado durante este camino, por brindarme la fortaleza, sabiduría y perseverancia necesarias para culminar esta etapa tan importante de mi vida. Gracias por guiar cada uno de mis pasos y permitirme alcanzar una meta que representa años de esfuerzo, dedicación y crecimiento.

Agradezco profundamente a mi tío Diego, quien fue una pieza fundamental en el inicio de este camino profesional. Gracias por brindarme la oportunidad de comenzar mis estudios, por confiar en mí, creer en mis capacidades y apoyarme en un momento determinante de mi vida. Este logro también es reflejo de esa confianza y del impulso que me permitió iniciar esta etapa.

A mis padres, Magaly y Manuel, a mi hermano Matías, y a toda mi familia, especialmente a mis tías Shirley y Karla, a mi abuela Tita, a mis primos, especialmente Alexander y a mis angelitos en el cielo: Tita Lili, Tito, Golo y Daniel, gracias por su amor, apoyo y por formar parte fundamental de mi vida. Cada palabra de aliento, cada muestra de cariño y cada momento compartido fueron una motivación para continuar y alcanzar esta meta. A Gabriel, por acompañarme durante esta última etapa de mi carrera universitaria, por su apoyo, paciencia y motivación en los momentos de mayor esfuerzo. Gracias por estar presente, brindarme tranquilidad y caminar conmigo en este proceso tan importante.

A la Universidad Internacional de las Américas, a mis profesores y a todas las personas que formaron parte de mi formación académica, les agradezco por los conocimientos transmitidos, la orientación brindada y las herramientas que contribuyeron a mi crecimiento profesional y personal. A Sauter Infomax S.A., gracias por brindarme la oportunidad de desarrollar este proyecto final de graduación dentro de la organización, por la confianza depositada en mí y por permitirme aplicar los conocimientos adquiridos durante mi carrera en un entorno profesional.

Finalmente, agradezco a todas las personas que estuvieron presentes durante este proceso y que, de una u otra manera, aportaron su apoyo, motivación y acompañamiento para que hoy pueda celebrar la culminación de esta importante etapa

CONTENIDO

CAPÍTULO I: INTRODUCCIÓN 10
Descripción del Problema 10
Objetivos 10
Justificación 11
Proyecciones 20
CAPÍTULO II: MARCO REFERENCIAL 28
Introducción al Marco Referencial 28
Seguridad de la Información 28
Propuesta de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO/IEC 27001:2022 31
Normas ISO/IEC 27001:2022 y ISO/IEC 27002:2022 aplicadas a la Seguridad Física y del Entorno 36
Política y Procedimientos de Seguridad Física y del Entorno 40
Gestión de Riesgos 45
Controles de Seguridad Física y Ambiental 48
Auditoria de Seguridad 49
Cumplimiento Legal 51
Clasificación y Protección de Activos de Información 53
CAPITULO III: MARCO METODOLÓGICO 55
Enfoques de Investigación 55
Enfoque Cuantitativo 56
Enfoque Cualitativo 57
Enfoque Mixto 57
Enfoque de Investigación Seleccionado 58
Tipos de Investigación 59
Investigación Exploratoria 59
Investigación Descriptiva 60

Investigación Correlacional 60
Tipo de investigación Seleccionado 60
Tipos de Variables 64
Variable Conceptual 64
Variable Operacional 64
Variable Instrumental 65
Importancia de las Variables en la Investigación 65
Población 69
Muestra 70
Tipo de Muestreo 70
Instrumentos de Recolección de Datos 71
Encuesta 71
Observación 71
Instrumentos de Recolección de Datos 72
Cuestionario 72
CAPÍTULO IV: ANÁLISIS DE RESULTADOS 73
Aplicación de instrumentos. 73
Matriz de Riesgos de Seguridad Física y del Entorno 87
Declaración de Aplicabilidad (SoA) – ISO/IEC 27001:2022 89
CAPÍTULO V: PROPUESTA 92
Partes Interesadas del SGSI 94
Elementos Incluidos dentro del Alcance del SGSI 95
Clasificación de Activos de Información 95
Relación entre Activos y Controles de Protección 96
Declaración de Aplicabilidad (SoA) – ISO/IEC 27001:2022 97
Gestión documental para la implementación y seguimiento de los controles 99
Política de Seguridad Física y del Entorno 110
Procedimiento de Control de Acceso Físico 111
Procedimiento de Seguridad Ambiental 112
Responsables 113

Procedimiento de Monitoreo y Vigilancia Física 114
Evidencias y registros 115
Procedimiento de Manejo y Almacenamiento de Información Física 115
Procedimiento de Gestión y Reporte de Incidentes de Seguridad Física y del Entorno 118
Plan de Capacitación y Concientización 119
Plan de Acción y Mejora Continua (PHVA) 122
Indicadores de Desempeño con Umbrales 123
Equipo implementador y esquema de seguimiento 125
Matriz RACI del SGSI 127
Conclusión de la Propuesta 130
CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES 132
Conclusiones 132
Recomendaciones 133
REFERENCIAS 135
ANEXOS 136

TABLAS

Tabla 1 Costos 15
Tabla 2 Fase de Desarrollo del SGSI (Construcción de la Propuesta) 16

Tabla 3 Fase de Implementación y Seguimiento del SGSI (Operación Mensual) 17
Tabla 4 Costos estimados y seguimiento 18
Tabla 5 Descripción de los Módulos del Sistema..... 22
Tabla 6 Partes Interesadas 33
Tabla 7 Mapa de Cobertura del SGSI..... 35
Tabla 8 Clasificación de Activos de Información según Nivel de Criticidad 53
Tabla 9 Relación entre Clasificación de Activos y Controles de Protección 54
Tabla 10 Enfoque comparativo..... 58
Tabla 11 Matriz de relación: Instrumento – Variable – Control – Evidencia..... 61
Tabla 12 Cuadro de Variables..... 65
Tabla 13 Matriz de Riesgos de Seguridad Física y del Entorno 87
Tabla 14 Declaración de Aplicabilidad (SoA) – Seguridad Física y del Entorno 89
Tabla 15 Descripción de los Módulos del Sistema..... 93
Tabla 16 Partes Interesadas del SGSI..... 94
Tabla 17 Elementos incluidos dentro del alcance del SGSI 95
Tabla 18 Clasificación de activos de información..... 96
Tabla 19 Relación entre activos y controles de protección..... 96
Tabla 20 Declaración de Aplicabilidad – Seguridad Física y del Entorno 97
Tabla 21 Gestión documental para la implementación de los controles 101
Tabla 22 Clasificación de soportes físicos por nivel de riesgo..... 116
Tabla 23 Plan de capacitación y concientización..... 119
Tabla 24 Plan de acción y mejora continua del SGSI 122
Tabla 25 Indicadores de desempeño y umbrales del SGSI..... 123
Tabla 26 Ejecución cotidiana de los controles 126
Tabla 27 Cronograma..... 129

FIGURAS

Figura 1Triada CIA de la seguridad de la información 30

Figura 2 Contexto Organizacional.....34
Figura 3 Estructura de la Norma ISO/IEC 27001:2022 38
Figura 4 Elementos de Seguridad Física y Control de Accesos 41
Figura 5 Proceso de Evaluación de Riesgos de Seguridad de la Información 47
Figura 6 Fases de la auditoría interna.....51
Figura 7 Pregunta 1 74
Figura 8 Pregunta 2 74
Figura 9 Pregunta 3 75
Figura 10 Pregunta 4 76
Figura 11 Pregunta 5 77
Figura 12 Pregunta 6 77
Figura 13 Pregunta7 78
Figura 14 Pregunta 8 78
Figura 15 Pregunta 9 79
Figura 16 Pregunta 10 79

ANEXOS

Anexo 1 Cuestionario 136
Anexo 2 Entrevista 139
Anexo 3 Guía de observación 141
Anexo 4 Bitácora de control de acceso físico 145
Anexo 5 Registro de visitantes 146
Anexo 6 Formato de reporte de incidentes de Seguridad Física y del Entorno 146
Anexo 7 Lista de verificación de controles de Seguridad Física y del Entorno 147
Anexo 8 Registro de mantenimiento preventivo 148
Anexo 9 Registro de capacitación y concientización 149

CAPÍTULO I: INTRODUCCIÓN

Descripción del Problema

Sauter Infomax S.A. es una organización costarricense ubicada en San José, dedicada íntegramente a la comercialización, soporte y ejecución de soluciones tecnológicas avanzadas. En la actualidad, sus operaciones principales dependen de un manejo riguroso de la información y de la protección efectiva de sus activos físicos y digitales. No obstante, la empresa presenta debilidades críticas en su seguridad física, tales como la inexistencia de políticas documentadas y deficiencias en los controles de acceso a áreas de alta sensibilidad. Estas limitaciones incrementan la exposición a riesgos operativos, haciendo imperativo el desarrollo de una propuesta técnica alineada a la norma ISO/IEC 27001:2022 que fortalezca la protección institucional.

Objetivos

Objetivo General

Elaborar una propuesta para la implementación de la Seguridad Física y del Entorno en la empresa Sauter Infomax S.A., ubicada en San José, alineada a la norma ISO/IEC 27001:2022.

Objetivos Específicos

Analizar la situación actual de la seguridad física y del entorno en Sauter Infomax S.A., utilizando herramientas investigativas como el análisis FODA y cuadros comparativos, con el propósito de identificar brechas, riesgos y vulnerabilidades en relación con los lineamientos de la norma ISO/IEC 27001:2022.

Determinar los requerimientos normativos, el alcance y los elementos críticos del Sistema de Gestión de Seguridad de la Información (SGSI) que serán considerados en la propuesta, tomando en cuenta los activos, procesos, infraestructura y responsabilidades vinculadas con la seguridad física y del entorno.

Elaborar la política y los procedimientos documentados necesarios para la implementación de la seguridad física y del entorno, conforme a los controles establecidos en la norma ISO/IEC 27001:2022 y las buenas prácticas definidas en la norma ISO/IEC 27002:2022.

Desarrollar los instrumentos investigativos y de apoyo técnico, tales como matrices de control, cuadros comparativos y esquemas metodológicos, que respalden la aplicación práctica de la propuesta dentro del marco del SGSI.

Proponer un plan de acción y mejora continua que contemple estrategias de evaluación, seguimiento y retroalimentación, orientado a asegurar la vigencia, efectividad y actualización permanente de la seguridad física y del entorno en la empresa.

Justificación

La presente investigación se desarrolla con el propósito de elaborar una propuesta para la implementación de la seguridad física y del entorno en la empresa Sauter Infomax S.A., conforme a los lineamientos establecidos en la norma ISO/IEC 27001:2022. La seguridad de los activos físicos, tecnológicos y de información constituye un elemento fundamental para el adecuado funcionamiento de las organizaciones, ya que permite garantizar la continuidad de los procesos operativos. En este sentido, la ausencia de controles adecuados puede generar riesgos que afecten la confidencialidad, integridad y disponibilidad de la información. Asimismo, estas debilidades pueden provocar pérdidas económicas, afectaciones en la imagen institucional y disminución de la confianza de los usuarios. Ante esta realidad, resulta necesario analizar las condiciones actuales de seguridad física y ambiental de la empresa, identificar posibles brechas y establecer mecanismos de protección. Lo anterior contribuirá a una gestión más eficiente de los riesgos y al cumplimiento de estándares internacionales reconocidos.

La investigación se lleva a cabo con el fin de proporcionar a la organización una herramienta técnica y metodológica que facilite la toma de decisiones en materia de seguridad, así

como la implementación de procedimientos documentados y planes de mejora continua dentro del Sistema de Gestión de Seguridad de la Información. De igual forma, permitirá fortalecer los controles internos y promover una cultura organizacional orientada a la prevención de riesgos. Los resultados obtenidos contribuirán a optimizar los procesos internos, reducir la exposición a incidentes y mejorar la imagen institucional. Asimismo, se espera fortalecer la confianza de clientes, colaboradores y proveedores mediante la aplicación de buenas prácticas de seguridad. Finalmente, el estudio favorecerá el desarrollo académico y profesional de la autora, al promover la aplicación práctica de conocimientos relacionados con la gestión de la seguridad de la información y las normativas internacionales.

Viabilidad Técnica

La presente investigación es técnicamente viable, debido a que la empresa Sauter Infomax S.A. cuenta con los recursos tecnológicos, físicos y organizacionales necesarios para el desarrollo de la propuesta de implementación de la seguridad física y del entorno, conforme a la norma ISO/IEC 27001:2022.

Desde el punto de vista del hardware, la organización dispone de equipos de cómputo, servidores, dispositivos de red, sistemas de almacenamiento, cámaras de vigilancia, controles de acceso, infraestructura eléctrica y sistemas de respaldo que permiten el análisis, documentación y evaluación de los controles establecidos en los diferentes módulos de la investigación. Estos recursos facilitan la elaboración de mapas de cobertura, diagnósticos de riesgos, matrices de control y esquemas de monitoreo.

En cuanto al software, la empresa cuenta con sistemas operativos actualizados, herramientas ofimáticas, plataformas administrativas y aplicaciones de gestión que permiten la elaboración de cuadros comparativos, matrices de evaluación, diagramas, indicadores de desempeño y procedimientos documentados. Estas herramientas respaldan el desarrollo de instrumentos técnicos necesarios para la implementación teórica del Sistema de Gestión de Seguridad de la Información.

Respecto a las licencias, la organización dispone de software debidamente autorizado, lo cual garantiza el uso legal y estable de las plataformas utilizadas. Además, la norma ISO/IEC

27001:2022 no exige el uso obligatorio de herramientas especializadas de alto costo, por lo que la investigación puede desarrollarse con los recursos existentes.

En relación con el espacio físico, la empresa cuenta con oficinas administrativas, áreas operativas, zonas de almacenamiento, espacios tecnológicos y áreas de acceso restringido que permiten evaluar y documentar los controles de seguridad física, ambiental y de monitoreo. Estas instalaciones facilitan la elaboración de mapas de riesgo, análisis de vulnerabilidades y propuestas de mejora.

Adicionalmente, el personal de la organización posee conocimientos básicos en el uso de herramientas tecnológicas y en la gestión de procesos internos, lo que favorece la recopilación de información, la aplicación de instrumentos investigativos y la validación de los procedimientos propuestos.

Asimismo, la estructura modular de la investigación, que abarca el alcance del SGSI, el control de accesos, la seguridad ambiental, el manejo de información física, el monitoreo, la capacitación, el plan de acción y el seguimiento, permite desarrollar la propuesta de manera ordenada, progresiva y técnicamente sustentada.

Por lo anterior, se concluye que la investigación es viable desde el punto de vista técnico, ya que existen los recursos, herramientas y condiciones necesarias para su adecuada ejecución, sin requerir inversiones extraordinarias ni modificaciones estructurales significativas.

Viabilidad Operativa

La presente investigación es viable desde el punto de vista operativo, ya que la propuesta de implementación de la seguridad física y del entorno basada en la norma ISO/IEC 27001:2022 se adapta a la estructura organizacional, a los procesos internos y a las capacidades del personal de la empresa Sauter Infomax S.A.

En relación con los conocimientos requeridos, el desarrollo y aplicación de la propuesta demanda competencias básicas en gestión de procesos, uso de herramientas tecnológicas, manejo documental y principios de seguridad de la información. Dichos conocimientos se encuentran presentes en el personal administrativo, técnico y operativo de la organización, lo cual facilita la comprensión y aplicación de los procedimientos establecidos.

Asimismo, la empresa cuenta con personal calificado en áreas como tecnología, soporte técnico, administración y gestión comercial, quienes participan directamente en el manejo de la

información, los equipos y las instalaciones. Esta condición favorece la adopción de los controles propuestos en materia de acceso físico, seguridad ambiental, manejo de documentos, monitoreo y seguimiento.

No obstante, para garantizar una correcta implementación, se contempla la realización de procesos de capacitación y concientización dirigidos a los colaboradores, con el fin de fortalecer la cultura organizacional de seguridad y asegurar el cumplimiento adecuado de las políticas y procedimientos definidos.

Los principales usuarios de la propuesta serán el personal administrativo, el área de tecnología, los encargados de seguridad, la gerencia y los colaboradores que tienen acceso a información, equipos o espacios críticos. Estos actores participarán activamente en la aplicación, seguimiento y evaluación de los controles establecidos dentro del Sistema de Gestión de Seguridad de la Información.

En cuanto al impacto organizacional, la implementación de la propuesta no generará reducción de personal, ya que su enfoque se orienta al fortalecimiento de los procesos existentes y no a la sustitución de funciones. Por el contrario, permitirá una mejor distribución de responsabilidades y una mayor claridad en los roles relacionados con la seguridad.

Asimismo, la propuesta sí implicará ajustes en la forma en que se realizan algunas actividades, tales como el control de accesos, el registro de visitantes, el manejo de documentos físicos, el monitoreo de instalaciones y la atención de incidentes. Estos cambios buscan estandarizar los procesos, reducir riesgos y mejorar la eficiencia operativa, sin afectar negativamente el desempeño del personal.

Por lo anterior, se concluye que la investigación es operativamente viable, debido a que puede integrarse de manera efectiva a la dinámica laboral de la empresa, cuenta con el respaldo del personal y permite la obtención de los beneficios esperados en materia de seguridad, organización y mejora continua.

Viabilidad Económica

La viabilidad económica de la presente investigación se fundamenta en el análisis de los costos asociados al desarrollo de la propuesta para la implementación de la seguridad física y del entorno, conforme a la norma ISO/IEC 27001:2022, en la empresa Sauter Infomax S.A. El análisis

contempla los gastos relacionados con software, hardware, mobiliario, recursos humanos y otros costos operativos necesarios para el desarrollo de los módulos, instrumentos técnicos, cuadros, matrices y procedimientos documentados que conforman la investigación.

Tabla 1

Costos

Categoría	Descripción	Costo Unitario (₡)	Cantidad	Costo Total (₡)
Software	Licencia Microsoft 365 Empresa Premium	10 900	1	10 900
Software	Plataforma de gestión documental Softland	120 000	1	120 000
Hardware	Computadoras de escritorio	450 000	2	900 000
Hardware	Servidor de almacenamiento	850 000	1	850 000
Hardware	Cámaras devideovigilancia	85 000	4	340 000
Hardware	Dispositivos de control de acceso	150 000	2	300 000
Mobiliario	Archivadores metálicos	95 000	2	190 000
Mobiliario	Escritorios administrativos	180 000	2	360 000
Recurso Humano	Análisis y documentación (estudiante)	6 000	120	720 000
Recurso Humano	Supervisión técnica	12 000	40	480 000
Otros Costos	Material impreso y papelería	50 000	1	50 000
Otros Costos	Capacitación interna	150 000	1	150 000
Otros Costos	Mantenimiento preventivo	120 000	1	120 000
Servicio externo	Evaluación independiente posterior	150.000	3	450.000
Servicio externo especializado	Acompañamiento y evaluación durante la implementación: revisión inicial, seguimiento y evaluación final	250.000	1	250.000
Total, General				₡5.290.900

Fuente: Elaboración propia, 2026.

Adicionalmente, es necesario considerar las horas hombre requeridas para la implementación, seguimiento y mejora continua de los controles de seguridad física y del entorno propuestos en la presente investigación. Si bien el desarrollo inicial de los procedimientos y la documentación técnica es realizado por la investigadora, la correcta implementación del Sistema de Gestión de Seguridad de la Información implica la participación activa del personal de la organización en la ejecución, monitoreo y control de las medidas establecidas.

En este sentido, la aplicación de los controles definidos con base en la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022 requiere la asignación de tiempo por parte de los colaboradores para actividades como el control de accesos, registro de visitantes, supervisión de instalaciones, verificación de condiciones ambientales y seguimiento de incidentes. Estas actividades forman parte del ciclo de mejora continua (PHVA), el cual establece la necesidad de planificar, ejecutar, verificar y actuar sobre los controles implementados.

Por lo tanto, aunque la empresa no incurre en costos adicionales directos, sí existe una inversión en tiempo operativo del personal, la cual se integra dentro de sus funciones habituales. Este enfoque permite garantizar la sostenibilidad del sistema en el tiempo, asegurando que los controles no solo se implementen, sino que también sean evaluados y mejorados continuamente.

Para efectos de la presente investigación, se estima la siguiente distribución de horas hombre asociadas a la implementación y seguimiento de los controles:

Horas Hombre para el Desarrollo, Implementación y Seguimiento correcto de implementación del Sistema de Gestión de Seguridad de la Información.

Con el fin de estimar el esfuerzo requerido para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) orientado a la seguridad física y del entorno, se contemplan tanto las actividades de **desarrollo (diseño y documentación)** como las de **implementación y seguimiento**, en concordancia con el ciclo de mejora continúa establecido en la norma ISO/IEC 27001:2022

Tabla 2 Fase de Desarrollo del SGSI (Construcción de la Propuesta)

Actividad	Responsable	Horas Estimadas
Levantamiento de información y diagnóstico de brechas	Investigadora	40 horas
Definición del alcance del SGSI	Investigadora	16 horas
Elaboración de la política de seguridad física y del entorno	Investigadora	12 horas
Desarrollo de procesos y procedimientos documentados	Investigadora	48 horas

Identificación y análisis de riesgos (seguridad física)	Investigadora	32 horas
Selección de controles (alineados a ISO 27002:2022)	Investigadora	24 horas
Elaboración de matriz de riesgos y plan de tratamiento	Investigadora	24 horas
Documentación de la Declaración de Aplicabilidad (SoA)	Investigadora	16 horas

Total, fase de desarrollo: 212 horas

Tabla 3 Fase de Implementación y Seguimiento del SGSI (Operación Mensual)

Actividad	**Responsable**	**Frecuencia**	**Horas estimadas**
Control de acceso y registro de visitantes	Administración	Continua / revisión mensual	20 h mensuales
Supervisión de instalaciones y equipos	Soporte Técnico	Mensual	16 h mensuales
Verificación de condiciones ambientales	Soporte Técnico	Mensual	10 h mensuales
Monitoreo y registro de incidentes	Administración	Continua / revisión mensual	12 h mensuales
Revisión y mejora de procedimientos	Administración	Mensual	8 h mensuales

Capacitación y concientización	Recursos Humanos	Trimestral	6 h trimestrales
Evaluación independiente de controles	Proveedor externo especializado	Anual	Según alcance contratado

Total, estimado mensual: 72 horas

Tabla 4 Costos estimados y seguimiento

Actividad	**Frecuencia**	**Costo estimado**
Mantenimiento preventivo	Trimestral	₡120.000 por intervención
Capacitación y concientización	Trimestral	₡150.000 por actividad
Seguimiento interno de indicadores, registros y controles	Mensual	Incluido en horas operativas del personal
Revisión de matriz de riesgos y SoA	Anual o ante cambios significativos	Incluido en horas operativas del personal
Evaluación independiente de controles	Anual	₡250.000
Actualización documental	Según resultados de seguimiento o cambios significativos	Incluido en horas operativas del personal

Los costos recurrentes permiten proyectar los recursos necesarios para mantener la propuesta después de su implementación inicial. Las actividades de seguimiento interno se desarrollarán principalmente mediante horas operativas del personal asignado, mientras que el mantenimiento preventivo, las capacitaciones y la evaluación independiente requieren una previsión presupuestaria de acuerdo con la frecuencia establecida. Estas actividades se encuentran

vinculadas con las fases Verificar y Actuar del ciclo PHVA, permitiendo identificar desviaciones, establecer acciones correctivas y actualizar los controles cuando sea necesario.

Análisis

La estimación realizada evidencia que la mayor carga de trabajo se concentra inicialmente en el desarrollo y preparación de la propuesta, donde se elaboran la política, los procedimientos, la matriz de riesgos, la Declaración de Aplicabilidad (SoA) y los instrumentos requeridos para la implementación de los controles de Seguridad Física y del Entorno.

Posteriormente, durante la operación, los recursos se orientan principalmente al seguimiento de los controles, mantenimiento preventivo, gestión de incidentes, capacitación, revisión de indicadores y actualización documental. Estas actividades se desarrollan con frecuencias mensuales, trimestrales o anuales según su naturaleza, permitiendo distribuir los recursos necesarios durante el ciclo de mejora continua.

De esta manera, la viabilidad económica no contempla únicamente la inversión requerida para iniciar la propuesta, sino también los costos y recursos necesarios para mantenerla, evaluarla y mejorarla en el tiempo. Esto permite a Sauter Infomax S.A. contar con una proyección más realista de los recursos requeridos para sostener los controles de Seguridad Física y del Entorno.

Viabilidad Legal

La viabilidad legal de la presente investigación se fundamenta en el cumplimiento de la normativa nacional vigente y de los lineamientos establecidos por la ISO/IEC 27001:2022, la cual regula la implementación de un Sistema de Gestión de Seguridad de la Información orientado a la protección de los activos organizacionales. En este sentido, la investigación define claramente sus requisitos legales, institucionales y normativos, asegurando el respeto de las políticas internas, los derechos de los colaboradores y las disposiciones relacionadas con el uso responsable de la información y la tecnología.

En complemento con lo anterior, se incorporan los lineamientos de la ISO/IEC 27002:2022, la cual proporciona un conjunto de buenas prácticas para la implementación de controles de seguridad de la información, permitiendo que los requisitos establecidos en la ISO/IEC 27001:2022

sean aplicados de manera efectiva dentro de la organización. Esta norma contribuye a fortalecer el cumplimiento legal al establecer medidas concretas relacionadas con el control de accesos, la protección de instalaciones, la gestión de activos y la prevención de riesgos físicos y ambientales, aspectos que inciden directamente en la responsabilidad jurídica de la empresa.

Asimismo, la evaluación de alternativas permite seleccionar la opción más adecuada desde el punto de vista legal, considerando su impacto organizacional, su factibilidad de aplicación y su nivel de cumplimiento normativo. De igual forma, el análisis de oportunidades evidencia que la propuesta contribuye al fortalecimiento del marco legal institucional y a la reducción de riesgos jurídicos asociados a la pérdida, alteración o acceso no autorizado a la información.

Finalmente, se promueve la preparación de la empresa para procesos de auditoría y certificación bajo estándares internacionales, lo cual incrementa su competitividad, credibilidad y sostenibilidad en el mercado, garantizando además una gestión alineada con buenas prácticas reconocidas en materia de seguridad de la información.

Proyecciones

En este apartado se establecen los resultados esperados a partir del desarrollo de la presente investigación y de la propuesta para la implementación de la seguridad física y del entorno conforme a la norma ISO/IEC 27001:2022. Se proyecta que el producto final del estudio permita a la empresa contar con una base técnica, metodológica y documental para la gestión adecuada de sus activos físicos, tecnológicos y de información, mediante la elaboración de políticas, procedimientos, matrices, indicadores y planes de mejora debidamente estructurados. Asimismo, se espera que la propuesta contribuya al fortalecimiento del Sistema de Gestión de Seguridad de la Información, facilitando la estandarización de procesos, la reducción de vulnerabilidades y la mejora en la toma de decisiones relacionadas con la seguridad institucional.

Desde el punto de vista operativo, se prevé que el prototipo metodológico desarrollado sirva como una herramienta de apoyo para la implementación, seguimiento y evaluación de los controles de seguridad física y ambiental, permitiendo a la organización aplicar de manera sistemática los lineamientos establecidos en la norma ISO/IEC 27001:2022. De igual forma, se proyecta que la investigación funcione como un referente técnico para futuras auditorías, procesos de certificación

e iniciativas de mejora continua, contribuyendo al cumplimiento progresivo de los estándares internacionales.

En cuanto a los beneficios organizacionales, la implementación de la propuesta permitirá fortalecer la protección de los activos físicos, tecnológicos y documentales, reducir los riesgos asociados a accesos no autorizados, incidentes físicos y fallas ambientales, mejorar la organización y el control de los procesos internos, e incrementar la confianza de clientes, colaboradores y proveedores. Asimismo, favorecerá la optimización de los recursos destinados a la seguridad y preparará a la empresa para procesos de evaluación externa y certificación, consolidando su imagen institucional.

Finalmente, estos resultados contribuirán al fortalecimiento institucional, a la sostenibilidad operativa y al posicionamiento competitivo de Sauter Infomax S.A. en el mercado, al promover una cultura organizacional orientada a la prevención, la gestión de riesgos y la mejora continua en materia de seguridad física y del entorno.

Alcance Funcional.

El sistema propuesto, enmarcado dentro del Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022, contará con capacidades orientadas al análisis, documentación, control, seguimiento y mejora continua de la seguridad física y del entorno en la empresa Sauter Infomax S.A. Estas capacidades permitirán definir y documentar el alcance de la política de seguridad física y del entorno, establecer controles de acceso en zonas críticas, gestionar la seguridad ambiental y de infraestructura, y regular el manejo y almacenamiento de la información física. Asimismo, el sistema facilitará la implementación de mecanismos de monitoreo y vigilancia, el desarrollo de programas de capacitación y concientización, y el diseño de planes de acción orientados a la mejora continua. De igual forma, permitirá aplicar procesos sistemáticos de seguimiento y evaluación del desempeño, con el fin de verificar el cumplimiento de los controles establecidos. Todas estas funcionalidades contribuyen al fortalecimiento de la protección de los activos institucionales, a la estandarización de los procesos internos y a la optimización de la gestión de riesgos. En este sentido, el sistema se constituye como una herramienta integral para el apoyo a la toma de decisiones en materia de seguridad física y del entorno

Tabla 5 Descripción de los Módulos del Sistema

Nombre del apartado	Descripción del apartado
Alcance de la Política de Seguridad Física y del Entorno.	Se definirá el alcance de la política de seguridad física y del entorno dentro del marco del SGSI, bajo los lineamientos de la ISO/IEC 27001:2022, abarcando los procesos internos, infraestructura tecnológica y espacios físicos que resguardan información. **Objetivos tangibles:** • Elaborar un mapa de cobertura del SGSI que delimite los activos, área de tecnología y procesos incluidos. • Crear un procedimiento documentado para la definición, revisión y actualización del alcance del SGSI.
Control de Acceso Físico.	Se establecerán lineamientos de control de acceso físico para las zonas críticas, conforme al control A.11.1 de la ISO/IEC 27001:2022, garantizando la protección del entorno y los activos. **Objetivos tangibles:** • Diseñar una matriz de control de acceso físico que relacione áreas, riesgos y niveles de autorización. • Realizar un análisis comparativo entre las prácticas actuales de acceso y las recomendaciones de la norma. • Elaborar un procedimiento documentado de acceso físico (registro de visitantes, control de credenciales, restricción de áreas).
Seguridad Ambiental y de Infraestructura.	Se documentarán los mecanismos necesarios para resguardar los activos tecnológicos y físicos contra amenazas ambientales. **Objetivos tangibles:** • Elaborar un FODA sobre las condiciones ambientales y de infraestructura actuales. • Crear un cuadro diagnóstico de vulnerabilidades ambientales, basado en los controles A.11.2 de la ISO/IEC 27001:2022. • Redactar un procedimiento de seguridad ambiental que incluya monitoreo de temperatura, control eléctrico y mantenimiento preventivo.

Manejo y Almacenamiento de Información Física.	Se definirán procedimientos para el manejo, almacenamiento y disposición de documentos o dispositivos físicos. **Objetivos tangibles:** • Elaborar un cuadro de riesgos por tipo de soporte físico (papel, discos, USB, etc.). • Desarrollar un esquema metodológico de buenas prácticas para el almacenamiento seguro de la información. • Elaborar un procedimiento de manipulación y eliminación segura de documentos y dispositivos físicos.
Monitoreo y Vigilancia Física.	Se propondrán controles de monitoreo y seguimiento, basados en los lineamientos de la ISO/IEC 27001:2022, control A.7.4, para fortalecer la detección temprana de incidentes. **Objetivos tangibles:** • Construir un mapa de riesgo y puntos críticos para vigilancia. • Diseñar un cuadro comparativo de herramientas o métodos de monitoreo aplicables según la norma. • Crear un procedimiento de monitoreo y respuesta ante incidentes físicos (CCTV, bitácoras, revisión de grabaciones).
Capacitación y Concientización	Se desarrollará una propuesta de programa de sensibilización para fortalecer la cultura organizacional de seguridad. **Objetivos tangibles:** • Diseñar un cuadro estratégico de impacto organizacional sobre la cultura de seguridad. • Redactar un procedimiento de capacitación interna, que defina periodicidad, responsables y métodos de evaluación.
Diseño del Plan de Acción.	Se desarrollará un modelo metodológico de mejora para el SGSI, enfocado en la política de seguridad física y ambiental. Este plan definirá estrategias, fases y herramientas analíticas para su ejecución teórica dentro del contexto organizacional. **Objetivos tangibles:** • Elaborar un FODA organizacional que identifique fortalezas, debilidades, oportunidades y amenazas en materia de seguridad física. • Crear una matriz de acciones correctivas y preventivas basadas en los resultados del FODA. • Desarrollar un cuadro

	comparativo entre el estado actual y el nivel de madurez esperado del SGSI según ISO/IEC 27001:2022. • Diseñar un esquema estratégico de implementación teórica que detalle fases, responsables y tiempos estimados.
Seguimiento y Evaluación del Plan de Mejora Continua.	Se propone un sistema investigativo de evaluación continúa basado en indicadores teóricos de rendimiento (KPI), retroalimentación y revisión periódica, alineado a los principios del ciclo PHVA (Planificar– Hacer–Verificar– Actuar) de la ISO/IEC 27001:2022. **Objetivos tangibles:** • Elaborar una matriz de indicadores clave (KPI) para la medición del avance del SGSI. • Diseñar un plan de revisión periódica y retroalimentación documentado. • Desarrollar un cuadro comparativo de métodos de evaluación usados en SGSI similares. • Proponer un cronograma de evaluación teórico con tiempos y responsables estimados para el ciclo de mejora.

Fuente: Elaboración propia

Alcance Metodológico

Para el desarrollo de la presente investigación se adopta una metodología de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basada en los lineamientos establecidos en la norma ISO/IEC 27001:2022, complementada con la guía de controles definida en la ISO/IEC 27002:2022, lo cual permite estructurar de manera ordenada, sistemática y alineada a estándares internacionales cada una de las etapas del proceso investigativo. Este enfoque metodológico se fundamenta en las cláusulas 4 a 10 de la ISO/IEC 27001:2022, las cuales establecen los requisitos para la planificación, implementación, evaluación y mejora continua del sistema, integrando el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) como eje central del proceso.

A diferencia de enfoques tradicionales, esta metodología no se limita a la definición de controles aislados, sino que establece una secuencia estructurada de fases que permiten diagnosticar la situación actual de la organización, identificar y evaluar los riesgos, seleccionar los

controles adecuados, documentar los procesos y asegurar su seguimiento y mejora continua. De esta manera, se garantiza que la propuesta desarrollada responda de forma integral a las necesidades de la empresa Sauter Infomax S.A., asegurando su aplicabilidad y sostenibilidad en el tiempo.

La metodología se organiza en las siguientes fases:

Diagnóstico del contexto organizacional

En esta fase se realiza el análisis del contexto interno y externo de la organización, así como la identificación de las partes interesadas y sus necesidades, en cumplimiento de la Cláusula 4 de la ISO/IEC 27001:2022. Este diagnóstico permite comprender la situación actual de la empresa en materia de seguridad de la información y establecer las bases para la definición del alcance del SGSI.

Entregables: definición del contexto organizacional, identificación de partes interesadas y documento de alcance del SGSI.

Evaluación de riesgos de seguridad de la información

Con base en la Cláusula 6.1.2 de la norma, se realiza la identificación, análisis y valoración de los riesgos asociados a la seguridad física y del entorno, considerando amenazas, vulnerabilidades e impactos potenciales. Esta fase permite priorizar los riesgos y establecer criterios para su tratamiento.

Entregables: criterios de evaluación de riesgos y matriz de riesgos de seguridad de la información.

Evaluación de riesgos de seguridad de la información.

A partir de los riesgos identificados, se procede a la selección de controles de seguridad alineados con la ISO/IEC 27002:2022, asegurando que estos respondan de manera efectiva a los riesgos priorizados. Esta fase se fundamenta en la Cláusula 6.1.3 de la ISO/IEC 27001:2022, relacionada con el tratamiento de riesgos.

Entregables: Declaración de Aplicabilidad (SoA) y plan de tratamiento de riesgos.

Documentación e implementación.

En esta fase se desarrollan las políticas, procesos y procedimientos necesarios para la implementación de los controles seleccionados, incluyendo la política de seguridad física y del entorno y los procedimientos documentados asociados. Asimismo, se plantea la aplicación progresiva de dichos controles dentro de la organización.

Entregables: políticas de seguridad, procedimientos documentados y registros de implementación.

Evaluación del desempeño.

Se establecen mecanismos de seguimiento y evaluación de los controles implementados, mediante revisiones internas, verificación del cumplimiento y análisis de resultados, en concordancia con las Cláusulas 9 de la ISO/IEC 27001:2022. Esta fase permite determinar la eficacia del sistema y detectar oportunidades de mejora.

Entregables: informes de evaluación, evidencias de cumplimiento y registros de seguimiento.

Mejora continua

Finalmente, se desarrollan acciones orientadas a la mejora continua del SGSI, en cumplimiento de la Cláusula 10 de la norma, permitiendo la actualización de controles, la optimización de procesos y la adaptación del sistema a cambios organizacionales o del entorno. *Entregables:* plan de mejora continua y acciones correctivas documentadas.

En conjunto, esta metodología permite estructurar la investigación bajo un enfoque integral, en el cual cada fase genera productos concretos y verificables que respaldan la propuesta de implementación de controles de seguridad física y del entorno dentro del marco de un SGSI alineado con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Asimismo, la integración del ciclo PHVA garantiza que el sistema no sea estático, sino que evolucione continuamente, fortaleciendo la gestión de la seguridad física y del entorno y asegurando su alineación con los estándares internacionales establecidos en la ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Alcance Tecnológico

El alcance tecnológico de la presente investigación se orienta al análisis, evaluación y aprovechamiento de la infraestructura tecnológica existente en la empresa Sauter Infomax S.A., como soporte para la propuesta de implementación de la seguridad física y del entorno conforme a la norma ISO/IEC 27001:2022. Debido a que el proyecto corresponde a un estudio de carácter investigativo y documental, no contempla el desarrollo de nuevos sistemas informáticos ni la adquisición obligatoria de plataformas especializadas, sino que se enfoca en el uso estratégico de los recursos tecnológicos ya disponibles en la organización, tales como equipos de cómputo, servidores locales, redes internas, sistemas de almacenamiento, herramientas ofimáticas y plataformas administrativas.

La investigación abarca la revisión y utilización de sistemas de gestión documental, sistemas de videovigilancia, controles de acceso, dispositivos de monitoreo y mecanismos de respaldo de información, los cuales permiten el almacenamiento, control, resguardo y trazabilidad de los datos generados durante el desarrollo del estudio. Estos recursos tecnológicos constituyen un apoyo fundamental para la implementación de los controles relacionados con la seguridad física, ambiental y de la información, conforme a los lineamientos establecidos en la norma ISO/IEC 27001:2022.

El entorno tecnológico de trabajo comprende principalmente estaciones administrativas, servidores locales, infraestructura de red interna, sistemas de monitoreo y plataformas institucionales utilizadas para la gestión de procesos y comunicación interna. No se contempla el desarrollo de aplicaciones web, ni el uso de servidores externos, ni la contratación de servicios en la nube, ya que la propuesta se fundamenta en el fortalecimiento, optimización y aprovechamiento de los recursos tecnológicos internos existentes en la empresa.

Desde la perspectiva normativa, el uso de la infraestructura tecnológica actual permite respaldar la aplicación de los controles relacionados con la protección de activos, el control de accesos, el monitoreo de áreas críticas, la gestión segura de documentos físicos y digitales, y el respaldo de la información institucional. En este sentido, el alcance tecnológico se limita al soporte técnico necesario para la elaboración de matrices, procedimientos, diagnósticos, indicadores y planes de mejora, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de la información generada.

Finalmente, el enfoque tecnológico adoptado resulta pertinente y viable, debido a que promueve el aprovechamiento eficiente de la infraestructura existente, optimiza los recursos institucionales y asegura la sostenibilidad de la propuesta, sin requerir inversiones adicionales significativas en plataformas, servidores externos o desarrollos tecnológicos especializados.

CAPÍTULO II: MARCO REFERENCIAL

Introducción al Marco Referencial

El presente capítulo tiene como finalidad establecer los fundamentos teóricos, conceptuales y normativos que sustentan el desarrollo de la presente investigación, orientada a la implementación de la seguridad física y del entorno conforme a la norma ISO/IEC 27001:2022 en la empresa Sauter Infomax S.A. A través de la revisión de libros, artículos científicos, normas internacionales y documentos especializados, se busca fortalecer el sustento académico del estudio y garantizar la validez de la propuesta planteada.

En este apartado se analizan conceptos relacionados con la seguridad de la información, el Sistema de Gestión de Seguridad de la Información, la gestión de riesgos, la seguridad física, el control de accesos y los controles ambientales, los cuales resultan fundamentales para comprender la problemática abordada. Asimismo, se examina la estructura, los principios y los beneficios de la norma ISO/IEC 27001:2022 como marco de referencia para el diseño de la propuesta.

De igual forma, el marco referencial permite contextualizar el problema de investigación dentro del entorno organizacional de Sauter Infomax S.A., facilitando la interpretación de los resultados y la formulación de recomendaciones. Los contenidos desarrollados en este capítulo constituyen la base teórica que respalda el análisis, la metodología y las conclusiones del estudio, contribuyendo al fortalecimiento del rigor académico y metodológico del trabajo.

Seguridad de la Información

La seguridad de la información constituye un elemento esencial en el funcionamiento de las organizaciones modernas, debido a la creciente dependencia de los sistemas tecnológicos para la gestión de procesos administrativos y operativos. En este sentido, proteger los activos informacionales implica prevenir accesos no autorizados, alteraciones indebidas o pérdidas que

puedan comprometer la operación institucional. Laudon y Laudon señalan que “la seguridad de la información consiste en proteger los datos contra accesos no autorizados, alteraciones y destrucción” (2020, p. 213). Esta protección favorece la continuidad operativa y reduce riesgos asociados a fraudes, errores humanos o incidentes tecnológicos.

Uno de los fundamentos conceptuales más relevantes en este campo es la tríada CIA, integrada por los principios de confidencialidad, integridad y disponibilidad. La norma internacional establece que “la información debe protegerse para preservar su confidencialidad, integridad y disponibilidad” (ISO, 2022, p. 6). La confidencialidad garantiza que solo personas autorizadas accedan a la información; la integridad asegura la exactitud y consistencia de los datos; y la disponibilidad permite que la información esté accesible cuando se requiera. Estos principios constituyen la base para la definición de controles físicos, técnicos y administrativos.

La norma también enfatiza que la seguridad debe integrarse como parte de la gestión organizacional, indicando lo siguiente:

> La organización debe implementar controles apropiados para proteger la información frente a amenazas internas y externas, asegurando su confidencialidad, integridad y disponibilidad. Estos controles deben ser proporcionales al riesgo identificado y mantenerse bajo revisión continua para garantizar su eficacia. (ISO, 2022, p. 15)

Este enfoque evidencia que la seguridad no depende únicamente de soluciones tecnológicas, sino de una estructura organizacional que incorpore políticas, supervisión y evaluación permanente. La estructura general se presenta en la Figura 1.

Figura 1Triada CIA de la seguridad de la información

Fuente: Adaptado de *Definición de la tríada de la CIA: ejemplos de confidencialidad, integridad y disponibilidad*, por Wallarm, s.f. (https://lab.wallarm.com/what/definicion-de-la-triada-de-la-cia-ejemplos-de-confidencialidad-integridad-y-disponibilidad/?lang=es). Basado en Laudon y Laudon (2020).

Desde la perspectiva de la gestión integral, Calder afirma que "una gestión efectiva de la seguridad requiere integrar controles técnicos, físicos y administrativos" (2019, p. 85), destacando además que "la ausencia de políticas claras incrementa significativamente los riesgos organizacionales" (p. 92). Estas afirmaciones subrayan la importancia de establecer lineamientos institucionales formales que orienten la protección de los activos.

En relación con la documentación y control de procesos, Hernández Sampieri et al. indican que "la sistematización de la información facilita el control, el seguimiento y la evaluación de los procedimientos" (2018, p. 142), mientras que una adecuada documentación fortalece la transparencia institucional (p. 145). Estos elementos resultan esenciales para garantizar la trazabilidad de las acciones de seguridad.

En el contexto de Sauter Infomax S.A., la aplicación de estos principios fortalece la protección de activos informáticos, administrativos y documentales, permitiendo una gestión preventiva de riesgos. La implementación de controles alineados con ISO/IEC 27001:2022 favorece la continuidad operativa, el cumplimiento normativo y la consolidación de una cultura organizacional orientada a la protección integral de la información.

Propuesta de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO/IEC 27001:2022

El Sistema de Gestión de Seguridad de la Información (SGSI) constituye un marco estructurado de políticas, procedimientos y controles orientados a proteger los activos de información, garantizando su confidencialidad, integridad y disponibilidad. De acuerdo con la norma ISO/IEC 27001:2022, este sistema establece los requisitos para identificar, analizar y tratar los riesgos de seguridad de la información, promoviendo una gestión sistemática y alineada con los objetivos organizacionales.

El SGSI se fundamenta en el ciclo de mejora continua Planificar–Hacer–Verificar–Actuar (PHVA), el cual permite gestionar de manera dinámica los controles implementados, evaluar su eficacia y aplicar mejoras continuas conforme a los cambios del entorno organizacional. Este enfoque asegura que la seguridad de la información no sea un proceso estático, sino una práctica en constante evolución.

En el contexto de la empresa Sauter Infomax S.A., la presente propuesta se orienta a la estructuración de un SGSI enfocado en la seguridad física y del entorno, considerando la ausencia de políticas formales y la existencia de controles no documentados. En este sentido, la implementación del sistema se desarrolla de manera progresiva, iniciando con la definición del contexto organizacional, las partes interesadas y el alcance, conforme a lo establecido en la Cláusula 4 de la norma ISO/IEC 27001:2022.

La norma también enfatiza la necesidad de definir políticas formales, asignar responsabilidades claras y documentar procedimientos que regulen el manejo de la información. En este sentido, establece:

> La organización debe establecer, implementar y mantener políticas y procedimientos documentados que aseguren la gestión adecuada de la seguridad de la información, incluyendo la asignación de responsabilidades, la definición de controles y la evaluación periódica de su eficacia. Estos elementos deben integrarse dentro de la estructura organizacional para garantizar su cumplimiento y sostenibilidad. (ISO, 2022, p. 6)

Esta disposición evidencia que la gobernanza de la seguridad depende no solo de la tecnología, sino del compromiso institucional. Laudon y Laudon (2020) señalan que "la definición clara de funciones y responsabilidades reduce significativamente los riesgos derivados del error humano" (p. 312), reforzando la importancia de la estructura organizacional dentro del SGSI.

Asimismo, el sistema contempla la aplicación de controles técnicos, físicos y administrativos que protegen integralmente los activos de información. Hernández Sampieri et al. (2018) indican que la integración de mecanismos de prevención, monitoreo y respuesta permite a las organizaciones minimizar impactos operativos ante incidentes. Entre estos controles se incluyen la gestión de accesos, respaldo de información, monitoreo físico y planes de recuperación.

Análisis del Contexto Organizacional

En cumplimiento de la Cláusula 4.1, se identifican los factores internos y externos que influyen en la seguridad de la información dentro de la organización.

Contexto interno:

La empresa presenta una estructura organizacional pequeña, con aproximadamente 15 a 18 colaboradores. No cuenta con políticas formales de seguridad ni procedimientos documentados, lo que evidencia una gestión empírica de los controles. Asimismo, existe una alta dependencia de la infraestructura tecnológica y de los activos físicos para la operación diaria.

Se identifican riesgos asociados a accesos no autorizados, amenazas ambientales (fallas eléctricas, incendios), así como la necesidad de cumplir con estándares internacionales y responder a las exigencias de los clientes en materia de protección de la información.

Este análisis permite evidenciar la necesidad de estructurar un SGSI que fortalezca la protección de los activos organizacionales y reduzca las vulnerabilidades existentes.

Partes Interesadas

De acuerdo con la Cláusula 4.2, se identifican las partes interesadas relevantes y sus necesidades:

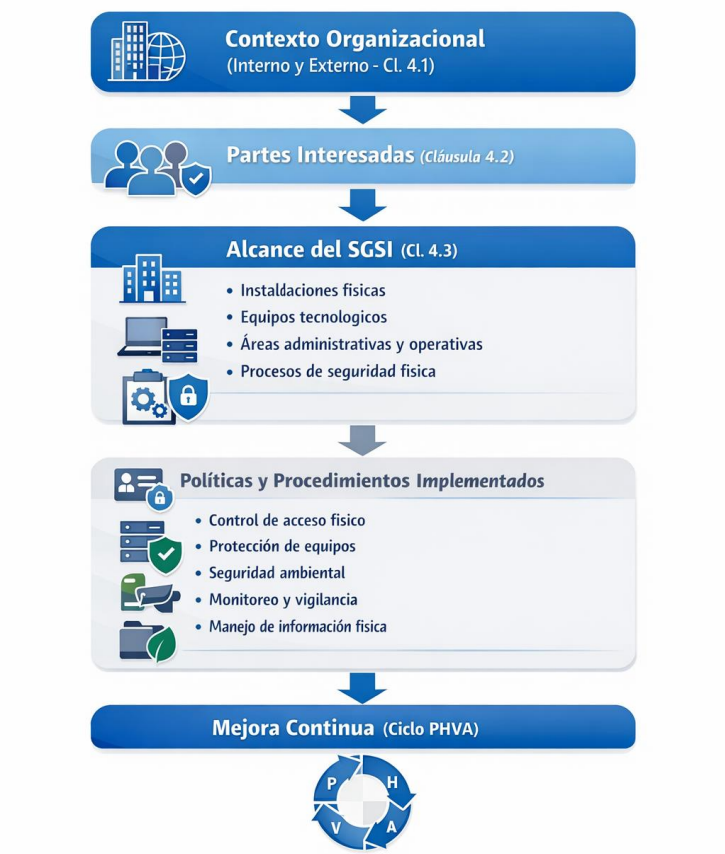
Tabla 6 Partes Interesadas

Parte interesada	Necesidad / Expectativa
Colaboradores	Seguridad en el entorno laboral
Clientes	Protección de la información
Empresa	Continuidad operativa
Proveedores	Acceso controlado a instalaciones
Entidades regulatorias	Cumplimiento normativo

Fuente: Elaboración propia, 2026

La identificación de estas partes permite orientar la propuesta de implementación de controles de seguridad física y del entorno dentro del marco de un SGSI alineado con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. hacia el cumplimiento de sus expectativas y requisitos.

Figura 2 Contexto Organizacional



Fuente: Elaboración propia, con la herramienta de canva, con base en la ISO/IEC 27001:2022 e ISO/IEC 27002:2022

Con base en la Cláusula 4.3, el alcance del SGSI se define considerando el contexto organizacional, las partes interesadas y los activos críticos de la empresa.

El alcance se enfoca en la seguridad física y del entorno, abarcando:

- Instalaciones físicas de la empresa
- Equipos tecnológicos y activos de información

- Áreas administrativas y operativas
- Procesos relacionados con la seguridad física y ambiental

Este alcance delimita claramente los límites del sistema, asegurando que los controles implementados se orienten a la protección de los activos críticos frente a riesgos físicos y ambientales.

Tabla 7 Mapa de Cobertura del SGSI

Elemento	Descripción	Incluido en el SGSI
Instalaciones físicas	Oficinas administrativas y áreas operativas	Sí
Equipos tecnológicos	Computadoras, dispositivos y sistemas	Sí
Información física	Documentos y archivos	Sí
Procesos internos	Procesos administrativos y operativos	Sí
Áreas externas	Espacios fuera del control de la empresa	No

Fuente: Elaboración propia, 2026

Procedimiento para la Definición y Gestión del Alcance del SGSI

El presente procedimiento establece los lineamientos para definir, documentar y mantener actualizado el alcance del SGSI en la empresa Sauter Infomax S.A.

La definición del alcance se realiza considerando:

- El análisis del contexto organizacional
- La identificación de partes interesadas
- La evaluación de activos críticos

El alcance deberá documentarse formalmente, especificando los límites del sistema y los elementos incluidos. Asimismo, se realizará una revisión periódica para asegurar su vigencia ante cambios organizacionales, tecnológicos o del entorno.

La responsabilidad de este proceso recae en la administración de la empresa, en conjunto con el personal encargado de la gestión de la seguridad de la información.

Integración con la Política y los Procedimientos

El alcance definido se encuentra directamente vinculado con la política y los procedimientos de seguridad física y del entorno desarrollados en la presente investigación, los cuales constituyen la base para la implementación de controles dentro de la organización. En este sentido, la propuesta del SGSI no parte de un sistema previamente implementado, sino de la construcción progresiva de sus elementos fundamentales, alineados con la norma ISO/IEC 27001:2022 y apoyados en las buenas prácticas de la ISO/IEC 27002:2022. La propuesta de implementación de controles de seguridad física y del entorno dentro del marco de un SGSI alineado con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. permite estructurar de manera integral la gestión de la seguridad de la información en la empresa Sauter Infomax S.A., mediante la definición del contexto organizacional, la identificación de partes interesadas y el establecimiento del alcance del sistema. Este enfoque se complementa con el desarrollo de políticas y procedimientos orientados a la seguridad física y del entorno, facilitando la implementación de controles, la reducción de riesgos y el fortalecimiento de la continuidad operativa, bajo un modelo de mejora continúa alineado con estándares internacionales.

Normas ISO/IEC 27001:2022 y ISO/IEC 27002:2022 aplicadas a la Seguridad Física y del Entorno

La norma ISO/IEC 27001:2022 establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información, proporcionando un marco estructurado para la gestión de riesgos organizacionales. Según ISO (2022), “esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información” (p. 1), lo cual permite integrar la seguridad en la estrategia institucional.

En relación con la estructura del sistema, la norma indica lo siguiente:

> La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de la información. Asimismo, debe identificar las partes interesadas pertinentes y los requisitos aplicables relacionados con la seguridad de la información. (ISO, 2022, p. 5)

Esta disposición evidencia que la seguridad no debe gestionarse de forma aislada, sino integrada al contexto organizacional, considerando factores internos, externos y normativos. Además, la norma establece que "los controles deben seleccionarse con base en el tratamiento de riesgos identificado" (ISO, 2022, p. 12), reforzando la relación directa entre análisis de riesgos y aplicación de medidas de protección.

Desde la perspectiva de los módulos abordados en la investigación, la ISO/IEC 27001:2022 se vincula directamente con el módulo de seguridad física y del entorno, el cual contempla controles orientados a la protección de instalaciones, equipos y áreas críticas. La norma señala que "las áreas seguras deben protegerse mediante controles de entrada apropiados para asegurar que únicamente el personal autorizado tenga acceso" (ISO, 2022, p. 21). Este requisito se relaciona con la necesidad de implementar controles de acceso físico, sistemas de videovigilancia y mecanismos de registro de visitantes en la empresa Sauter Infomax S.A. La estructura de la norma se organiza en cláusulas que establecen los requisitos para el diseño, implementación y evaluación del SGSI. Estas cláusulas abarcan aspectos relacionados con el contexto organizacional, liderazgo, planificación, operación, evaluación del desempeño y mejora continua.

Figura 3 Estructura de la Norma ISO/IEC 27001:2022

Fuente: Adaptado de *¿Qué es la norma ISO 27001 y para qué sirve?*, por Delta Protect, 2022 (https://www.deltaprotect.com/blog/que-es-iso-27001). CC BY-NC.

Asimismo, el estándar enfatiza la importancia de la mejora continua, indicando que "la organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información" (ISO, 2022, p. 18). Este principio se vincula con el módulo de evaluación y seguimiento desarrollado en la presente investigación, el cual propone estrategias de monitoreo y retroalimentación permanente para garantizar la vigencia de los controles implementados.

En complemento con la ISO/IEC 27001:2022, la ISO/IEC 27002:2022 desempeña un papel fundamental en la implementación del Sistema de Gestión de Seguridad de la Información, al proporcionar una guía detallada de controles que permiten operacionalizar los requisitos establecidos por la norma principal. Mientras la ISO/IEC 27001 define el marco de gestión, la ISO/IEC 27002 orienta la aplicación práctica de medidas de seguridad, facilitando la adopción de buenas prácticas alineadas con estándares internacionales.

En el contexto de la seguridad física y del entorno, la ISO/IEC 27002:2022 establece un conjunto de controles diseñados para proteger las instalaciones, los equipos y los activos de información frente a amenazas físicas y ambientales. Estos controles abarcan aspectos como la delimitación de áreas seguras, el establecimiento de perímetros de seguridad, la implementación de controles de acceso físico, la protección de equipos y la prevención de riesgos derivados de condiciones ambientales adversas.

De manera específica, la norma contempla la necesidad de restringir el acceso a áreas críticas mediante mecanismos de autenticación física, registros de ingreso y supervisión continua, con el fin de garantizar que únicamente el personal autorizado tenga acceso a los activos organizacionales. Asimismo, se enfatiza la importancia de ubicar los equipos en condiciones adecuadas que reduzcan su exposición a riesgos como fallas eléctricas, temperatura inadecuada, humedad o manipulación indebida, lo cual contribuye directamente a la preservación de la disponibilidad e integridad de la información.

Adicionalmente, la ISO/IEC 27002:2022 establece lineamientos relacionados con la protección contra amenazas ambientales, incluyendo la implementación de medidas de seguridad como sistemas contra incendios, control de energía eléctrica y condiciones de ventilación adecuadas. Estos controles permiten mitigar riesgos que podrían afectar la continuidad operativa de la organización, fortaleciendo así la resiliencia institucional frente a incidentes físicos.

Otro aspecto relevante de esta norma es la incorporación de mecanismos de monitoreo y vigilancia, los cuales permiten detectar de manera oportuna situaciones de riesgo dentro del entorno físico de la organización. La supervisión constante de las instalaciones, el control de accesos y el registro de incidentes constituyen prácticas esenciales para mantener un entorno seguro y controlado.

En el caso de la empresa Sauter Infomax S.A., la aplicación de los controles establecidos en la ISO/IEC 27002:2022 respalda directamente el desarrollo de políticas, procesos y procedimientos de seguridad física y del entorno, previamente definidos en la presente investigación. Estos controles permiten traducir los lineamientos teóricos de la ISO/IEC

27001:2022 en acciones concretas, tales como el control de acceso físico, la protección de equipos tecnológicos, la gestión ambiental y el monitoreo de las instalaciones.

De esta manera, la integración de ambas normas permite estructurar un enfoque integral de seguridad de la información, en el cual se establecen los requisitos del sistema de gestión y, simultáneamente, se definen los mecanismos operativos para su implementación. Esta complementariedad fortalece la capacidad de la organización para prevenir incidentes, reducir vulnerabilidades y garantizar la protección de sus activos físicos y de información, consolidando así una gestión alineada con las mejores prácticas internacionales.

Política y Procedimientos de Seguridad Física y del Entorno

La seguridad física y del entorno constituye un componente esencial dentro del Sistema de Gestión de Seguridad de la Información, ya que protege las instalaciones, equipos y activos organizacionales frente a accesos no autorizados, daños intencionales o incidentes ambientales. La protección de las áreas críticas permite reducir vulnerabilidades asociadas a amenazas internas y externas, garantizando la continuidad operativa de la organización. En este sentido, la seguridad física no solo complementa los controles tecnológicos, sino que forma parte integral de la gestión de riesgos institucional.

La norma ISO/IEC 27001:2022 establece controles específicos relacionados con la protección de instalaciones y áreas seguras. En el Anexo A se indica lo siguiente:

> Las áreas seguras deben protegerse mediante controles de entrada apropiados para asegurar que únicamente el personal autorizado tenga acceso. Las instalaciones deben diseñarse y mantenerse para proteger los activos contra daños físicos y ambientales, incluyendo incendios, inundaciones, fallas eléctricas u otras amenazas. (ISO, 2022, p. 21)

Este lineamiento evidencia la necesidad de implementar mecanismos de control de acceso físico, sistemas de videovigilancia, registros de visitantes y medidas de protección ambiental. Asimismo, la norma establece que "los equipos deben ubicarse y protegerse para reducir los riesgos derivados de amenazas ambientales y peligros físicos" (ISO, 2022, p. 23), reforzando la

importancia de la infraestructura adecuada y el mantenimiento preventivo. Los principales elementos que conforman la seguridad física y el control de accesos se ilustran en la Figura 3.

Figura 4 Elementos de Seguridad Física y Control de Accesos

Fuente: Adaptado de El punto en el que seguridad y ciberseguridad convergen, por INCIBE-CERT, 2021 (*https://www.incibe.es/incibe-cert/blog/el-punto-el-seguridad-y-ciberseguridad-convergen*). Basado en la norma ISO/IEC 27001:2022.

Desde una perspectiva complementaria, Calder (2019) señala que "la seguridad física es la primera línea de defensa en la protección de la información y los activos organizacionales" (p. 148), destacando que la ausencia de controles físicos adecuados puede comprometer incluso los sistemas tecnológicos más avanzados. Además, el autor indica que "los controles ambientales, como sistemas contra incendios y respaldo eléctrico, son fundamentales para garantizar la disponibilidad de la información" (p. 152), lo cual se relaciona directamente con el principio de disponibilidad de la tríada CIA.

En el marco de los módulos desarrollados en esta investigación, la seguridad física y del entorno se vincula con el análisis de riesgos, la implementación de controles y el seguimiento continuo de las condiciones ambientales. La evaluación de accesos, la delimitación de zonas críticas y el monitoreo de dispositivos constituyen acciones concretas orientadas al fortalecimiento del SGSI. Estos controles permiten prevenir incidentes que puedan afectar la integridad de los activos físicos y tecnológicos.

En el contexto de la empresa Sauter Infomax S.A., la aplicación de controles de seguridad física resulta fundamental para proteger áreas administrativas, bodegas, equipos informáticos y documentación sensible. La implementación de mecanismos de control de acceso, sistemas de vigilancia y protocolos de emergencia contribuye a reducir riesgos asociados a intrusiones, daños materiales o eventos ambientales. De esta manera, la organización fortalece su estructura de seguridad y consolida una gestión integral alineada con los requisitos de la norma ISO/IEC 27001:2022.

En complemento con la norma ISO/IEC 27001:2022, se consideran los lineamientos de la norma ISO/IEC 27002:2022, la cual proporciona un conjunto de controles de seguridad de la información que orientan la implementación práctica del Sistema de Gestión de Seguridad de la Información. En el ámbito de la seguridad física y del entorno, esta norma establece controles relacionados con la protección de áreas seguras, equipos, accesos físicos y monitoreo, permitiendo fortalecer la gestión de riesgos y la protección de los activos organizacionales.

En relación con los lineamientos establecidos por la norma ISO/IEC 27001:2022 y considerando la situación actual de la empresa Sauter Infomax S.A., donde no se evidencian políticas formales en materia de seguridad física, se propone el desarrollo de una política de seguridad física y del entorno como base para la implementación del Sistema de Gestión de Seguridad de la Información.

La empresa Sauter Infomax S.A. establece la presente política con el propósito de proteger sus instalaciones, equipos tecnológicos y activos de información frente a accesos no autorizados, daños físicos y amenazas ambientales, garantizando la continuidad de sus operaciones.

Para el cumplimiento de la presente política, la organización establece los siguientes lineamientos:

- Establecer controles de acceso físico a las instalaciones, limitando el ingreso únicamente a personal autorizado.
- Implementar mecanismos de registro y control de visitantes.

- Proteger los equipos tecnológicos mediante una adecuada ubicación y condiciones ambientales.
- Prevenir riesgos físicos mediante la implementación de medidas de seguridad, tales como sistemas de vigilancia y control.
- Garantizar condiciones ambientales adecuadas que protejan los activos frente a amenazas como fallas eléctricas, incendios o daños estructurales.
- Promover la concientización del personal en temas relacionados con la seguridad física y del entorno.

Esta política deberá ser comunicada a todo el personal y será revisada periódicamente como parte del proceso de mejora continua del SGSI.

Procesos y procedimientos de seguridad física y del entorno

Con base en los lineamientos establecidos en la norma ISO/IEC 27002:2022, se desarrollan los siguientes procedimientos orientados a la seguridad física y del entorno en la empresa Sauter Infomax S.A. Estos procedimientos permiten operacionalizar la política definida, estableciendo acciones concretas para la protección de los activos, el control de accesos y la gestión de riesgos físicos y ambientales dentro de la organización.

Procedimiento de Control de Acceso Físico

El presente procedimiento establece los lineamientos para regular el acceso a las instalaciones de la empresa Sauter Infomax S.A., con el propósito de prevenir el ingreso no autorizado y proteger los activos físicos y de información. En concordancia con los controles de la norma ISO/IEC 27001:2022, se define que únicamente el personal autorizado podrá ingresar a las áreas críticas de la organización, mediante mecanismos de identificación previamente establecidos. Asimismo, se deberá llevar un registro de visitantes, incluyendo datos como nombre, motivo de la visita, hora de ingreso y salida, con el fin de mantener trazabilidad sobre las personas que acceden a las instalaciones. Este procedimiento también contempla la delimitación de zonas restringidas, en las cuales el acceso será limitado según el nivel de responsabilidad del colaborador, garantizando así un control adecuado de la seguridad física.

Procedimiento de Protección de Equipos y Activos Tecnológicos

Este procedimiento tiene como objetivo garantizar la protección de los equipos tecnológicos y activos físicos frente a riesgos de daño, pérdida o acceso no autorizado. De acuerdo con la norma ISO/IEC 27001:2022, los equipos deben ubicarse en áreas seguras, con condiciones ambientales adecuadas que reduzcan la exposición a amenazas físicas. En este sentido, la empresa deberá asegurar que los dispositivos se encuentren protegidos contra factores como humedad, temperatura inadecuada, fallas eléctricas o manipulación indebida. Además, se establecerán lineamientos para el uso adecuado de los equipos por parte del personal, promoviendo el cuidado y la responsabilidad en el manejo de los recursos tecnológicos, así como la implementación de medidas básicas de protección física.

Procedimiento de Seguridad Ambiental

El presente procedimiento define las acciones orientadas a prevenir y mitigar riesgos derivados de condiciones ambientales que puedan afectar la infraestructura y los activos de la organización. En concordancia con la norma ISO/IEC 27001:2022, se deberán establecer medidas para proteger las instalaciones frente a amenazas como incendios, fallas eléctricas o condiciones inadecuadas del entorno. La empresa deberá garantizar la existencia de sistemas básicos de protección, tales como extintores, reguladores de voltaje y condiciones adecuadas de ventilación, así como realizar revisiones periódicas para asegurar su correcto funcionamiento. Este procedimiento busca preservar la disponibilidad de los activos y reducir el impacto de incidentes ambientales.

Procedimiento de Monitoreo y Vigilancia Física

Este procedimiento establece los mecanismos de supervisión y control necesarios para detectar oportunamente situaciones que puedan representar un riesgo para la seguridad física de la organización. En este sentido, se plantea la implementación de medidas de vigilancia, tales como la supervisión del ingreso y salida de personas, la revisión periódica de las instalaciones y el registro de incidentes relevantes. Asimismo, se deberá promover la responsabilidad del personal en la identificación y reporte de situaciones anómalas, fortaleciendo así la cultura de seguridad dentro

de la empresa. Este procedimiento permite mejorar la capacidad de respuesta ante posibles incidentes y contribuye al control continuo del entorno físico.

Procedimiento de Manejo y Resguardo de Información Física

El presente procedimiento tiene como finalidad establecer lineamientos para el manejo seguro de documentos físicos y otros medios de almacenamiento de información, garantizando su protección frente a pérdida, daño o acceso no autorizado. De acuerdo con los principios de la norma ISO/IEC 27001:2022, la información debe ser resguardada en condiciones que aseguren su confidencialidad, integridad y disponibilidad. En este sentido, la empresa deberá implementar prácticas adecuadas de almacenamiento, tales como el uso de archivadores, control de acceso a documentos sensibles y disposición segura de la información cuando ya no sea requerida. Este procedimiento fortalece la gestión documental y reduce riesgos asociados al manejo inadecuado de la información.

La definición de la política y los procedimientos descritos anteriormente permite establecer una base estructurada para la creación de un manual de seguridad física y del entorno en la empresa Sauter Infomax S.A. Este manual integra lineamientos, procesos y controles necesarios para la gestión de la seguridad física, facilitando su implementación, seguimiento y mejora continua dentro del Sistema de Gestión de Seguridad de la Información, en concordancia con los requisitos establecidos en la norma ISO/IEC 27001:2022 y los controles de la ISO/IEC 27002:2022.

Gestión de Riesgos

En cualquier organización, la seguridad no puede gestionarse sin una identificación previa de las amenazas que podrían afectar sus activos. La gestión de riesgos permite anticipar escenarios adversos y establecer medidas preventivas antes de que ocurran incidentes que comprometan la información o la infraestructura física. Este proceso se convierte en el eje articulador entre los controles establecidos por la norma ISO/IEC 27001:2022 y la realidad operativa de la empresa.

La norma establece que el análisis de riesgos debe realizarse de manera estructurada y documentada, considerando el impacto potencial sobre la confidencialidad, integridad y disponibilidad de la información. En este sentido, señala:

> La organización debe definir y aplicar un proceso de evaluación de riesgos de la seguridad de la información que establezca y mantenga criterios de riesgo, identifique los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información, y determine el nivel de riesgo correspondiente. (ISO, 2022, p. 10)

Lo anterior implica que el riesgo no puede evaluarse de forma subjetiva o informal, sino mediante criterios previamente establecidos que permitan obtener resultados coherentes y comparables. La definición de niveles de impacto y probabilidad facilita clasificar los riesgos según su criticidad y priorizar aquellos que puedan afectar significativamente la operación institucional. Además, la norma indica que "la organización debe aplicar un proceso de tratamiento de riesgos para seleccionar las opciones apropiadas" (ISO, 2022, p. 11), lo que obliga a tomar decisiones estratégicas sobre la mitigación, transferencia, aceptación o eliminación de los riesgos identificados.

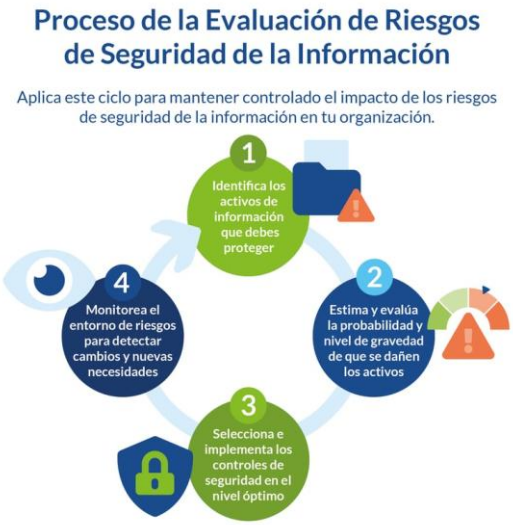
Desde una perspectiva técnica, Calder (2019) advierte que "la evaluación de riesgos constituye la base para la selección de controles efectivos dentro del SGSI" (p. 103), resaltando que una mala identificación puede conducir a medidas inadecuadas o insuficientes. Esta afirmación refuerza la importancia de vincular el análisis de riesgos con los controles físicos y ambientales desarrollados en los módulos anteriores, particularmente en lo relativo a accesos físicos, protección de equipos, almacenamiento de documentación y condiciones del entorno.

Asimismo, la gestión de riesgos no se limita a identificar amenazas, sino que implica establecer un proceso continuo de revisión y actualización frente a cambios internos o externos. Las modificaciones en infraestructura, incorporación de nuevos equipos o variaciones en los procesos operativos pueden generar nuevos escenarios de riesgo que deben evaluarse oportunamente. Este enfoque dinámico garantiza que el sistema de seguridad se mantenga alineado con la realidad organizacional y con los requisitos establecidos por la norma ISO/IEC 27001:2022.

En el caso de Sauter Infomax S.A., la aplicación de este proceso permite identificar riesgos asociados a accesos no autorizados en áreas críticas, fallas eléctricas que afecten los servidores o incidentes ambientales que comprometan documentación sensible. La utilización de matrices de riesgo y registros formales facilita documentar cada etapa del análisis y sustentar las decisiones

adoptadas. El proceso de gestión de riesgos comprende etapas como identificación, análisis, evaluación y tratamiento, las cuales se representan de forma estructurada en la Figura 4.

Figura 5
Proceso de Evaluación de Riesgos de Seguridad de la Información



Fuente: Adaptado or Innevo, 2022 (https://innevo.com/blog/ la norma ISO/IEC 27001:2022.

Una vez analizados los riesgos, se procede a su evaluación, la cual consiste en compararlos con criterios previamente establecidos para determinar su nivel de aceptabilidad. En función de los resultados obtenidos, la organización puede optar por diversas estrategias de tratamiento, tales como la mitigación, transferencia, aceptación o eliminación del riesgo. Laudon y Laudon (2020) indican que la selección adecuada de estas estrategias permite reducir la exposición a amenazas y fortalecer la estabilidad operativa.

Por lo tanto, la gestión de riesgos debe ser un proceso continuo y dinámico, sujeto a revisiones periódicas y actualizaciones constantes. Hernández Sampieri et al. (2018) señalan que el monitoreo permanente facilita la detección temprana de cambios en el entorno organizacional, tecnológico y normativo, permitiendo ajustar oportunamente los controles implementados. De esta manera, se promueve una cultura preventiva orientada a la mejora continua.

En la implementación de la empresa Sauter Infomax S.A., la aplicación de un modelo estructurado de gestión de riesgos permitirá identificar oportunamente las amenazas relacionadas con la seguridad física, ambiental y tecnológica. Asimismo, facilitará el diseño de planes de contingencia, protocolos de respuesta y mecanismos de control que contribuyan a la protección integral de los activos institucionales. De esta forma, la organización fortalece su capacidad de adaptación, resiliencia y cumplimiento normativo conforme a la norma ISO/IEC 27001:2022.

Controles de Seguridad Física y Ambiental

Los controles de seguridad física y ambiental constituyen un componente esencial dentro del Sistema de Gestión de Seguridad de la Información, ya que permiten proteger los activos organizacionales frente a amenazas que pueden materializarse a través del entorno físico. La norma ISO/IEC 27001:2022 establece que la protección no debe limitarse únicamente a los sistemas digitales, sino que debe abarcar instalaciones, equipos, áreas críticas y condiciones ambientales que puedan afectar la continuidad operativa. En este sentido, la seguridad física se convierte en un elemento complementario de la seguridad lógica, formando un sistema integral orientado a la reducción de riesgos organizacionales.

La norma establece lo siguiente:

> Las áreas seguras deben protegerse mediante controles de entrada apropiados para asegurar que únicamente el personal autorizado tenga acceso. Los equipos deben protegerse contra amenazas físicas y ambientales, tales como incendios, inundaciones, fallas eléctricas y otras condiciones que puedan interrumpir las operaciones. (ISO, 2022, p. 21)

Esta disposición evidencia que la protección física no se limita a la restricción de accesos, sino que incluye la prevención de incidentes ambientales que puedan comprometer la disponibilidad de la información. Además, la norma indica que “los equipos deben ubicarse y protegerse para reducir los riesgos derivados de amenazas y peligros ambientales” (ISO, 2022, p. 22), reforzando la necesidad de adoptar medidas estructurales, técnicas y administrativas que respalden la seguridad organizacional.

Desde una perspectiva técnica, Whitman y Mattord (2021) señalan que “la seguridad física constituye la primera línea de defensa en cualquier programa de seguridad de la información” (p.

156), lo cual demuestra que, sin controles físicos adecuados, los controles lógicos pueden verse fácilmente vulnerados. Esta afirmación se vincula directamente con el módulo de Seguridad Física y del Entorno desarrollado en la presente investigación, el cual propone la implementación de controles como sistemas de videovigilancia, registros de visitantes, delimitación de zonas restringidas y protección ambiental de equipos tecnológicos.

El enfoque de seguridad física también se relaciona con el módulo de Gestión de Riesgos, dado que la selección de controles debe responder a amenazas previamente identificadas dentro del análisis institucional. Asimismo, guarda relación con el módulo de Evaluación y Seguimiento, ya que la efectividad de los controles implementados debe revisarse periódicamente mediante auditorías internas e indicadores de desempeño. En el caso de Sauter Infomax S.A., la implementación estructurada de estos controles permitirá fortalecer la protección de sus instalaciones comerciales y áreas técnicas, reduciendo vulnerabilidades asociadas a accesos no autorizados y riesgos ambientales.

El conjunto de controles físicos y ambientales puede clasificarse en controles preventivos, detectivos y correctivos, los cuales actúan de manera complementaria para garantizar la protección integral de los activos. Entre ellos se incluyen controles de acceso físico, cerraduras electrónicas, sistemas biométricos, cámaras de vigilancia, sistemas contra incendios, reguladores de voltaje y planes de contingencia ambiental.

Auditoria de Seguridad

La auditoría de seguridad constituye un mecanismo fundamental dentro de los sistemas de gestión, ya que permite evaluar de manera objetiva el cumplimiento de políticas, controles y procedimientos establecidos para la protección de la información. En el contexto de la seguridad física y del entorno, la auditoría permite verificar no solo la existencia de controles, sino también su eficacia, pertinencia y correcta aplicación dentro de la organización.

Dentro de un Sistema de Gestión de Seguridad de la Información (SGSI) completo, la auditoría interna cumple una función estratégica orientada a la mejora continua, permitiendo identificar desviaciones, brechas de cumplimiento y oportunidades de fortalecimiento. La norma ISO/IEC 27001:2022 establece que:

"La organización debe realizar auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de seguridad de la información: a) es conforme con los requisitos propios de la organización y con los requisitos de esta norma; y b) se implementa y mantiene eficazmente" (ISO, 2022, p. 17).

No obstante, es importante señalar que este requisito aplica cuando el SGSI se encuentra implementado de manera integral en toda la organización, ya que la auditoría forma parte de un sistema transversal que abarca todos los procesos, activos y áreas organizacionales.

En el caso de la presente investigación, la propuesta se enfoca específicamente en el diseño de políticas, procedimientos y controles relacionados con la seguridad física y del entorno, por lo que no contempla la implementación completa del SGSI ni un proceso formal de auditoría bajo certificación ISO. No obstante, la propuesta busca contribuir al fortalecimiento gradual de la seguridad de la información dentro de la organización, mediante la adopción progresiva de controles y buenas prácticas alineadas con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

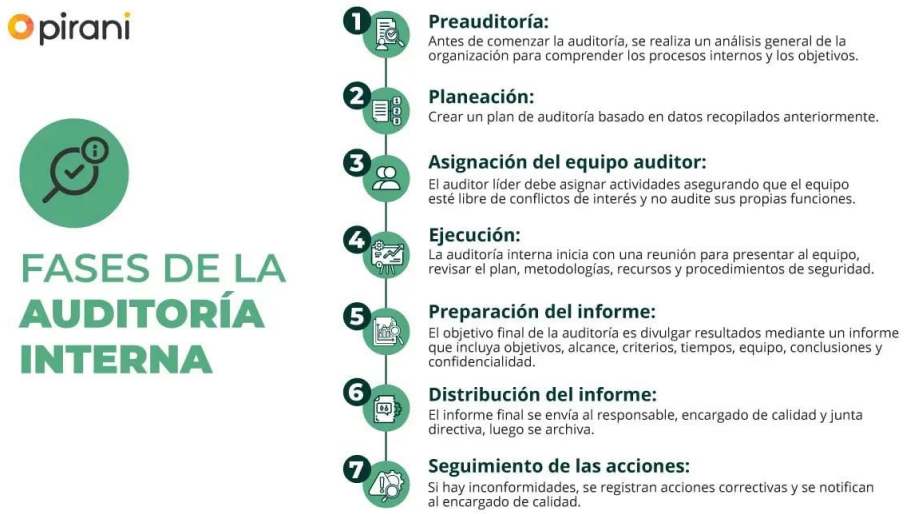
Sin embargo, se recomienda que la empresa Sauter Infomax S.A., como parte de una fase futura de madurez en la gestión de la seguridad de la información, considere la implementación de auditorías internas como mecanismo de evaluación y mejora continua. Estas auditorías permitirían:

- Verificar el cumplimiento de los controles físicos implementados.
- Evaluar la efectividad de los procedimientos establecidos.
- Identificar oportunidades de mejora en la gestión de la seguridad.
- Fortalecer progresivamente las prácticas organizacionales relacionadas con la seguridad de la información.

De manera complementaria, se sugiere que estas evaluaciones se realicen mediante revisiones periódicas internas, listas de verificación y seguimiento de incidentes, como un primer paso hacia la adopción de prácticas formales de auditoría alineadas con la norma ISO/IEC 27001:2022.

En este sentido, la auditoría de seguridad se plantea como una recomendación estratégica a futuro, orientada a fortalecer la gestión organizacional de la seguridad y servir como referencia para futuras iniciativas relacionadas con la adopción de estándares internacionales.

Figura 6 Fases de la auditoría interna



Fuente: Adaptado de ¿Cuáles son las etapas de una auditoría interna? | Blog Pirani (https://www.piranirisk.com/es/blog/etapas-y-fases-de-la-auditoria-interna).

Cumplimiento Legal

El cumplimiento legal constituye un componente esencial dentro de cualquier Sistema de Gestión de Seguridad de la Información, ya que garantiza que las políticas, procedimientos y controles implementados por la organización se ajusten a las disposiciones normativas vigentes. En el ámbito de la seguridad física y del entorno, el marco legal regula aspectos relacionados con la protección de datos, el resguardo de activos, la privacidad, la responsabilidad institucional y la prevención de incidentes que puedan generar consecuencias jurídicas o sanciones administrativas.

La norma ISO/IEC 27001:2022 incorpora el cumplimiento legal como un requisito obligatorio dentro del SGSI. Al respecto, establece:

> La organización debe determinar y tener acceso a los requisitos legales, reglamentarios y contractuales aplicables relacionados con la seguridad de la información y debe asegurarse de que estos requisitos se tengan en cuenta al establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información (ISO, 2022, p. 6).

Esta disposición evidencia que la seguridad de la información no puede gestionarse de manera aislada del entorno jurídico, sino que debe integrarse a las obligaciones legales que rigen la operación organizacional. Asimismo, el incumplimiento de dichos requisitos puede generar sanciones económicas, pérdida de reputación institucional o responsabilidades civiles.

En el contexto costarricense, el cumplimiento legal se vincula directamente con la Ley N.º 8968, Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, la cual establece principios como confidencialidad, seguridad y uso adecuado de la información. Dicha normativa dispone que los responsables del tratamiento deben adoptar medidas técnicas y organizativas que garanticen la protección de los datos personales contra acceso no autorizado o pérdida accidental. Este marco legal se relaciona con los controles físicos, ambientales y tecnológicos desarrollados en la presente investigación.

Desde una perspectiva técnica, Calder (2019) señala que "el incumplimiento legal en materia de seguridad de la información puede representar uno de los riesgos más significativos para una organización" (p. 142), debido a que involucra consecuencias regulatorias y contractuales. Por esta razón, la gestión del cumplimiento debe formar parte integral del análisis de riesgos y del proceso de auditoría interna.

En el caso de Sauter Infomax S.A., el cumplimiento legal implica asegurar que los accesos físicos a instalaciones estén debidamente controlados, que la documentación sensible se resguarde conforme a normativa vigente y que los registros de incidentes se mantengan como evidencia ante eventuales revisiones externas. De esta manera, la empresa no solo fortalece su estructura de seguridad, sino que también reduce la exposición a contingencias jurídicas.

Clasificación y Protección de Activos de Información

La clasificación y protección de activos de información constituye un proceso fundamental dentro de la seguridad física y del entorno, ya que permite identificar, valorar y resguardar los recursos que soportan las operaciones organizacionales. Un activo no se limita únicamente a datos digitales, sino que incluye equipos, documentación física, infraestructura tecnológica, dispositivos de almacenamiento y cualquier recurso que contenga o procese información crítica.

La norma ISO/IEC 27001:2022 establece que la organización debe identificar sus activos y definir niveles de protección adecuados según su valor, criticidad y sensibilidad. Esto implica que no todos los activos requieren el mismo nivel de seguridad, sino que deben clasificarse para aplicar controles proporcionales al riesgo.

> La información y otros activos asociados deben identificarse y clasificarse de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la organización (ISO, 2022, p. 14).

Este principio permite priorizar recursos de protección física, ambiental y administrativa, evitando la aplicación indiscriminada de controles que podrían resultar ineficientes.

Desde una perspectiva operativa, la clasificación de activos se realiza mediante criterios que facilitan su gestión dentro del Sistema de Seguridad. La Tabla 3 presenta un esquema de clasificación aplicable al contexto organizacional.

Tabla 8 Clasificación de Activos de Información según Nivel de Criticidad

Tipo de Activo	Ejemplo Organizacional	Nivel de Clasificación	Impacto ante pérdida	Medidas de Protección
Documentación física crítica	Contratos, registros internos	Alta	Legal y operativo	Archivo seguro, control de acceso

Equipos tecnológicos	Servidores, estaciones administrativas	Alta	Interrupción operativa	Protección eléctrica y ambiental
Información administrativa	Reportes internos	Media	Afectación organizacional	Control de usuarios
Material operativo	Manuales internos	Baja	Impacto limitado	Almacenamiento básico

Fuente: Elaboración propia con base en criterios de ISO/IEC 27001:2022.

Una vez clasificados los activos, es necesario establecer mecanismos de protección coherentes con el nivel asignado. Whitman y Mattord señalan que:

> La clasificación de activos permite asignar controles de seguridad apropiados, asegurando que los recursos más críticos reciban protección prioritaria (2021, p. 141).

Esto refuerza la relación entre clasificación, gestión de riesgos y seguridad física.

La Tabla 5 muestra una matriz de relación entre clasificación de activos y controles de protección física y ambiental.

Tabla 9 Relación entre Clasificación de Activos y Controles de Protección

Nivel de Clasificación	**Control de Acceso Físico**	**Protección Ambiental**	**Monitoreo**	**Respaldo**

Alta	Restringido	Completo	Permanente	Obligatorio
Media	Supervisado	Preventivo	Periódico	Recomendado
Baja	General	Básico	Eventual	Opcional

Fuente: Elaboración propia.

En el contexto de Sauter Infomax S.A., la clasificación de activos permite priorizar la protección de servidores locales, documentación operativa y equipos críticos, reduciendo la exposición a incidentes físicos o ambientales. Este enfoque facilita la asignación eficiente de recursos de seguridad y fortalece la gestión preventiva.

En consecuencia, la clasificación de activos no debe entenderse únicamente como un ejercicio administrativo, sino como una herramienta estratégica que vincula la gestión de riesgos, la protección física y la sostenibilidad operativa de la organización.

CAPITULO III: MARCO METODOLÓGICO

Enfoques de Investigación

La definición del enfoque de investigación constituye una etapa fundamental dentro del diseño metodológico, ya que orienta la forma en que se recolectarán, analizarán e interpretarán los datos. En estudios relacionados con la seguridad de la información, la elección del enfoque debe responder a la necesidad de comprender procesos técnicos, organizacionales y de gestión que influyen en la protección de los activos informativos. En este sentido, el enfoque metodológico determina la estructura del análisis, el tipo de instrumentos empleados y la naturaleza de los resultados obtenidos.

En relación con el enfoque cuantitativo, se reconoce su utilidad para medir variables y evaluar comportamientos observables dentro de una organización. Sobre este enfoque, Metodología de la investigación establece lo siguiente:

“El enfoque cuantitativo utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer patrones de comportamiento y probar teorías.” (Hernández Sampieri et al., 2022, p. 4)

Esta perspectiva resulta pertinente cuando se requiere evaluar niveles de cumplimiento, frecuencia de incidentes o indicadores de desempeño relacionados con controles de seguridad.

Por otra parte, el enfoque cualitativo permite examinar fenómenos desde una perspectiva interpretativa, considerando el contexto organizacional y las prácticas internas. Al respecto, los autores señalan:

"El enfoque cualitativo se basa en métodos de recolección de datos no estandarizados ni completamente predeterminados, con el propósito de explorar y comprender significados." (Hernández Sampieri et al., 2022, p. 9)

Este enfoque facilita el análisis de políticas, procedimientos y cultura organizacional vinculada a la seguridad de la información, aspectos esenciales dentro de un Sistema de Gestión de Seguridad de la Información.

La integración de ambos enfoques da lugar al enfoque mixto, el cual combina medición objetiva con interpretación contextual. Según Hernández Sampieri et al. (2022):

"Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos." (p. 612)

Este planteamiento permite abordar fenómenos complejos desde múltiples perspectivas, lo cual resulta especialmente útil en investigaciones que involucran gestión de riesgos, evaluación de controles y análisis organizacional.

Enfoque Cuantitativo

El enfoque cuantitativo se fundamenta en la medición objetiva de variables y el uso de procedimientos estadísticos para analizar fenómenos de manera sistemática. Este enfoque busca producir resultados verificables que permitan establecer patrones y relaciones entre variables. Según Metodología de la investigación:

"El enfoque cuantitativo utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer patrones de comportamiento y probar teorías." (Hernández Sampieri et al., 2022, p. 4)

Esta definición evidencia que el enfoque cuantitativo se orienta hacia la precisión, la objetividad y la replicabilidad de los resultados. En el contexto de la presente investigación, este

enfoque permite medir indicadores relacionados con riesgos, cumplimiento de controles y desempeño del Sistema de Gestión de Seguridad de la Información (SGSI), facilitando la evaluación estructurada de la seguridad física y del entorno.

Enfoque Cualitativo

El enfoque cualitativo se orienta a comprender fenómenos desde la perspectiva de los participantes, priorizando la interpretación de significados, percepciones y contextos organizacionales. Este enfoque busca explorar la realidad de manera profunda, reconociendo la complejidad de los procesos humanos y sociales involucrados. Según Metodología de la investigación, el enfoque cualitativo "se fundamenta en la recolección de datos no numéricos con el propósito de comprender los fenómenos desde la perspectiva de los participantes en su ambiente natural" (p. 7). Esta aproximación permite analizar dinámicas internas, prácticas organizacionales y comportamientos relacionados con la seguridad.

En el ámbito de la seguridad física y del entorno, el enfoque cualitativo facilita la identificación de percepciones del personal, cultura organizacional, cumplimiento de procedimientos y factores humanos que influyen en la protección de activos. A través de entrevistas, observaciones y análisis documental, es posible comprender cómo se aplican los controles en la práctica. Hernández Sampieri et al. destacan que este enfoque privilegia la interpretación contextual, lo cual resulta esencial cuando se estudian procesos organizacionales complejos (2018, p. 9). Por ello, su aplicación contribuye a fortalecer la dimensión humana del SGSI y a diseñar estrategias de mejora alineadas con la realidad institucional.

Enfoque Mixto

El enfoque mixto integra procedimientos cuantitativos y cualitativos para lograr una comprensión más amplia del fenómeno investigado. Esta combinación metodológica permite contrastar mediciones objetivas con interpretaciones contextuales. De acuerdo con Hernández Sampieri et al.:

"Los métodos mixtos implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta para realizar inferencias." (Hernández Sampieri et al., 2022, p. 534)

Esta integración fortalece la validez de los resultados al permitir la triangulación de información. En el desarrollo de esta investigación, el enfoque mixto resulta pertinente porque posibilita medir indicadores de seguridad y, al mismo tiempo, analizar factores organizacionales y humanos relacionados con la protección física y ambiental de los activos.

Enfoque de Investigación Seleccionado

Para el desarrollo del presente estudio orientado al fortalecimiento del Sistema de Gestión de Seguridad de la Información en Sauter Infomax S.A., se adopta el **enfoque mixto**, debido a su capacidad para integrar mediciones objetivas con análisis interpretativo. Desde el componente cuantitativo se evaluarán indicadores relacionados con controles físicos y ambientales, mientras que el componente cualitativo permitirá examinar procesos internos, documentación institucional y prácticas de seguridad existentes.

La adopción de este enfoque responde a la necesidad de obtener una visión integral del estado de la seguridad organizacional, permitiendo relacionar evidencia medible con análisis contextual. Esta integración favorece la formulación de propuestas fundamentadas, alineadas con los principios de gestión establecidos en la International Organization for Standardization, particularmente en lo referente a la gestión sistemática de riesgos y controles dentro del SGSI.

Tabla 10 Enfoque comparativo.

Enfoque	Propósito principal	Aplicación en el SGSI
Cuantitativo	Medición objetiva de variables	Evaluar cumplimiento de controles
Cualitativo	Comprensión de procesos organizacionales	Analizar políticas y prácticas
Mixto	Integración de medición e interpretación	Diagnóstico integral de seguridad

*Fuente***:** Elaboración propia, 2026

Tipos de Investigación

Los tipos de investigación constituyen clasificaciones metodológicas que permiten definir el alcance, propósito y nivel de profundidad de un estudio. Su selección orienta la forma en que se analiza el fenómeno investigado, así como los procedimientos utilizados para la obtención de información. De acuerdo con Metodología de la investigación:

"Los tipos de investigación se clasifican según el alcance que tengan los estudios, pudiendo ser exploratorios, descriptivos, correlacionales o explicativos." (Hernández Sampieri et al., 2022, p. 90)

Investigación Exploratoria

Esta clasificación facilita la organización del proceso investigativo y permite seleccionar el enfoque más adecuado de acuerdo con los objetivos planteados. En el contexto de la presente investigación, la elección del tipo de estudio resulta fundamental para analizar la seguridad física y del entorno dentro del Sistema de Gestión de Seguridad de la Información.

La investigación exploratoria se emplea cuando el fenómeno de estudio presenta poca información previa o requiere un primer acercamiento analítico. Hernández Sampieri et al. establecen:

"Los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes." (Hernández Sampieri et al., 2022, p. 91)

Este tipo de investigación permite identificar condiciones actuales, riesgos potenciales y oportunidades de mejora en materia de seguridad física y ambiental, proporcionando una base diagnóstica inicial.

Investigación Descriptiva

La investigación descriptiva tiene como finalidad detallar características, procesos y situaciones observables dentro del fenómeno analizado. Según Hernández Sampieri et al.:

> "Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, procesos u objetos que se sometan a análisis." (Hernández Sampieri et al., 2022, p. 92)

Este enfoque favorece la documentación estructurada de políticas, controles y procedimientos de seguridad existentes dentro de la organización.

Investigación Correlacional

La investigación correlacional se orienta a identificar asociaciones entre variables sin establecer relaciones de causa directa. Hernández Sampieri et al. señalan:

> Los estudios correlacionales tienen como finalidad conocer la relación o grado de asociación que exista entre dos o más variables en un contexto particular. (Hernández Sampieri et al., 2022, p. 93)

Este tipo de estudio permite analizar la relación entre factores organizacionales, controles de seguridad y gestión de riesgos.

Tipo de investigación Seleccionado

La presente investigación adopta un enfoque exploratorio–descriptivo, debido a que busca examinar las condiciones actuales de seguridad física y ambiental dentro de la empresa, así como documentar los procesos relacionados con la protección de activos. El carácter exploratorio facilita la identificación de brechas y riesgos, mientras que el enfoque descriptivo permite estructurar la información necesaria para el diseño de propuestas alineadas con la norma ISO/IEC 27001:2022.

Este enfoque se fundamenta en los lineamientos establecidos en la norma ISO/IEC 27001:2022, particularmente en sus cláusulas 4.1 a 4.4 relacionadas con el contexto de la organización, así como en la cláusula 6.1.2 referente a la evaluación de riesgos. Asimismo, se apoya en los controles definidos en la norma ISO/IEC 27002:2022, los cuales permiten establecer criterios prácticos para evaluar el nivel de cumplimiento de la organización en materia de seguridad física.

El levantamiento de información tiene como finalidad identificar la situación actual de la empresa Sauter Infomax S.A., detectar debilidades en los controles existentes y generar insumos para la posterior elaboración de la matriz de riesgos, la selección de controles y el diseño de la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI).

Las variables de investigación se definen en función de los objetivos específicos del estudio y se relacionan directamente con los controles de seguridad física y del entorno establecidos en la norma ISO/IEC 27002:2022. Estas variables permiten evaluar el nivel de implementación, cumplimiento y efectividad de los controles dentro de la organización.

A continuación, se presenta la relación entre instrumentos, variables, ítems evaluados, controles asociados y evidencia esperada:

Tabla 11 Matriz de relación: Instrumento – Variable – Control – Evidencia

Instrumento	Variable	Ítem / Pregunta	Control ISO/IEC 27002:2022	Evidencia esperada
Encuesta a colaboradores	Control de acceso físico	¿El acceso a las instalaciones está restringido al personal autorizado?	Control de acceso físico a áreas seguras	Registros de acceso, llaves, tarjetas
Encuesta a colaboradores	Registro de visitantes	¿Se lleva control de ingreso y salida de visitantes?	Gestión de visitantes	Bitácoras o registros físicos
Observación directa	Protección de equipos	¿Los equipos están ubicados en condiciones seguras?	Protección de equipos	Ubicación adecuada, condiciones ambientales

Observación directa	Seguridad ambiental	¿Existen medidas contra incendios o fallas eléctricas?	Protección contra amenazas ambientales	Extintores, reguladores, ventilación
Entrevista	Monitoreo y vigilancia	¿Se realizan controles o supervisión de las instalaciones?	Monitoreo físico	Reportes o registros de supervisión
Revisión documental	Gestión documental física	¿Se protegen los documentos físicos sensibles?	Protección de información física	Archivadores, control de acceso

Fuente: Elaboración propia,2026

Procedimiento de Aplicación de Instrumentos

El proceso de recolección de información se llevará a cabo mediante la aplicación de técnicas cualitativas y cuantitativas, garantizando la obtención de datos confiables y relevantes para el diagnóstico del SGSI.

Responsable:

La aplicación de los instrumentos estará a cargo de la investigadora, Mariana de los Ángeles Chinchilla Murillo.

Población objetivo:

Colaboradores de la empresa Sauter Infomax S.A., incluyendo personal administrativo y operativo.

Técnicas utilizadas:

- Encuestas estructuradas
- Entrevistas semiestructuradas
- Observación directa

- Revisión documental

Duración:

El proceso de levantamiento de información tendrá una duración aproximada de 2 a 3 semanas.

Validación de instrumentos:

Se realizará una prueba piloto con un grupo reducido de colaboradores, con el fin de validar la claridad, pertinencia y comprensión de los instrumentos antes de su aplicación definitiva.

Procesamiento de la información:

Los datos recolectados serán analizados mediante matrices de diagnóstico, permitiendo identificar brechas existentes entre la situación actual de la organización y los controles establecidos en la norma ISO/IEC 27002:2022.

El levantamiento de información constituye una fase fundamental dentro de la metodología de la propuesta de implementación de controles de seguridad física y del entorno dentro del marco de un SGSI alineado con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. ya que permite:

- Identificar el estado actual de la seguridad física y del entorno
- Detectar vulnerabilidades y riesgos asociados
- Generar evidencia para la evaluación de riesgos (ISO 27001:2022, cláusula 6.1.2)
- Facilitar la selección de controles adecuados (ISO 27002:2022)
- Fundamentar la elaboración de la Declaración de Aplicabilidad (SoA)

De esta manera, el diagnóstico obtenido no solo permite comprender la situación de la organización, sino que también establece una base sólida para la toma de decisiones y la implementación de mejoras dentro del Sistema de Gestión de Seguridad de la Información

Asimismo, se define un procedimiento de aplicación de los instrumentos, en el cual se establece quién realiza el levantamiento de información, a qué población va dirigido, el tiempo estimado de aplicación y el método de validación. En este caso, los instrumentos serán aplicados

por la investigadora a los colaboradores de la empresa Sauter Infomax S.A., mediante encuestas y observación directa, con una duración aproximada de 20 a 30 minutos por participante. Previamente, se realizará una validación piloto con el fin de asegurar la claridad, pertinencia y confiabilidad de los ítems planteados

Variables de la Investigación

Las variables de investigación constituyen elementos fundamentales dentro del proceso metodológico, ya que permiten estructurar, medir y analizar los fenómenos objeto de estudio. En este sentido, Hernández Sampieri et al. (2014) señalan que: *"una variable es una propiedad que puede fluctuar y cuya variación es susceptible de medirse u observarse"* (p. 105).

Asimismo, las variables se derivan directamente de los objetivos específicos de la investigación, lo que permite establecer una relación clara entre lo que se pretende estudiar y los datos que se desean recolectar. En relación con esto, los mismos autores indican que: *"plantear el problema no es sino afinar y estructurar más formalmente la idea de investigación"* (Hernández Sampieri et al., 2014, p. 36).

Tipos de Variables

Para efectos de la presente investigación, las variables se clasifican en:

Variable Conceptual

La variable conceptual define el significado teórico del elemento que se desea estudiar. Permite comprender qué se entiende por cada variable dentro del contexto de la investigación.

Ejemplo:

Según Kendall y Kendall (2011): *"Proveen retroalimentación para el analista"* (p. 158).

Variable Operacional

La variable operacional traduce el concepto en elementos medibles, permitiendo su análisis a través de indicadores concretos dentro del estudio.

Variable Instrumental

La variable instrumental hace referencia al medio mediante el cual se recolectará la información, tales como cuestionarios, entrevistas o guías de observación.

Importancia de las Variables en la Investigación

Las variables permiten organizar y dar claridad al proceso investigativo, facilitando la construcción de instrumentos de recolección de datos y el análisis de la información. Además, garantizan que la investigación mantenga coherencia con los objetivos planteados.

Tabla 12 Cuadro de Variables

Objetivo Específico	Variable	Variable Conceptual	Variable Instrumental	Variable Operacional
Analizar la situación actual de la seguridad física y del entorno en Sauter Infomax S.A., utilizando herramientas investigativas como el análisis FODA y cuadros comparativos, con el propósito de identificar brechas, riesgos y	Seguridad física y del entorno	La seguridad física y del entorno corresponde al conjunto de controles orientados a prevenir accesos no autorizados, daños, pérdidas o interferencias sobre instalaciones, activos físicos y recursos de información,	Cuestionario, guía de observación ,matriz, FODA , cuadro comparativo	Aplicación de encuestas a una muestra de **11 colaboradores** de la organización. Observación directa de accesos físicos, infraestructura y controles existentes. Identificación de brechas y vulnerabilidades mediante FODA.Comparación con los controles de la ISO/IEC 27001:2022.

vulnerabilidades en relación con los lineamientos de la norma ISO/IEC 27001:2022.		garantizando la protección de la infraestructura organizacional y la continuidad de las operaciones, conforme a los lineamientos establecidos en la norma ISO/IEC 27002:2022.		
Objetivo Específico	**Variable**	**Variable Conceptual**	**Variable Instrumental**	**Variable Operacional**
Determinar los requerimientos normativos, el alcance y los elementos críticos del Sistema de Gestión de Seguridad de la Información (SGSI) que serán considerados en la propuesta, tomando en cuenta los	Requerimientos del SGSI	Un Sistema de Gestión de Seguridad de la Información (SGSI) es un conjunto de políticas, procesos, procedimientos y controles diseñados para gestionar y proteger la confidencialidad, integridad y	Revisión documental, matriz de análisis normativo. cuadro comparativo	Identificación de activos críticos. Definición del alcance del SGSI. Análisis de los controles aplicables de la ISO/IEC 27001:2022.Asignación de responsabilidades dentro de la empresa.

activos, procesos, infraestructura y responsabilidades vinculadas con la seguridad física y del entorno		disponibilidad de la información dentro de una organización, conforme a los requisitos establecidos en la norma ISO/IEC 27001:2022.		
Objetivo Específico	**Variable**	**Variable Conceptual**	**Variable Instrumental**	**Variable Operacional**
Elaborar los procedimientos documentados necesarios para la implementación de la seguridad física y del entorno, conforme a los controles establecidos en la norma ISO/IEC 27001:2022.	Procedimientos documentados de seguridad	Los procedimientos documentados de seguridad corresponden a documentos formales que establecen lineamientos, responsabilidades y actividades necesarias para la ejecución uniforme y controlada de procesos relacionados con	Plantillas documentales. Guía estructural de procedimientos	Redacción de políticas de seguridad física. Diseño de procedimientos de control de acceso. Establecimiento de controles ambientales y protección de equipos.

		la seguridad de la información dentro de la organización.		
Desarrollar los instrumentos investigativos y de apoyo técnico, tales como matrices de control, cuadros comparativos y esquemas metodológicos, que respalden la aplicación práctica de la propuesta dentro del marco del SGSI.	Instrumentos metodológicos y técnicos	Los instrumentos metodológicos y técnicos constituyen herramientas de análisis, evaluación y control utilizadas para apoyar la implementación, seguimiento y mejora de los procesos relacionados con la seguridad de la información dentro de la organización.	Matriz de control. Cuadros comparativos. Esquemas metodológicos.	Diseño y aplicación de matrices de control. Elaboración de cuadros comparativos entre situación actual y norma. Estructuración metodológica del SGSI.
Objetivo Específico	**Variable**	**Variable Conceptual**	**Variable Instrumental**	**Variable Operacional**
Proponer un plan de acción y mejora continua que contemple estrategias de evaluación,	Plan de acción y mejora continua	La mejora continua corresponde al proceso	Plan de acción. Matriz de seguimiento.	Definición de acciones correctivas y preventivas. Establecimiento de

seguimiento y retroalimentación, orientado a asegurar la vigencia, efectividad y actualización permanente de la seguridad física y del entorno en la empresa.		sistemático de evaluación, seguimiento y optimización de controles y procedimientos de seguridad de la información, basado en el ciclo Planificar-Hacer-Verificar-Actuar (PHVA), con el propósito de mantener la eficacia y actualización permanente de los controles implementados.	Indicadores de desempeño.	indicadores de seguimiento. Programación de evaluaciones periódicas. Retroalimentación y actualización de controles.

Fuente: Elaboración propia.

Población

La población corresponde al conjunto total de elementos que comparten características comunes dentro del estudio. Según Hernández Sampieri y Mendoza (2023), "la población o universo es el conjunto de todos los casos que concuerdan con determinadas especificaciones" (p. 170).

En la presente investigación, la población está conformada por todos los colaboradores de la empresa Sauter Infomax S.A., la cual cuenta con aproximadamente entre 15 y 18 empleados.

Estos colaboradores pertenecen a diferentes áreas:

- Administrativa
- Comercial

- Técnica
- Soporte

Todos ellos interactúan con información organizacional, por lo que resultan relevantes para el estudio.

Muestra

La muestra se define como un subconjunto de la población seleccionado para participar en el proceso de investigación. Hernández Sampieri y Mendoza (2023) indican que la muestra corresponde a un grupo de elementos representativos de la población sobre los cuales se recolecta la información necesaria para el estudio. En la presente investigación, la muestra estuvo conformada por **11 colaboradores** de la empresa Sauter Infomax S.A., seleccionados en función de su disponibilidad y participación durante el período de aplicación de los instrumentos de recolección de datos.

Aunque la población total de la organización está compuesta por aproximadamente entre **15 y 18 colaboradores**, factores asociados a la disponibilidad y a los tiempos operativos de algunos empleados limitaron la participación del total de la población en el proceso de recolección de información.

Tipo de Muestreo

El tipo de muestreo utilizado en la presente investigación corresponde a un **muestreo no probabilístico por conveniencia**, el cual consiste en seleccionar aquellos participantes que se encuentran disponibles y accesibles para el investigador durante el proceso de recolección de información.

Hernández Sampieri y Mendoza (2023) señalan que el muestreo por conveniencia permite seleccionar casos accesibles que facilitan la obtención de información relevante para el estudio. Bajo este criterio, participaron 11 colaboradores de Sauter Infomax S.A., pertenecientes a distintas áreas de la organización, permitiendo obtener información

representativa sobre las condiciones actuales de seguridad física y del entorno dentro de la empresa.

Instrumentos de Recolección de Datos

Las técnicas de recolección de datos permiten obtener información del fenómeno estudiado. Hernández Sampieri y Mendoza (2023) establecen que "la recolección de datos implica elaborar un plan detallado de procedimientos que conduzcan a reunir datos con un propósito específico" (p. 198).

En esta investigación se utilizarán las siguientes técnicas:

Encuesta

La encuesta permite recopilar información de manera estructurada. Según Hernández Sampieri y Mendoza (2023), "la encuesta es un instrumento que consiste en un conjunto de preguntas respecto a una o más variables a medir" (p. 217).

Se aplicará a los colaboradores de la empresa para evaluar:

- Nivel de conocimiento en seguridad
- Cumplimiento de políticas
- Percepción de riesgos

Observación

La observación permite analizar directamente el entorno. Hernández Sampieri y Mendoza (2023) indican que "observar implica registrar sistemáticamente comportamientos y situaciones" (p. 222).

Se utilizará para evaluar:

- Accesos físicos
- Infraestructura
- Condiciones ambientales

Instrumentos de Recolección de Datos

Los instrumentos de recolección de datos constituyen herramientas fundamentales dentro del proceso investigativo, ya que permiten obtener información relevante de manera sistemática y organizada. En este sentido, Hernández Sampieri y Mendoza (2023) establecen que: "un instrumento de medición es cualquier recurso que utiliza el investigador para registrar información" (p. 200).

En la presente investigación, orientada al análisis de la seguridad física y del entorno en la empresa Sauter Infomax S.A., se emplearán instrumentos que permitan recolectar datos objetivos y medibles, en concordancia con el enfoque cuantitativo adoptado.

Cuestionario

Se utilizará un **cuestionario estructurado con preguntas cerradas**, dirigido a los colaboradores de Sauter Infomax S.A., con el propósito de recolectar información sobre la seguridad física y del entorno dentro de la organización.

El instrumento estará compuesto por preguntas diseñadas en función de las variables de investigación, permitiendo obtener datos cuantificables y comparables. Se emplearán escalas tipo dicotómicas (Sí/No) y escalas tipo Likert, con el fin de medir percepciones, niveles de cumplimiento y condiciones actuales de seguridad.

Considerando que la organización cuenta con una población reducida y que participaron 11 colaboradores pertenecientes a distintas áreas de la empresa, permitiendo obtener información directa y representativa sobre las condiciones actuales de seguridad física y del entorno.

Estructura del Cuestionario

El cuestionario se organizará en secciones según las variables definidas en la investigación:

- Seguridad física y del entorno
- Requerimientos del SGSI
- Procedimientos de seguridad
- Cultura organizacional en seguridad
- Riesgos y vulnerabilidades
- Mejora continua

CAPÍTULO IV: ANÁLISIS DE RESULTADOS

Aplicación de instrumentos.

Para el desarrollo del diagnóstico de seguridad física y del entorno en la empresa Sauter Infomax S.A., se aplicaron los instrumentos de recolección de información definidos en el marco metodológico, los cuales corresponden al cuestionario, la entrevista y la guía de observación.

La población objeto de estudio estuvo conformada por aproximadamente entre 15 y 18 colaboradores de la organización. Debido a las limitaciones de tiempo y disponibilidad del personal para participar en el proceso de recolección de datos, el cuestionario fue aplicado a una muestra de 11 colaboradores seleccionados por conveniencia, permitiendo obtener información representativa sobre el nivel de conocimiento, percepción y cumplimiento relacionado con la seguridad física y del entorno dentro de la empresa.

Asimismo, la entrevista fue dirigida a personal con conocimiento del funcionamiento organizacional y de los procesos vinculados con la seguridad de la información, permitiendo obtener información cualitativa sobre las prácticas actuales y las necesidades de mejora. De igual forma, se utilizó una guía de observación para verificar directamente las condiciones físicas, ambientales y de control existentes dentro de las instalaciones de la empresa, generando evidencia diagnóstica relacionada con los controles establecidos en la norma ISO/IEC 27002:2022. La información recopilada permitió identificar brechas, riesgos y oportunidades de mejora relacionadas con la protección de activos físicos y tecnológicos, sirviendo como base para el análisis de riesgos, la evaluación GAP y la selección de controles aplicables dentro de la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI).

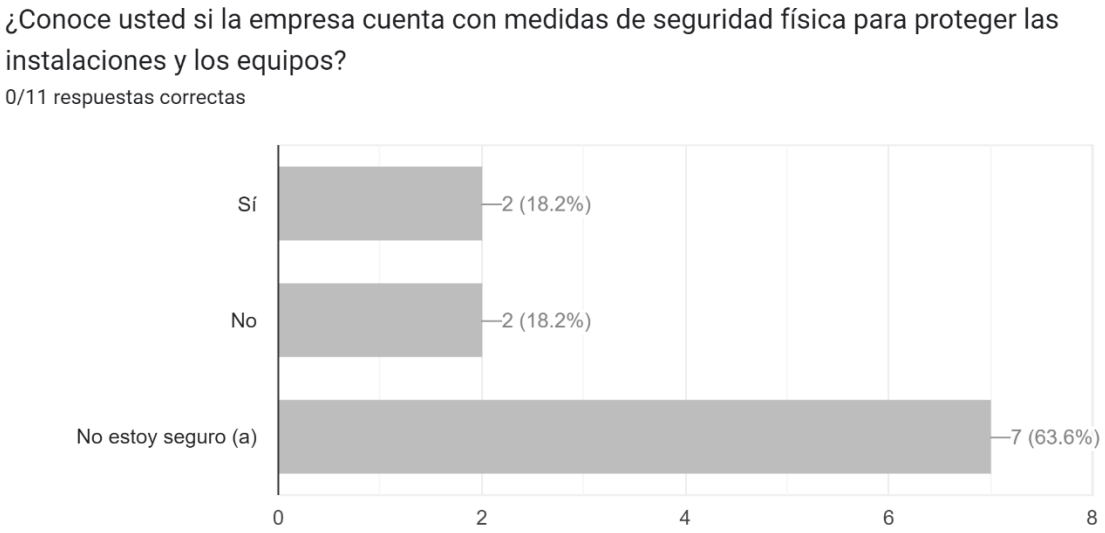
Resultados del cuestionario.

El cuestionario fue aplicado a un total de 11 colaboradores de la empresa Sauter Infomax S.A., con el propósito de identificar el nivel de conocimiento, percepción y aplicación de controles

relacionados con la seguridad física y del entorno dentro de la organización. Los resultados obtenidos permitieron analizar las condiciones actuales de seguridad y detectar oportunidades de mejora alineadas con los lineamientos de las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

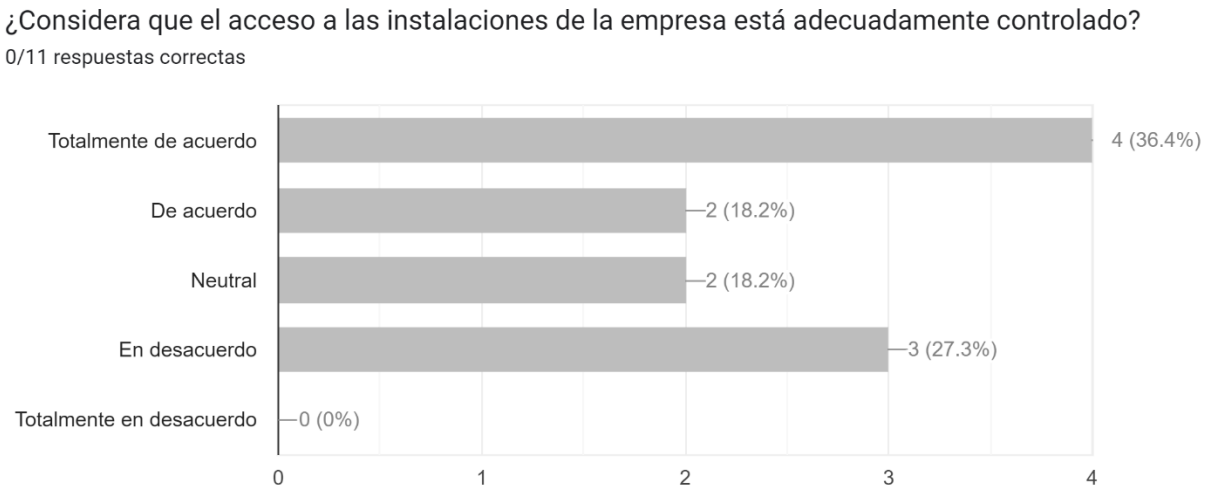
Figura 7

Pregunta 1



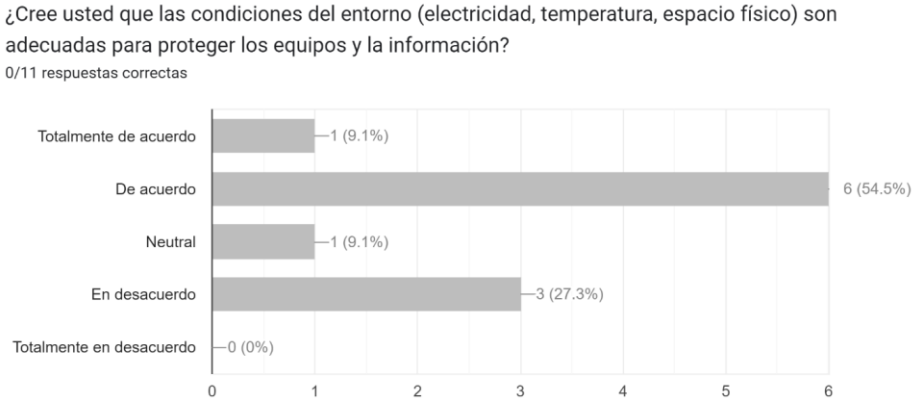
Los resultados evidencian que la mayoría de los colaboradores no tiene claridad sobre la existencia de medidas de seguridad física dentro de la organización. Esto refleja debilidades en la comunicación institucional y en la formalización de controles relacionados con la protección de activos físicos y tecnológicos.

Figura 8
Pregunta 2



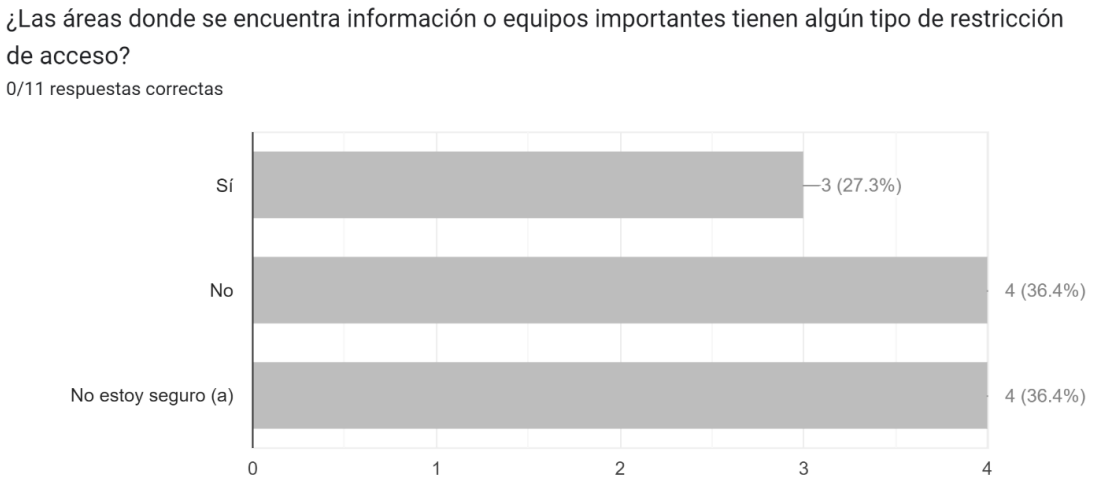
Los resultados muestran opiniones divididas respecto al control de acceso a las instalaciones. Aunque una parte de los colaboradores considera que existen controles adecuados, también se evidencia un porcentaje importante de desacuerdo, lo cual demuestra la necesidad de fortalecer y formalizar los mecanismos de control físico.

Figura 9
Pregunta 3



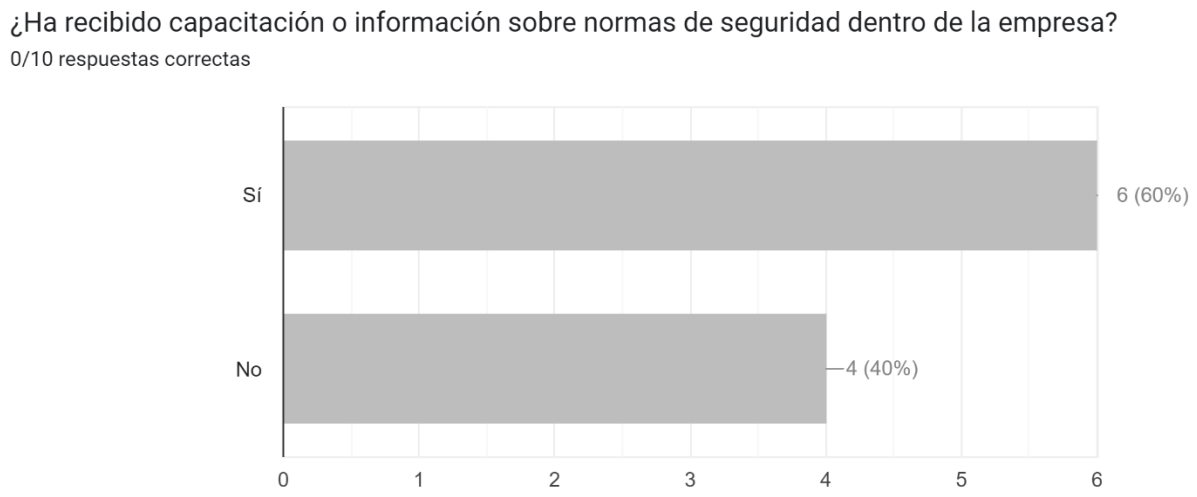
La mayoría de los colaboradores considera que las condiciones ambientales son adecuadas; sin embargo, existe un grupo significativo que percibe deficiencias relacionadas con factores físicos y ambientales, lo cual podría representar riesgos para los equipos tecnológicos y la continuidad operativa.

Figura 10
Pregunta 4



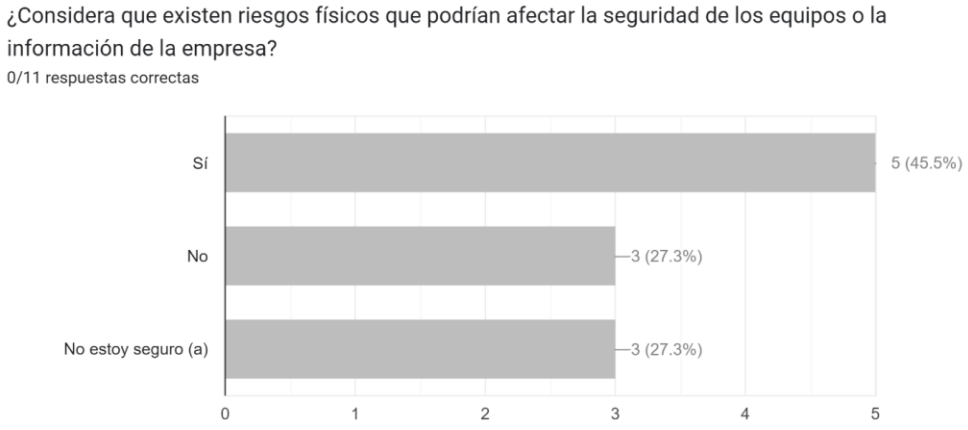
Los resultados evidencian que no existe claridad sobre la existencia de áreas restringidas o controles de acceso específicos para la protección de activos críticos, lo cual representa una vulnerabilidad importante dentro de la seguridad física de la organización.

Figura 11
Pregunta 5



Aunque parte del personal ha recibido información relacionada con seguridad, aún existe una cantidad considerable de colaboradores sin capacitación formal, lo que evidencia la necesidad de fortalecer los procesos de concientización y formación institucional.

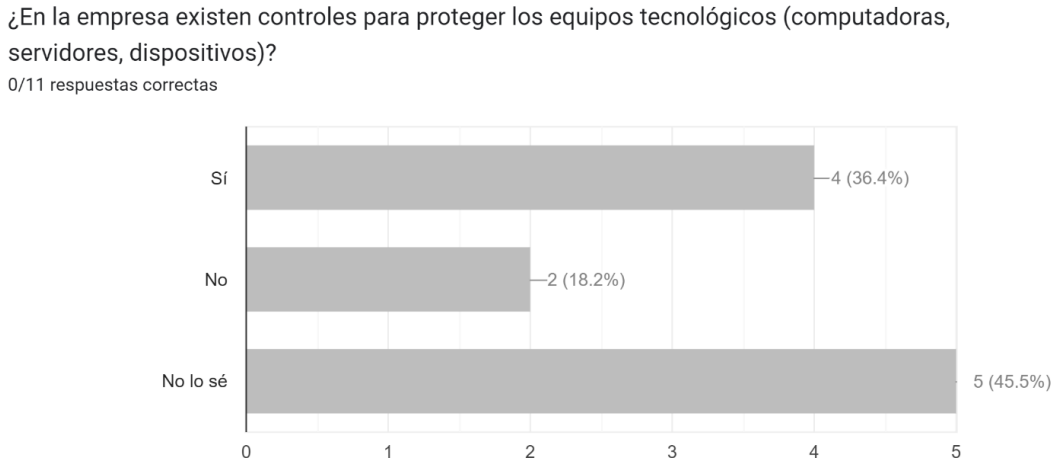
Figura 12
Pregunta 6



Los resultados reflejan que una parte importante de los colaboradores reconoce la existencia de riesgos físicos

dentro de la organización, relacionados principalmente con accesos no autorizados y condiciones ambientales, lo cual justifica la necesidad de implementar controles preventivos.

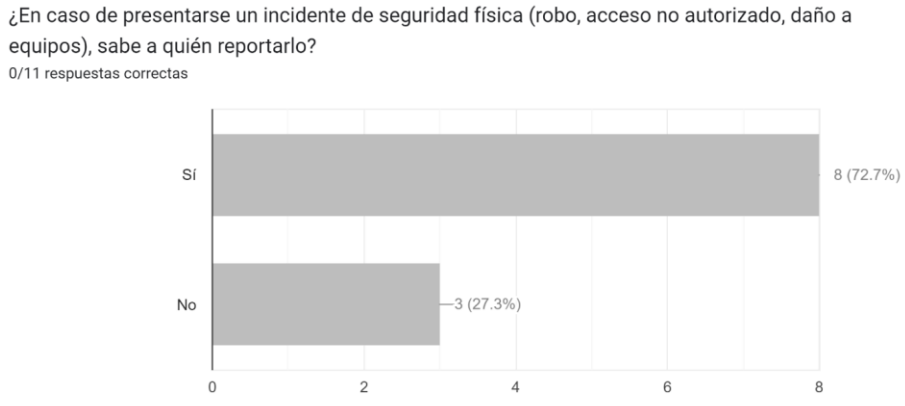
Figura 13
Pregunta7



La mayoría de los participantes desconoce si existen controles formales para proteger los equipos tecnológicos, lo que evidencia falta de documentación, comunicación y visibilidad de las medidas de seguridad implementadas.

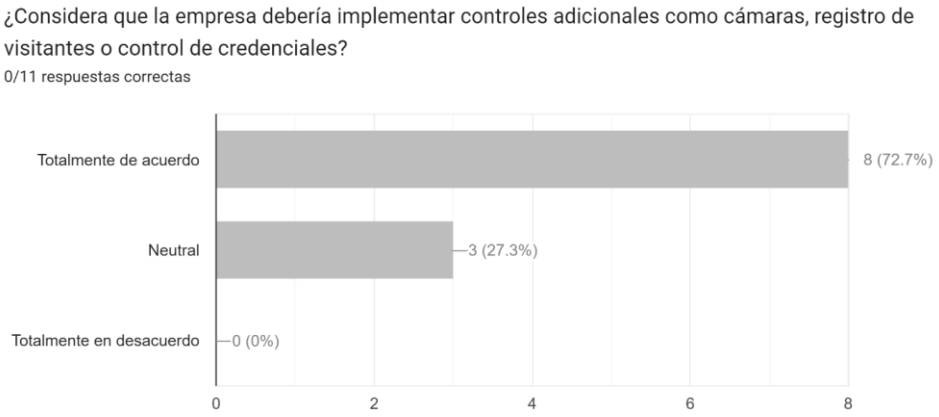
Figura 14

Pregunta 8



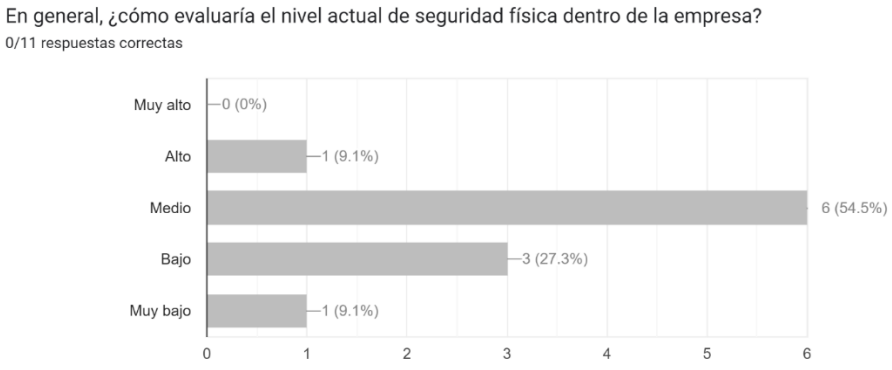
Los resultados muestran que la mayoría del personal conoce a quién reportar incidentes de seguridad; sin embargo, todavía existe un porcentaje de colaboradores que desconoce el procedimiento de reporte, lo que podría afectar la atención oportuna de incidentes.

Figura 15
Pregunta 9



La mayoría de los colaboradores considera necesaria la implementación de controles adicionales de seguridad física, evidenciando una percepción positiva hacia el fortalecimiento de la protección de instalaciones y activos organizacionales.

Figura 16
Pregunta 10



En términos generales, los colaboradores perciben que el nivel actual de seguridad física de la organización es medio o bajo, lo cual evidencia oportunidades de mejora relacionadas con

la formalización de políticas, procedimientos y controles alineados con las buenas prácticas de seguridad de la información.

Resultados de la entrevista

La entrevista realizada permitió identificar que actualmente la empresa implementa controles básicos de seguridad física; sin embargo, estos no se encuentran formalmente documentados dentro de políticas o procedimientos institucionales. Asimismo, se identificó que los principales riesgos percibidos corresponden a accesos no autorizados, fallas eléctricas y ausencia de mecanismos formales de control de visitantes. En relación con la gestión de incidentes, se evidenció que no existe un procedimiento estandarizado para el reporte y seguimiento de eventos relacionados con seguridad física, lo cual limita la capacidad de respuesta organizacional.

Por otra parte, se determinó que la organización reconoce la importancia de implementar controles alineados con la norma ISO/IEC 27001:2022, considerando que esto contribuiría al fortalecimiento de la protección de activos y a la mejora de la continuidad operativa. Con el propósito de complementar la información obtenida mediante el cuestionario y la guía de observación, se aplicó una entrevista semiestructurada al gerente general de la empresa Sauter Infomax S.A., señor Víctor Hugo Fonseca Martínez, debido a su conocimiento sobre la operación organizacional, la infraestructura tecnológica y las medidas actuales relacionadas con la seguridad física y del entorno. La entrevista permitió identificar la percepción de la administración respecto al estado actual de la seguridad de la información, así como las principales debilidades, riesgos y oportunidades de mejora presentes en la organización.

Datos Generales de la Entrevista

Elemento	**Descripción**
Empresa	Sauter Infomax S.A.
Entrevistado	Víctor Hugo Fonseca Martínez
Puesto	Gerente General
Investigadora	Mariana Chinchilla Murillo
Fecha	27/04/2026
Medio	Entrevista presencial en oficina

Desarrollo de la Entrevista

1. ¿Cómo describiría actualmente las medidas de seguridad física implementadas en la empresa para proteger las instalaciones y los equipos?

El entrevistado indicó que actualmente la empresa cuenta con medidas básicas de seguridad física, tales como cerraduras, supervisión del acceso a las instalaciones y resguardo de equipos tecnológicos dentro de áreas administrativas. Sin embargo, señaló que muchos de estos controles se aplican de manera empírica y no se encuentran formalmente documentados.

2. ¿Qué controles existen actualmente para regular el acceso de personas a las instalaciones o a las áreas donde se encuentran equipos o información importante?

Según lo expresado por el gerente general, el acceso a la empresa se controla principalmente mediante supervisión del personal administrativo y restricción de ingreso a determinadas áreas. Asimismo, mencionó que no existe actualmente un sistema formal de registro de visitantes ni controles automatizados de acceso.

3. Desde su perspectiva, ¿cuáles considera que son los principales riesgos físicos o ambientales que podrían afectar la seguridad de los activos de la empresa?

El entrevistado señaló que los principales riesgos corresponden a accesos no autorizados, fallas eléctricas, incendios, daños a equipos tecnológicos y pérdida de información debido a incidentes físicos o ambientales.

4. ¿La empresa cuenta con procedimientos o políticas documentadas relacionadas con la seguridad física o el control de accesos?

El gerente indicó que actualmente la empresa no posee políticas ni procedimientos formalmente documentados relacionados con seguridad física y control de accesos, aunque existen prácticas internas aplicadas de forma operativa.

5. ¿Qué tipo de controles se aplican para proteger los equipos tecnológicos y la infraestructura física de la empresa?

Se mencionó que los equipos tecnológicos se mantienen dentro de áreas supervisadas y que se realizan medidas básicas de protección, tales como respaldo de información, control del uso de equipos y supervisión general de las instalaciones.

6. ¿Cómo se gestionan actualmente los incidentes relacionados con seguridad física, como accesos no autorizados, pérdidas de equipos o daños en la infraestructura?

El entrevistado manifestó que los incidentes son atendidos directamente por la administración según la situación presentada; sin embargo, reconoció que no existe un procedimiento formal documentado para el reporte, seguimiento y tratamiento de incidentes de seguridad física.

7. ¿Se realizan capacitaciones o acciones de concientización al personal sobre seguridad de la información y protección de activos?

El gerente general indicó que ocasionalmente se brindan indicaciones al personal relacionadas con el uso adecuado de equipos y protección de información, aunque actualmente no existe un programa formal de capacitación o concientización en seguridad de la información.

8. ¿Considera que la empresa cuenta con las condiciones ambientales adecuadas (electricidad, ventilación, espacio físico) para proteger los equipos tecnológicos?

El entrevistado considera que las condiciones generales son aceptables para el funcionamiento de la empresa; no obstante, señaló que existen oportunidades de mejora relacionadas con la protección eléctrica, organización de espacios y fortalecimiento de controles ambientales.

9. Desde su experiencia, ¿qué aspectos considera que deberían mejorarse para fortalecer la seguridad física y del entorno dentro de la empresa?

Entre los principales aspectos de mejora, mencionó la necesidad de implementar políticas documentadas, fortalecer los controles de acceso, mejorar el monitoreo de instalaciones, establecer procedimientos formales y aumentar la capacitación del personal en temas de seguridad.

10. ¿Considera que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 podría beneficiar a la organización? ¿Por qué?

El entrevistado manifestó que la implementación de un SGSI representaría un beneficio importante para la empresa, debido a que permitiría mejorar la organización de los controles de seguridad, reducir riesgos, proteger los activos críticos y fortalecer la confianza de clientes y colaboradores mediante la adopción de buenas prácticas alineadas con estándares internacionales.

Análisis de la Entrevista

A partir de la información obtenida, se evidencia que la empresa Sauter Infomax S.A. cuenta con controles básicos de seguridad física y protección de activos; sin embargo, estos no se encuentran

formalmente estructurados ni documentados conforme a un Sistema de Gestión de Seguridad de la Información.

Asimismo, se identifican debilidades relacionadas con la ausencia de políticas formales, procedimientos documentados, mecanismos de control de acceso y programas de capacitación, lo cual incrementa la exposición de la organización ante riesgos físicos y ambientales.

No obstante, la administración reconoce la importancia de fortalecer la seguridad organizacional y muestra disposición para implementar controles alineados con los lineamientos de las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, especialmente en materia de seguridad física y del entorno.

Resultados de la guía de observación

Con el propósito de complementar la información obtenida mediante el cuestionario y la entrevista, se aplicó una guía de observación dentro de las instalaciones de la empresa Sauter Infomax S.A., orientada a verificar el estado actual de los controles relacionados con la seguridad física y del entorno. La observación permitió identificar condiciones reales de infraestructura, control de accesos, protección de equipos y medidas de vigilancia, tomando como referencia los lineamientos establecidos en la norma ISO/IEC 27001:2022 y las buenas prácticas de la ISO/IEC 27002:2022.

Los resultados obtenidos se presentan a continuación:

No.	Aspecto observado	Cumple	No cumple	Oportunidad de mejora	Detalle de observación
1	Existencia de control de acceso físico a las instalaciones de la empresa	✓		Implementar controles documentados de ingreso	El acceso a la empresa se realiza de forma manual y no existe un procedimiento

					formal documentado.
2	Registro o control de ingreso de visitantes		✓	Establecer bitácora o sistema de registro	No se evidenció un registro formal de visitantes ni control de ingreso temporal.
3	Protección física de equipos tecnológicos (computadoras, servidores, impresoras)	✓		Mejorar mecanismos de resguardo	Los equipos se encuentran protegidos dentro de las oficinas; sin embargo, no todos cuentan con medidas adicionales de seguridad física.
4	Existencia de áreas restringidas para personal autorizado		✓	Delimitar áreas críticas y restringidas	No se identificaron áreas claramente restringidas ni controles de acceso diferenciados.
5	Protección contra riesgos ambientales (temperatura, humedad, polvo)	✓		Implementar monitoreo ambiental	Las condiciones generales son adecuadas, aunque no existen controles

					específicos para monitoreo ambiental.
6	Condiciones adecuadas de infraestructura (orden, espacio, ventilación)	✓		Mantener controles preventivos	Las instalaciones presentan condiciones aceptables de orden y ventilación.
7	Existencia de sistemas de vigilancia o monitoreo (cámaras, supervisión)	✓		Fortalecer cobertura y monitoreo	Se observó la existencia de cámaras de vigilancia en puntos específicos de la empresa.
8	Condiciones de seguridad eléctrica y protección de equipos	✓		Implementar protección adicional	Los equipos cuentan con conexiones eléctricas básicas, aunque no se evidenció protección especializada contra variaciones eléctricas.
9	Existencia de controles para evitar acceso no autorizado a equipos		✓	Definir políticas y controles de acceso	No se identificaron controles formales para restringir el

					acceso físico a determinados equipos.
10	Ubicación segura de equipos críticos o información sensible	✓		Reforzar protección de activos críticos	Los equipos críticos se encuentran ubicados dentro de áreas internas de la empresa, aunque sin delimitación formal de seguridad.

Análisis de los resultados de observación

Los resultados evidencian que la empresa Sauter Infomax S.A. cuenta con ciertos controles básicos de seguridad física y del entorno; sin embargo, estos se aplican de manera empírica y no documentada. Se identificaron debilidades relacionadas con el control de visitantes, delimitación de áreas restringidas y establecimiento de procedimientos formales para el acceso a equipos e instalaciones.

Asimismo, aunque existen medidas generales de vigilancia y condiciones físicas adecuadas, no se evidencian controles estructurados alineados completamente con las buenas prácticas establecidas en la ISO/IEC 27002:2022, especialmente en aspectos relacionados con control de acceso físico, protección ambiental y resguardo de activos críticos.

A partir de esta observación, se confirma la necesidad de desarrollar políticas, procedimientos y controles documentados que permitan fortalecer la gestión de la seguridad física y del entorno dentro de la organización, contribuyendo a la reducción de riesgos y al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI).

Matriz de Riesgos de Seguridad Física y del Entorno

En cumplimiento de la cláusula 6.1.2 de la norma ISO/IEC 27001:2022, se realizó el proceso de identificación, análisis y valoración de riesgos relacionados con la seguridad física y del entorno dentro de la empresa Sauter Infomax S.A.

La matriz de riesgos tiene como propósito identificar las amenazas y vulnerabilidades que podrían afectar los activos físicos, tecnológicos y documentales de la organización, permitiendo establecer controles adecuados para reducir el impacto y la probabilidad de ocurrencia de incidentes de seguridad.

Para el desarrollo de esta matriz se tomó como referencia la información obtenida mediante la aplicación del cuestionario, la entrevista y la guía de observación, así como los lineamientos establecidos en la norma ISO/IEC 27002:2022 relacionados con controles de seguridad física y ambiental.

La valoración de riesgos se realizó considerando los siguientes criterios:

- **Probabilidad:** posibilidad de que ocurra el incidente.
- **Impacto:** nivel de afectación para la organización.
- **Nivel de riesgo:** resultado de la combinación entre probabilidad e impacto.

Tabla 13 Matriz de Riesgos de Seguridad Física y del Entorno

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo	Control Recomendado ISO 27002
Equipos tecnológicos	Robo de equipos	Ausencia de control de acceso físico	Alto	Alta	Alto	Control de acceso físico y monitoreo
Información física	Acceso no autorizado	Falta de áreas restringidas	Alto	Media	Alto	Restricción de acceso y

						almacenamiento seguro
Servidores y computadoras	Fallas eléctricas	Ausencia de reguladores o protección eléctrica	Alto	Media	Alto	Protección eléctrica y mantenimiento preventivo
Instalaciones físicas	Incendio	Falta de procedimientos ambientales documentados	Alto	Baja	Medio	Plan de emergencia y extintores
Equipos tecnológicos	Daño ambiental	Condiciones inadecuadas de temperatura y ventilación	Medio	Media	Medio	Monitoreo ambiental
Información organizacional	Pérdida de documentos físicos	Falta de control documental	Medio	Media	Medio	Procedimiento de manejo documental
Áreas operativas	Ingreso de personas no autorizadas	Ausencia de registro formal de visitantes	Alto	Alta	Alto	Registro de visitantes y credenciales
Infraestructura tecnológica	Manipulación indebida de equipos	Falta de supervisión	Medio	Media	Medio	Supervisión y vigilancia física

Fuente: Elaboración propia con base en ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Los resultados de la matriz evidencian que los principales riesgos identificados dentro de la empresa Sauter Infomax S.A. se relacionan con el acceso no autorizado a instalaciones, la falta de procedimientos documentados, la ausencia de controles formales de ingreso y las debilidades en la protección ambiental de los equipos tecnológicos.

Asimismo, se identificó que gran parte de los riesgos poseen un nivel de criticidad alto o medio, lo cual justifica la necesidad de implementar controles alineados con la norma ISO/IEC 27002:2022, especialmente aquellos relacionados con control de acceso físico, protección de equipos, monitoreo ambiental y gestión de incidentes.

La matriz de riesgos constituye la base para la selección de controles y la elaboración de la Declaración de Aplicabilidad (SoA), permitiendo establecer acciones de tratamiento orientadas a fortalecer la seguridad física y del entorno dentro de la organización.

Declaración de Aplicabilidad (SoA) – ISO/IEC 27001:2022

Mapeo de Controles del Anexo A relacionados con Seguridad Física y del Entorno

La Declaración de Aplicabilidad (Statement of Applicability – SoA) constituye un documento requerido por la cláusula 6.1.3 d) de la norma ISO/IEC 27001:2022, el cual permite identificar los controles seleccionados para el Sistema de Gestión de Seguridad de la Información (SGSI), justificar su aplicabilidad y determinar su estado de implementación dentro de la organización.

En el contexto de la presente investigación, la SoA se desarrolla tomando como referencia los controles de la norma ISO/IEC 27002:2022 relacionados con seguridad física y del entorno, considerando las necesidades identificadas durante el diagnóstico realizado en la empresa Sauter Infomax S.A.

La finalidad de este documento es evidenciar qué controles son aplicables a la organización, cuáles requieren fortalecimiento y cuáles no aplican según el alcance definido del SGSI. Asimismo, la Declaración de Aplicabilidad permite establecer la relación entre los riesgos identificados y los controles seleccionados para su tratamiento.

Tabla 14 Declaración de Aplicabilidad (SoA) – Seguridad Física y del Entorno

Código del Control	Nombre del Control ISO/IEC 27002:2022	Aplicable	Justificación	Estado Actual
7.1	Perímetros de seguridad física	Sí	La empresa requiere delimitar áreas críticas y proteger instalaciones físicas.	Parcialmente implementado

7.2	Controles de entrada física	Sí	Es necesario regular el acceso de colaboradores y visitantes.	No implementado formalmente
7.3	Seguridad de oficinas, salas e instalaciones	Sí	Existen equipos e información sensibles dentro de las oficinas administrativas.	Parcial
7.4	Monitoreo de seguridad física	Sí	Se requiere fortalecer la vigilancia y supervisión de áreas críticas.	Parcial
7.5	Protección contra amenazas físicas y ambientales	Sí	Existen riesgos relacionados con electricidad, temperatura y daños ambientales.	Parcial
7.6	Trabajo en áreas seguras	Sí	Se requiere restringir acceso a determinadas áreas y equipos críticos.	No formalizado
7.7	Escritorio y pantalla limpios	Sí	Permite proteger la información física y visual frente a accesos no autorizados.	No implementado
7.8	Ubicación y protección de equipos	Sí	Los equipos tecnológicos requieren protección física adecuada.	Parcial

7.9	Seguridad de activos fuera de las instalaciones	No	El alcance del SGSI no contempla actualmente activos fuera de la organización.	No aplica
7.10	Medios de almacenamiento	Sí	La organización maneja dispositivos físicos y documentos impresos.	Parcial
7.11	Servicios de soporte	Sí	La continuidad eléctrica y mantenimiento son necesarios para proteger equipos.	Parcial
7.12	Cableado de seguridad	Sí	Se requiere proteger el cableado eléctrico y de red para evitar interrupciones.	Parcial
7.13	Mantenimiento de equipos	Sí	Los equipos tecnológicos requieren mantenimiento preventivo periódico.	Parcial
7.14	Eliminación o reutilización segura de equipos	Sí	La organización debe asegurar la eliminación adecuada de información y dispositivos.	No implementado

Fuente: Elaboración propia con base en ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Análisis de la Declaración de Aplicabilidad

Los resultados obtenidos evidencian que la mayoría de los controles relacionados con seguridad física y del entorno son aplicables dentro del contexto organizacional de Sauter Infomax S.A., debido a la necesidad de proteger instalaciones, equipos tecnológicos y activos de información frente a riesgos físicos y ambientales.

Asimismo, se identifica que gran parte de los controles se encuentran parcialmente implementados o carecen de formalización documental, lo cual representa una oportunidad de mejora para fortalecer la gestión de la seguridad dentro de la organización.

La Declaración de Aplicabilidad permite establecer una relación directa entre los riesgos identificados en la matriz de riesgos y los controles seleccionados para su tratamiento, facilitando la priorización de acciones y el desarrollo de procedimientos alineados con las buenas prácticas de la ISO/IEC 27002:2022.

De esta manera, la SoA se convierte en un elemento fundamental dentro de la propuesta del SGSI, ya que proporciona evidencia documental sobre los controles considerados necesarios para reducir vulnerabilidades y fortalecer la seguridad física y ambiental de la empresa.

CAPÍTULO V: PROPUESTA

La presente propuesta de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) surge a partir de los hallazgos obtenidos durante el diagnóstico realizado en la empresa Sauter Infomax S.A., en el cual se identificaron debilidades relacionadas con la seguridad física y del entorno, tales como la ausencia de políticas documentadas, controles de acceso limitados, procedimientos no formalizados y mecanismos insuficientes de seguimiento y monitoreo. Estos resultados evidenciaron la necesidad de establecer lineamientos estructurados que permitan fortalecer la protección de los activos físicos, tecnológicos y de información dentro de la organización.

En este sentido, la propuesta se fundamenta en los requisitos establecidos en la norma ISO/IEC 27001:2022 y en las buenas prácticas definidas por la norma ISO/IEC 27002:2022, específicamente en los

controles relacionados con seguridad física, control de acceso, protección ambiental y gestión de activos. Asimismo, se adopta un enfoque basado en la mejora continua mediante el ciclo PHVA (Planificar–Hacer–Verificar–Actuar), con el propósito de garantizar la sostenibilidad y actualización permanente de los controles implementados.

La propuesta contempla la definición del alcance del SGSI, la identificación de las partes interesadas, la clasificación de activos, la implementación de controles de seguridad física y ambiental, el desarrollo de procedimientos documentados y la creación de mecanismos de seguimiento y evaluación. De esta manera, se busca establecer una estructura organizacional orientada a la gestión de riesgos y a la protección integral de la información.

Asimismo, esta propuesta no representa la implementación total de un SGSI certificado bajo la norma ISO/IEC 27001:2022, sino el desarrollo de una base estructurada enfocada específicamente en la seguridad física y del entorno, tomando como referencia los controles aplicables de la ISO/IEC 27002:2022. Lo anterior permite a la empresa fortalecer progresivamente sus prácticas de seguridad y prepararse para futuras iniciativas de madurez y cumplimiento organizacional.

Tabla 15 Descripción de los Módulos del Sistema

Nombre del apartado	Descripción del apartado
Alcance de la Política de Seguridad Física y del Entorno.	Se definirá el alcance de la política de seguridad física y del entorno dentro del marco del SGSI, bajo los lineamientos de la ISO/IEC 27001:2022, abarcando los procesos internos, infraestructura tecnológica y espacios físicos que resguardan información. Objetivos tangibles: Elaborar un mapa de cobertura del SGSI que delimite los activos, área de tecnología y procesos incluidos. Crear un procedimiento documentado para la definición, revisión y actualización del alcance del SGSI.
Control de Acceso Físico.	Se establecerán lineamientos de control de acceso físico para las zonas críticas, conforme al control 7.2 de la ISO/IEC 27002:2022. Objetivos tangibles: Diseñar una matriz de control de acceso físico. Elaborar un procedimiento documentado de acceso físico (registro de visitantes, control de credenciales, restricción de áreas).
Seguridad Ambiental y de Infraestructura.	Se documentarán los mecanismos para resguardar los activos tecnológicos y físicos contra amenazas ambientales. Objetivos tangibles: Elaborar un FODA ambiental. Redactar un procedimiento de seguridad ambiental que incluya monitoreo de temperatura, control eléctrico y mantenimiento preventivo.
Manejo y Almacenamiento de Información Física.	Se definirán procedimientos para el manejo, almacenamiento y disposición de documentos o dispositivos físicos. Objetivos tangibles: Elaborar un cuadro de riesgos por tipo de soporte físico. Desarrollar un procedimiento de manipulación y eliminación segura de documentos y dispositivos físicos.

Monitoreo y Vigilancia Física.	Se propondrán controles de monitoreo y seguimiento (control 7.4 ISO/IEC 27002:2022). Objetivos tangibles: Construir un mapa de riesgo y puntos críticos. Crear un procedimiento de monitoreo y respuesta ante incidentes físicos.
Capacitación y Concientización.	Se desarrollará un programa de sensibilización para fortalecer la cultura organizacional de seguridad. Objetivos tangibles: Diseñar el plan de capacitación con contenido programático detallado por tema. Redactar el procedimiento de capacitación interna.
Diseño del Plan de Acción.	Se desarrollará un modelo metodológico de mejora para el SGSI mediante el ciclo PHVA. Objetivos tangibles: Elaborar un FODA organizacional. Crear una matriz de acciones correctivas y preventivas. Diseñar un cronograma de implementación.
Seguimiento y Evaluación del Plan de Mejora Continua.	Se propone un sistema de evaluación continúa basado en KPI alineados al ciclo PHVA. Objetivos tangibles: Elaborar una matriz de indicadores clave con umbrales y responsables. Diseñar un plan de revisión periódica documentado.

Fuente: Elaboración propia 2026

Partes Interesadas del SGSI

De acuerdo con la Cláusula 4.2 de la norma ISO/IEC 27001:2022, la identificación de las partes interesadas constituye un elemento fundamental para la definición y operación del Sistema de Gestión de Seguridad de la Información, ya que permite determinar las necesidades y expectativas que influyen en la seguridad de la información dentro de la organización.

Tabla 16 Partes Interesadas del SGSI

Parte interesada	Necesidad / Expectativa
Colaboradores	Seguridad en el entorno laboral
Clientes	Protección de la información
Empresa	Continuidad operativa
Proveedores	Acceso controlado a instalaciones
Entidades regulatorias	Cumplimiento normativo (Ley N.° 8968; ISO/IEC 27001:2022)

Fuente: Elaboración propia, 2026.

Elementos Incluidos dentro del Alcance del SGSI

De conformidad con la Cláusula 4.3 de la norma ISO/IEC 27001:2022, el alcance del SGSI debe definir claramente los límites y procesos incluidos. En la presente propuesta, el alcance se enfoca en la seguridad física y del entorno dentro de Sauter Infomax S.A., considerando aquellos activos, áreas y procesos con relación directa con la protección de la información y la continuidad operativa.

Tabla 17 Elementos incluidos dentro del alcance del SGSI

Elemento	Descripción	Incluido en el SGSI
Instalaciones físicas	Oficinas administrativas y áreas operativas	Sí
Equipos tecnológicos	Computadoras, impresoras, servidores y dispositivos	Sí
Información física	Documentos impresos, expedientes y archivos físicos	Sí
Infraestructura eléctrica	Sistemas eléctricos y reguladores de voltaje	Sí
Sistemas de vigilancia	Cámaras de monitoreo y controles de acceso	Sí
Personal interno	Colaboradores con acceso a instalaciones e información	Sí
Visitantes y proveedores	Personas externas que ingresan a las instalaciones	Sí
Áreas externas	Espacios fuera del control organizacional	No

Fuente: Elaboración propia, 2026.

Clasificación de Activos de Información

La clasificación de activos constituye un proceso esencial dentro del Sistema de Gestión de Seguridad de la Información, ya que permite identificar el nivel de criticidad de los recursos organizacionales y establecer controles proporcionales al impacto que podría generar su pérdida, daño o acceso no autorizado. En Sauter Infomax S.A. se establecen tres niveles de criticidad: alta, media y baja.

Tabla 18 Clasificación de activos de información

Activo	Tipo de activo	Nivel de criticidad
Servidor principal	Tecnológico	Alta
Computadoras administrativas	Tecnológico	Alta
Equipos de soporte técnico	Tecnológico	Media
Documentos financieros	Información física	Alta
Expedientes administrativos	Información física	Media
Sistemas de videovigilancia	Seguridad física	Media
Reguladores y UPS	Infraestructura eléctrica	Alta
Impresoras y periféricos	Tecnológico	Baja
Mobiliario administrativo	Físico	Baja
Archivos históricos	Información física	Media

Fuente: Elaboración propia, 2026.

Relación entre Activos y Controles de Protección

La relación entre activos y controles de protección permite establecer medidas de seguridad específicas para reducir los riesgos asociados a cada recurso organizacional. Estos controles se fundamentan en las buenas prácticas establecidas por la norma ISO/IEC 27002:2022.

Tabla 19 Relación entre activos y controles de protección

Activo	Riesgo asociado	Control de protección	Referencia ISO/IEC 27002:2022
Servidor principal	Acceso no autorizado	Restricción de acceso físico	Control 7.2
Computadoras administrativas	Robo o manipulación	Control de acceso y monitoreo	Control 7.1
Documentos financieros	Pérdida o divulgación	Archivadores seguros y acceso restringido	Control 7.10

Sistemas de videovigilancia	Fallo operativo	Mantenimiento preventivo	Control 7.13
Reguladores y UPS	Daños eléctricos	Protección eléctrica y monitoreo	Control 7.11
Equipos tecnológicos	Sobrecalentamiento	Control ambiental y ventilación	Control 7.8
Áreas operativas	Ingreso no autorizado	Registro de visitantes	Control 7.4
Archivos físicos	Deterioro o pérdida	Almacenamiento seguro	Control 7.9

Fuente: Elaboración propia, 2026.

Declaración de Aplicabilidad (SoA) – ISO/IEC 27001:2022

La Declaración de Aplicabilidad (Statement of Applicability – SoA) constituye un documento requerido por la cláusula 6.1.3 d) de la norma ISO/IEC 27001:2022, el cual identifica los controles seleccionados para el SGSI, justifica su aplicabilidad, determina su estado de implementación y establece trazabilidad con el procedimiento del SGSI que lo implementa y la evidencia esperada.

Tabla 20 Declaración de Aplicabilidad – Seguridad Física y del Entorno

Código	**Control ISO/IEC 27002:2022**	**Aplica**	**Justificación**	**Estado actual**	**Procedimiento del SGSI que lo implementa**	**Evidencia esperada**
7.1	Perímetros de seguridad física	Sí	Delimitar áreas críticas y proteger instalaciones.	Parcialmente implementado	Procedimiento de Control de Acceso Físico	Mapa de áreas, registros de acceso
7.2	Controles de entrada física	Sí	Regular acceso de colaboradores y visitantes.	No implementado formalmente	Procedimiento de Control de Acceso Físico	Bitácoras de acceso, registros de visitantes

7.3	Seguridad de oficinas, salas e instalaciones	Sí	Equipos e información sensibles en oficinas.	Parcial	Procedimiento de Control de Acceso Físico	Inventario de espacios seguros
7.4	Monitoreo de seguridad física	Sí	Fortalecer vigilancia de áreas críticas.	Parcial	Procedimiento de Monitoreo y Vigilancia Física	Reportes de monitoreo, registros CCTV
7.5	Protección contra amenazas físicas y ambientales	Sí	Riesgos de electricidad, temperatura y daños.	Parcial	Procedimiento de Seguridad Ambiental	Registros de mantenimiento ambiental
7.6	Trabajo en áreas seguras	Sí	Restringir acceso a áreas y equipos críticos.	No formalizado	Procedimiento de Control de Acceso Físico	Política de áreas restringidas
7.7	Escritorio y pantalla limpios	Sí	Proteger información física y visual.	No implementado	Procedimiento de Manejo y Almacenamiento de Información Física	Verificaciones de escritorio
7.8	Ubicación y protección de equipos	Sí	Los equipos tecnológicos requieren protección física.	Parcial	Procedimiento de Seguridad Ambiental	Inventario de equipos y condiciones
7.9	Seguridad de activos fuera de instalaciones	No	Fuera del alcance del SGSI.	No aplica	N/A	N/A
7.10	Medios de almacenamiento	Sí	Gestión de dispositivos físicos y documentos.	Parcial	Procedimiento de Manejo y Almacenamiento de Información Física	Registros de custodia y destrucción
7.11	Servicios de soporte	Sí	Continuidad eléctrica y mantenimiento.	Parcial	Procedimiento de Seguridad Ambiental	Reportes de revisión eléctrica

7.12	Cableado de seguridad	Sí	Proteger cableado eléctrico y de red.	Parcial	Procedimiento de Seguridad Ambiental	Inspecciones de cableado
7.13	Mantenimiento de equipos	Sí	Mantenimiento preventivo periódico.	Parcial	Procedimiento de Seguridad Ambiental	Registros de mantenimiento preventivo
7.14	Eliminación o reutilización segura de equipos	Sí	Asegurar eliminación adecuada de información.	No implementado	Procedimiento de Manejo y Almacenamiento de Información Física	Registros de baja y destrucción controlada

Fuente: Elaboración propia con base en ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Gestión documental para la implementación y seguimiento de los controles

La gestión documental constituye un elemento de apoyo para la implementación y seguimiento de los controles de Seguridad Física y del Entorno, debido a que permite establecer los insumos requeridos para cada actividad, los documentos necesarios para su ejecución y los registros que evidencian su cumplimiento.

Para efectos de la presente propuesta, la gestión documental se desarrollará mediante un proceso estructurado que comprende la identificación de los insumos, elaboración de los documentos y formatos requeridos, revisión y aprobación, utilización durante la ejecución de los controles, almacenamiento de las evidencias generadas y actualización periódica de la documentación.

Los **insumos** corresponden a la información necesaria para desarrollar o ejecutar un control, tales como la matriz de riesgos, inventarios de activos, identificación de áreas restringidas, información de colaboradores autorizados, reportes de incidentes, necesidades de mantenimiento y resultados obtenidos mediante los indicadores.

A partir de estos insumos se generan los **productos documentales**, entre ellos la Política de Seguridad Física y del Entorno, procedimientos, formularios, bitácoras, listas de verificación, matriz de riesgos y Declaración de Aplicabilidad (SoA). Estos productos permiten estandarizar la ejecución de las actividades y establecer los mecanismos mediante los cuales se recopilará evidencia.

Como resultado de la aplicación de los controles se generarán **registros de evidencia**, tales como bitácoras de acceso, registros de visitantes, reportes de incidentes, registros de mantenimiento preventivo, listas de asistencia a capacitaciones, resultados de verificaciones y registros de acciones correctivas. Estos registros servirán como insumo para el seguimiento de indicadores y para las revisiones realizadas por los responsables internos y el tercero especializado definido en el equipo implementador.

La Administración será responsable de coordinar el control de la documentación y aprobar los documentos de carácter general. Cada área responsable deberá generar y mantener los registros correspondientes a los controles bajo su responsabilidad. Los documentos deberán almacenarse en el repositorio institucional definido por la organización, procurando que únicamente se encuentre disponible la versión vigente y manteniendo un historial de las modificaciones realizadas.

Cada documento controlado deberá contener como mínimo su nombre, código de identificación, versión, fecha de elaboración o actualización, responsable de elaboración, responsable de aprobación y estado de vigencia. Cuando se realice una modificación, la versión anterior deberá identificarse como obsoleta y conservarse únicamente cuando sea necesario mantener evidencia histórica.

La revisión documental se integrará a la hoja de ruta de implementación y al ciclo PHVA de la propuesta. Durante la implementación se verificará la creación y utilización de los documentos y registros requeridos; posteriormente, su vigencia y efectividad serán evaluadas mediante el seguimiento de indicadores, revisiones internas y la evaluación periódica del tercero especializado. De esta manera, la gestión documental permitirá mantener trazabilidad entre los riesgos identificados, los controles aplicados, las actividades realizadas y las evidencias obtenidas.

Tabla 21 Gestión documental para la implementación de los controles

Actividad/ control	Insumo	Producto documental requerido	Registro / evidencia generada	Responsable
Gestión de riesgos	Amenazas, vulnerabilidades, activos y valoración de impacto	Matriz de riesgos	Matriz aprobada y actualizada	Administración / Soporte Técnico
Control de acceso físico	Áreas restringidas y personal autorizado	Procedimiento y formato de control de acceso	Bitácora de entradas y salidas	Administración / Soporte Técnico
Gestión de visitantes	Datos del visitante, motivo y autorización	Formato de registro de visitantes	Bitácora de visitantes	Administración
Monitoreo de instalaciones	Áreas críticas y necesidades de vigilancia	Procedimiento de monitoreo y lista de verificación	Registro de revisión y evidencias de monitoreo	Soporte Técnico
Protección de equipos	Inventario y estado de equipos	Plan/lista de mantenimiento	Reportes de mantenimiento	Soporte Técnico
Seguridad ambiental	Condiciones ambientales y riesgos identificados	Lista de verificación de condiciones ambientales	Registro de inspección y	Soporte Técnico

			mantenimiento	
Manejo de información física	Tipo de documentación y nivel de acceso	Procedimiento para manejo y almacenamiento	Registro de custodia o acceso cuando corresponda	Administración
Gestión de incidentes	Evento reportado y evidencia disponible	Formulario de reporte de incidentes	Bitácora e informe del incidente	Administración / Soporte Técnico
Capacitación	Necesidades identificadas y procedimientos vigentes	Plan y material de capacitación	Lista de asistencia y evaluación	Recursos Humanos
Seguimiento de controles	Registros, KPI e incidentes	Lista de verificación / informe de seguimiento	Resultado de revisión y acciones de mejora	Administración
Aplicabilidad de controles	Matriz de riesgos y controles seleccionados	Declaración de Aplicabilidad (SoA)	SoA aprobada y actualizada	Administración

Fuente:Elaboración propia,2026

Como parte de la gestión documental propuesta, se diseñaron instrumentos estandarizados que permitirán registrar y conservar las evidencias generadas durante la implementación y seguimiento de los controles de Seguridad Física y del Entorno. Estos instrumentos comprenden la bitácora de control de acceso físico, el registro de visitantes, el formato de reporte de incidentes, la lista de verificación de controles, el registro de mantenimiento preventivo y el registro de capacitación y concientización. Los formatos correspondientes se presentan en los anexos del presente documento y constituyen herramientas de apoyo para la ejecución, seguimiento y evaluación de los controles propuestos.

Ejemplo de bitácora de control de acceso físico

N.°	**Fecha**	**Nombre**	**Área de ingreso**	**Hora entrada**	**Hora salida**	**Motivo**	**Autorizado por**	**Observaciones**
01	03/08/2026	Carlos Rodríguez	Área de servidores	8:15	8:40	Mantenimiento preventivo	Administración	Sin incidentes
02	05/08/2026	José Ramírez	Área de servidores	0:20	0:45	Revisión de conectividad	Soporte Técnico	Acceso autorizado
03	07/08/2026	Andrea Vargas	Archivo físico	4:05	4:25	Consulta de documentación	Administración	Sin observaciones
04	10/08/2026	Luis Hernández	Área de servidores	9:30	0:10	Revisión de UPS	Soporte Técnico	Equipo funcionando

								correcta mente

Responsable: Administración / Soporte Técnico.

Frecuencia de registro: Cada vez que se ingrese a un área restringida.

Ejemplo de registro de visitantes

N.°	Fecha	Visitante	Empresa	Persona que visita	Motivo	Ingreso	Salida	Identificación	Observaciones
01	04/08/2026	María González	Proveedor externo	Administración	Entrega de suministros	9:10	9:30	Verificada	in novedades
02	06/08/2026	aniel Mora	Servicios Técnicos CR	Soporte Técnico	Revisión de equipo	1:00	2:15	Verificada	ngreso acompañado
03	11/08/2026	aura Jiménez	Proveedor comercial	Administración	Reunión comercial	3:30	4:20	Verificada	in novedades
04	14/08/2026	oberto Sánchez	Mantenimiento CR	Soporte Técnico	Mantenimiento preventivo	8:45	0:30	Verificada	cceso limitado al área autorizada

Ejemplo de registro de incidentes de Seguridad Física y del Entorno

N.°	Fecha	Área	Tipo de incidente	Descripción	Acción inmediata	Responsable	Estado
INC-001	05/08/2026	Área de servidores	Eléctrico	Se detectó una variación de voltaje durante la jornada.	Verificación de UPS y equipos conectados.	Soporte Técnico	Cerrado
INC-002	08/08/2026	Archivo físico	Acceso	Se detectó un intento de ingreso de una persona sin autorización previa.	Se restringió el ingreso y se verificó la autorización.	Administración	Cerrado
INC-003	12/08/2026	Área operativa	Ambiental	Se identificó una temperatura superior a la condición habitual del área.	Revisión de ventilación y equipos.	Soporte Técnico	En seguimiento
INC-004	18/08/2026	Instalaciones	Seguridad física	Se detectó una puerta de acceso	Cierre inmediato y	Administración	Cerrado

				restringido sin asegurar correctamente.	**comunicación al responsable.**		

Los registros de incidentes constituyen uno de los insumos utilizados para el cálculo de indicadores relacionados con la cantidad de incidentes, tiempos de respuesta y seguimiento de acciones correctivas.

Ejemplo de lista de verificación de controles

Fecha de revisión: 28/08/2026

Responsable: Administración / Soporte Técnico

N.°	**Aspecto evaluado**	**Cumple**	**No cumple**	**N/A**	**Evidencia / observación**	**Acción requerida**
1	**Áreas restringidas cuentan con control de acceso**	**X**			**Bitácora de acceso disponible**	**Mantener seguimiento**
2	**Se mantiene registro de visitantes**	**X**			**Registro actualizado**	**Mantener control**
3	**Equipos críticos cuentan con protección física**	**X**			**Verificación física realizada**	**Mantener condiciones**
4	**Cámaras de vigilancia se**	**X**			**Cámaras verificadas**	**Revisión periódica**

	encuentran operativas					
5	**Se conservan los registros de acceso**	**X**			**Registros disponibles**	**Mantener almacenamiento**
6	**Mantenimiento preventivo se encuentra actualizado**		**X**		**Se identificó un equipo pendiente**	**Programar mantenimiento**
7	**Condiciones ambientales son adecuadas**	**X**			**Verificación realizada**	**Mantener seguimiento**
8	**Documentación física se encuentra protegida**	**X**			**Documentación almacenada en área definida**	**Mantener control**
9	**Incidentes se encuentran documentados**	**X**			**Registro de incidentes disponible**	**Mantener actualización**
10	**Acciones correctivas tienen seguimiento**		**X**		**Existen acciones pendientes**	**Establecer fecha de cierre**

Resultado: 8 de 10 controles conformes.

Porcentaje de cumplimiento: (8 / 10) × 100 = 80 %

Acción de mejora: Programar el mantenimiento preventivo pendiente y establecer responsables y fechas de cierre para las acciones correctivas identificadas.

Ejemplo de registro de mantenimiento preventivo

N.°	Fecha	Activo/ equipo	Ubicación	Tipo	Actividad realizada	Resultado	Responsable	Próxima revisión
01	03/08/2026	UPS principal	Área de servidores	Preventivo	Revisión de batería y conexiones	Conforme	Soporte Técnico	03/11/2026
02	05/08/2026	Cámara CCTV 01	Entrada principal	Preventivo	Limpieza y prueba de grabación	Conforme	Soporte Técnico	05/11/2026
03	05/08/2026	Cámara CCTV 02	Área operativa	Preventivo	Verificación de imagen y almacenamiento	Conforme	Soporte Técnico	05/11/2026
04	10/08/2026	Control de acceso	Área restringida	Preventivo	Verificación de funcionamiento	Conforme	Soporte Técnico	10/11/2026

05	**12/08/2026**	**Equipo de ventilación**	**Área de servidores**	**Preventivo**	**Limpieza y revisión de funcionamiento**	**Requiere seguimiento**	**Soporte Técnico**	

Ejemplo de registro de capacitación y concientización

Tema: Seguridad Física y del Entorno

Fecha: 20/08/2026

Responsable: Recursos Humanos / Administración

Objetivo: Concientizar a los colaboradores sobre los controles, responsabilidades, gestión de accesos y reporte de incidentes establecidos en la propuesta.

N.°	**Colaborador**	**Área**	**Asistencia**	**Evaluación realizada**	**Resultado**
1	**Colaborador 01**	**Administración**	**Sí**	**Sí**	**Satisfactorio**
2	**Colaborador 02**	**Soporte Técnico**	**Sí**	**Sí**	**Satisfactorio**
3	**Colaborador 03**	**Ventas**	**Sí**	**Sí**	**Satisfactorio**
4	**Colaborador 04**	**Administración**	**Sí**	**Sí**	**Satisfactorio**
5	**Colaborador 05**	**Ventas**	**No**	**No**	**Reprogramar**

Resultado de participación: 4 de 5 colaboradores programados asistieron.

Porcentaje de personal capacitado:$(4 / 5) \times 100 = 80\ \%$

Acción de seguimiento: Reprogramar la capacitación para el colaborador pendiente.

Los datos incluidos en los siguientes instrumentos son de carácter simulado y se presentan únicamente con fines demostrativos, con el propósito de ejemplificar la forma en que Sauter Infomax S.A. podrá documentar y conservar las evidencias generadas durante la futura implementación de los controles propuestos. Estos registros no representan resultados obtenidos de una implementación realizada durante el desarrollo de la investigación.

Política de Seguridad Física y del Entorno

Objetivo

Establecer los lineamientos de seguridad física y del entorno necesarios para proteger los activos físicos, tecnológicos y de información de la empresa Sauter Infomax S.A., reduciendo los riesgos asociados a accesos no autorizados, daños ambientales, pérdida de información e incidentes que puedan afectar la continuidad operativa de la organización.

Alcance

La presente política aplica a todos los colaboradores, proveedores, visitantes y terceros que tengan acceso a las instalaciones, equipos tecnológicos, documentos físicos o áreas operativas de la empresa Sauter Infomax S.A. Asimismo, comprende las oficinas administrativas, áreas operativas, equipos tecnológicos, sistemas de almacenamiento de información y demás activos incluidos dentro del alcance del SGSI.

Lineamientos de la política

- Todo acceso a las instalaciones deberá realizarse únicamente por personal autorizado.
- Los visitantes deberán registrarse al ingresar y permanecer acompañados en áreas restringidas.
- Los equipos tecnológicos deberán mantenerse protegidos contra daños físicos, riesgos eléctricos y accesos no autorizados.
- Las áreas con información sensible o equipos críticos deberán contar con controles de acceso físico.
- Se deberán mantener condiciones ambientales adecuadas para proteger los equipos tecnológicos.

- Todo incidente relacionado con seguridad física deberá ser reportado inmediatamente a la administración.
- Los colaboradores deberán cumplir las disposiciones de los procedimientos de seguridad física y protección ambiental.
- La empresa promoverá actividades de capacitación y concientización en seguridad de la información.

Responsables

La administración de Sauter Infomax S.A. será responsable de supervisar el cumplimiento de la presente política y de coordinar las acciones necesarias para su actualización y mejora continua. Los colaboradores serán responsables de cumplir los lineamientos establecidos y reportar cualquier situación de riesgo.

Sanciones

El incumplimiento de las disposiciones de esta política podrá generar medidas administrativas internas conforme a los lineamientos organizacionales de la empresa.

Vigencia

La presente política entrará en vigor a partir de su aprobación y será revisada periódicamente como parte del proceso de mejora continua del SGSI.

Procedimiento de Control de Acceso Físico

Objetivo

Establecer un procedimiento documentado para regular el acceso físico a las instalaciones y áreas críticas de Sauter Infomax S.A., con el propósito de proteger los activos físicos, tecnológicos y documentales frente a accesos no autorizados.

Alcance

Este procedimiento aplica a colaboradores, visitantes, proveedores y cualquier persona que ingrese a las instalaciones de la empresa.

Responsables

- Administración
- Personal encargado de recepción
- Colaboradores autorizados

Procedimiento

Registro de visitantes:

- Todo visitante deberá registrarse al ingresar, indicando nombre completo, motivo de visita y hora de ingreso y salida.
- El visitante deberá permanecer acompañado durante su permanencia en áreas restringidas.

Control de credenciales:

- Los colaboradores autorizados deberán portar identificación institucional.
- El acceso a áreas críticas será limitado únicamente al personal autorizado.

Áreas restringidas:

- Las áreas donde se almacene información sensible o equipos críticos deberán permanecer bajo control de acceso.
- El ingreso a dichas áreas deberá registrarse cuando corresponda.

Bitácora de acceso:

- Se mantendrá un registro físico o digital de ingresos y salidas.
- La administración realizará revisiones periódicas de las bitácoras.

Reporte de incidentes:

- Todo acceso sospechoso o no autorizado deberá ser reportado inmediatamente.
- Los incidentes deberán documentarse para seguimiento y control.

Procedimiento de Seguridad Ambiental

Objetivo

Establecer controles orientados a proteger los equipos tecnológicos, instalaciones y activos organizacionales frente a riesgos ambientales que puedan afectar la continuidad operativa de la empresa.

Alcance

Este procedimiento aplica a las áreas administrativas, operativas y tecnológicas de Sauter Infomax S.A.

Responsables

- Administración
- Personal de soporte técnico
- Colaboradores responsables de áreas operativas

Procedimiento

Protección eléctrica:

- Los equipos tecnológicos deberán utilizar reguladores de voltaje y sistemas UPS cuando corresponda.
- Se realizarán revisiones periódicas de conexiones eléctricas.

Control de temperatura y ventilación:

- Las áreas con equipos tecnológicos deberán contar con ventilación adecuada.
- Se deberá evitar la exposición de equipos a humedad, polvo o calor excesivo.

Protección contra incendios:

- La empresa dispondrá de extintores en áreas estratégicas.
- Los colaboradores deberán conocer las rutas de evacuación y medidas básicas de emergencia.

Mantenimiento preventivo:

- Se realizarán revisiones periódicas de equipos tecnológicos e infraestructura.
- Toda anomalía detectada deberá documentarse y corregirse oportunamente.

Reporte de riesgos ambientales:

- Cualquier condición ambiental que represente un riesgo deberá ser reportada a la administración.
- Los incidentes deberán registrarse para seguimiento y mejora continua.

Procedimiento de Monitoreo y Vigilancia Física

Objetivo

Establecer los lineamientos para el monitoreo y vigilancia de las instalaciones, activos físicos y equipos tecnológicos de Sauter Infomax S.A., con el propósito de detectar oportunamente incidentes, accesos no autorizados y condiciones de riesgo que puedan afectar la seguridad de la información y la continuidad operativa.

Alcance

El presente procedimiento aplica a todas las áreas administrativas, operativas y tecnológicas incluidas dentro del alcance del SGSI de Sauter Infomax S.A.

Responsables

- Administración
- Personal de soporte técnico
- Colaboradores autorizados
- Encargado de vigilancia o supervisión interna

Procedimiento

Monitoreo de accesos físicos:

- La empresa supervisará el ingreso y salida de colaboradores, visitantes y proveedores.
- Todo visitante deberá registrarse previamente y permanecer acompañado en áreas restringidas.
- Se revisarán periódicamente las bitácoras de acceso para identificar accesos no autorizados.

Vigilancia de áreas críticas:

- Las áreas con equipos tecnológicos, documentos sensibles o infraestructura crítica deberán mantenerse bajo supervisión periódica.
- Se recomienda el uso de cámaras de monitoreo, supervisión administrativa o controles físicos de acceso.

Supervisión de equipos tecnológicos:

- El personal encargado verificará periódicamente el estado físico de computadoras, servidores, reguladores, UPS y demás dispositivos.

- Se comprobará que los equipos permanezcan en condiciones adecuadas de ventilación, protección eléctrica y seguridad física.

Monitoreo de condiciones ambientales:

- La empresa realizará revisiones periódicas de temperatura, ventilación, riesgos eléctricos, humedad y estado de reguladores.
- Cualquier anomalía detectada deberá documentarse y reportarse para su atención oportuna.

Registro y seguimiento de incidentes:

- Todo incidente de seguridad física deberá registrarse formalmente mediante bitácoras o reportes internos.
- Los incidentes incluyen accesos no autorizados, pérdida de equipos, fallas eléctricas, riesgos ambientales y fallos en sistemas de vigilancia.

Evidencias y registros

- Bitácoras de ingreso y salida
- Registros de visitantes
- Reportes de incidentes físicos
- Registros de monitoreo ambiental
- Evidencias de supervisión de equipos
- Informes de seguimiento y acciones correctivas

Procedimiento de Manejo y Almacenamiento de Información Física

Objetivo

Establecer los lineamientos para el manejo, custodia, almacenamiento, retención y destrucción controlada de documentos físicos y otros medios de almacenamiento de información en Sauter Infomax S.A., garantizando su protección frente a pérdida, daño, acceso no autorizado o divulgación indebida, conforme a los controles 7.7, 7.10 y 7.14 de la norma ISO/IEC 27002:2022.

Alcance

El presente procedimiento aplica a todos los colaboradores, áreas administrativas y operativas que gestionen, manipulen, almacenen o dispongan de documentos impresos, expedientes, contratos, registros contables, dispositivos de almacenamiento físico (USB, discos duros externos, CD/DVD) o cualquier otro soporte físico que contenga información organizacional.

Responsables

- Administración: aprobación del procedimiento y supervisión general
- Personal administrativo: manejo cotidiano de documentos físicos
- Soporte técnico: gestión de dispositivos de almacenamiento físico
- Todos los colaboradores: cumplimiento de las disposiciones establecidas

Tabla 22 Clasificación de soportes físicos por nivel de riesgo

Tipo de soporte	Ejemplos	Riesgo principal	Nivel de riesgo
Documentos en papel	Contratos, expedientes, registros contables	Acceso no autorizado, pérdida, deterioro	Alto
Dispositivos USB	Memorias flash, pendrives	Robo, pérdida, infección por malware	Alto
Discos duros externos	HDD, SSD externos	Robo, daño físico, acceso no autorizado	Alto
CD/DVD	Respaldos en disco óptico	Deterioro físico, pérdida	Medio
Registros internos impresos	Manuales, procedimientos, actas	Divulgación indebida	Medio

Procedimiento

Custodia y almacenamiento de documentos físicos:

- Los documentos clasificados como de alta criticidad (contratos, expedientes financieros, registros contables) deberán almacenarse en archivadores metálicos con llave, ubicados en áreas de acceso restringido.
- Los documentos de criticidad media deberán mantenerse en archivadores ordenados, accesibles únicamente al personal autorizado.

- Los documentos de baja criticidad podrán almacenarse en estantes o archivos generales, debidamente organizados y etiquetados.
- No deberán dejarse documentos sensibles sin custodia sobre escritorios o en áreas de acceso general (principio de escritorio limpio, control 7.7 ISO/IEC 27002:2022).

Ciclo de retención documental:

- La administración definirá los plazos de retención de cada tipo de documento conforme a los requisitos legales y operativos de la organización (Ley N.° 8968 y normativa tributaria aplicable).
- Los documentos que superen el período de retención establecido deberán someterse al proceso de destrucción controlada descrito en este procedimiento.
- Se mantendrá un registro de los documentos vigentes y sus fechas de vencimiento.

Gestión de dispositivos de almacenamiento físico:

- Todo dispositivo USB, disco duro externo o medio óptico utilizado para almacenamiento de información organizacional deberá estar registrado en el inventario de activos.
- Su uso quedará restringido al personal autorizado y deberá realizarse únicamente para fines organizacionales.
- Los dispositivos no utilizados deberán almacenarse en un lugar seguro, bajo custodia de la administración o del área de soporte técnico.

Destrucción controlada de documentos e información:

- Los documentos físicos que ya no sean requeridos deberán destruirse mediante trituradora de papel o mecanismo equivalente que garantice su ilegibilidad.
- Los dispositivos de almacenamiento físico fuera de uso deberán someterse a un proceso de borrado seguro o destrucción física antes de su descarte.
- Todo proceso de destrucción deberá registrarse formalmente, consignando fecha, tipo de material destruido, responsable y método de destrucción aplicado.

Restricciones de manejo:

- Está prohibida la reproducción o copia de documentos clasificados sin autorización expresa de la administración.
- Los documentos físicos no deberán retirarse de las instalaciones sin la debida autorización.

- En caso de detección de pérdida o acceso no autorizado a documentos o dispositivos, deberá activarse el Procedimiento de Gestión y Reporte de Incidentes de Seguridad Física.

Evidencias y registros

- Inventario de documentos y dispositivos de almacenamiento
- Registro de ciclo de retención documental
- Registros de acceso a archivadores y áreas de custodia
- Actas de destrucción controlada de documentos y dispositivos
- Reportes de incidentes relacionados con información física

Procedimiento de Gestión y Reporte de Incidentes de Seguridad Física y del Entorno

Establecer el procedimiento para la identificación, reporte, registro, atención y seguimiento de incidentes relacionados con la seguridad física y del entorno dentro de Sauter Infomax S.A., con el propósito de reducir impactos sobre los activos físicos, tecnológicos y de información.

El presente procedimiento aplica a todos los colaboradores, proveedores, visitantes y terceros que tengan acceso a las instalaciones, equipos tecnológicos o información física de la empresa.

Responsables

- Administración
- Personal de soporte técnico
- Colaboradores de la organización
- Personal autorizado para atención de incidentes

Procedimiento

Identificación del incidente:

- Todo colaborador deberá identificar y comunicar cualquier situación anormal o riesgo de seguridad física.
- La detección podrá realizarse mediante observación directa, reportes del personal, revisiones de monitoreo, bitácoras o sistemas de vigilancia.

Reporte del incidente:

- El incidente deberá ser reportado inmediatamente a la administración.
- El reporte incluirá fecha, hora, lugar, descripción, activos afectados, personas involucradas y evidencias disponibles.

  Registro y seguimiento:

- Todo incidente deberá documentarse formalmente mediante registros o bitácoras internas.
- La administración evaluará el impacto y determinará las acciones correctivas, preventivas o escalamiento interno.
- El cierre del incidente solo procederá cuando esté controlado y documentado formalmente.

Evidencias y registros

- Reportes y bitácoras de incidentes físicos
- Evidencias fotográficas cuando aplique
- Registros de acciones correctivas e informes de seguimiento

Plan de Capacitación y Concientización

El fortalecimiento de la cultura organizacional en materia de seguridad constituye un elemento fundamental dentro del SGSI. El plan de capacitación define los temas, contenido programático, responsables, frecuencia y participantes de las actividades de formación, con el propósito de garantizar que sea un instrumento ejecutable y no solo un anuncio de intenciones.

Tabla 23 Plan de capacitación y concientización

Tema	**Contenido programático(3-5 tópicos por sesión)**	**Materiales**	**Responsable**	**Frecuencia**	**Participantes**
Seguridad física y control de acceso	1.Conceptos de seguridad física. 2. Uso correcto de credenciales 3. Zonas restringidas	Presentación, manual de procedimiento , formulario de registro de visitantes	Administración	Trimestral	Todo el personal

	y procedimiento de acceso. 4. Registro de visitantes. 5. Reporte de accesos sospechosos.				
Protección de activos tecnológicos	1. Inventario y clasificación de activos. 2. Uso responsable de equipos. 3. Bloqueo de pantalla y escritorio limpio. 4. Mantenimiento preventivo básico. 5. Qué hacer ante fallo de equipo.	Presentación, guía de uso de equipos, checklist de mantenimiento	Soporte técnico	Semestral	Colaboradores
Manejo seguro de información física	1. Clasificación de documentos. 2. Custodia y almacenamiento correcto. 3. Principio de escritorio limpio. 4. Ciclo de retención documental. 5.	Presentación, procedimiento de manejo documental, acta de destrucción	Administración	Semestral	Personal administrativo

	Destrucción controlada de documentos.				
Prevención de incidentes físicos	1. Tipos de incidentes físicos más frecuentes. 2. Cómo identificar riesgos. 3. Procedimiento de reporte. 4. Cadena de responsabilidad. 5. Casos de ejemplo y lecciones aprendidas.	Presentación, formulario de reporte de incidentes, bitácora	Administración	Trimestral	Todo el personal
Respuesta ante emergencias	1. Plan de evacuación. 2. Uso de extintores. 3. Protocolos ante falla eléctrica. 4. Cadena de contactos de emergencia. 5. Simulacro y retroalimentación.	Presentación, mapa de evacuación, lista de contactos de emergencia	Administración	Anual	Todo el personal

Fuente: Elaboración propia, 2026.

Evaluación y seguimiento

Las actividades de capacitación deberán documentarse mediante listas de asistencia, evidencias fotográficas y registros de evaluación. Se aplicará una prueba corta al finalizar cada sesión para verificar el nivel de comprensión. Los resultados serán analizados por la administración y alimentarán el indicador de porcentaje de personal capacitado, definido en la matriz de indicadores de desempeño.

Plan de Acción y Mejora Continua (PHVA)

Con el propósito de garantizar la sostenibilidad y efectividad de los controles propuestos, se establece un Plan de Acción basado en el ciclo PHVA (Planificar – Hacer – Verificar – Actuar), principio fundamental de la norma ISO/IEC 27001:2022. Cada fase genera productos concretos que permiten verificar el avance del sistema.

Tabla 24 Plan de acción y mejora continua del SGSI

Fase PHVA	**Actividad**	**Responsable**	**Tiempo estimado**	**Hito verificable**
Planificar	Identificación de riesgos y necesidades de seguridad	Administración	Mensual	Matriz de riesgos actualizada
Planificar	Definición y actualización de políticas y procedimientos	Administración	Trimestral	Política y procedimientos aprobados
Hacer	Implementación de controles físicos y ambientales	Soporte técnico / Administración	Permanente	Controles operativos documentados
Hacer	Capacitación y concientización del personal	Administración / RRHH	Trimestral	Lista de asistencia y evaluación
Verificar	Revisión de cumplimiento de controles mediante listas de verificación	Administración	Mensual	Informe de cumplimiento
Verificar	Registro, análisis y seguimiento de incidentes	Administración	Permanente	Bitácora de incidentes actualizada

Actuar	Aplicación de acciones correctivas ante desviaciones	Administración	Según incidentes	Registro de acciones correctivas
Actuar	Actualización de procedimientos, controles y SoA	Administración	Semestral	Versión actualizada de documentos

Fuente: Elaboración propia, 2026.

Indicadores de Desempeño con Umbrales

Los indicadores de desempeño permiten evaluar la eficacia de los controles implementados, detectar desviaciones y orientar la toma de decisiones dentro del SGSI. Cada indicador incluye su objetivo de medición, método, frecuencia, umbral esperado, responsable de medición y acción requerida cuando se supera el umbral.

Tabla 25 Indicadores de desempeño y umbrales del SGSI

Indicador	**Objetivo**	**Método de medición**	**Frecuencia**	**Umbral esperado**	**Responsable de medición**	**Acción requerida si se supera umbral**
Cantidad de incidentes físicos reportados	Reducir incidentes de seguridad	Registro de incidentes	Mensual	Máximo 2 incidentes/mes	Administración	Análisis de causa raíz y acciones correctivas inmediatas
Tiempo de respuesta ante incidentes	Mejorar capacidad de atención	Tiempo promedio de resolución	Mensual	Menor a 30 minutos	Administración	Revisar y actualizar el procedimiento de incidentes
Porcentaje de personal capacitado	Fortalecer cultura de seguridad	Registros de asistencia y evaluación	Trimestral	≥90% del personal	RRHH / Administración	Programar sesiones adicionales de

						capacitación
Cumplimiento de controles físicos	Verificar aplicación de controles	Listas de verificación internas	Mensual	≥85% de cumplimiento	Administración	Reforzar supervisión y actualizar controles deficientes
Accesos no autorizados detectados	Minimizar vulnerabilidades de acceso	Revisión de bitácoras	Mensual	0 accesos no autorizados	Administración	Revisar y reforzar controles de acceso físico
Mantenimiento preventivo realizado	Garantizar protección de equipos	Reportes técnicos de mantenimiento	Trimestral	100% de equipos revisados	Soporte técnico	Ejecutar mantenimiento pendiente e investigar causa de omisión
Registro de visitantes completado	Fortalecer control de ingreso	Revisión de bitácoras de visitantes	Mensual	≥95% de registros completos	Recepción / Administración	Reforzar control en la recepción y capacitar al personal

Fuente: Elaboración propia, 2026.

Equipo implementador y esquema de seguimiento

Para garantizar una implementación adecuada de la propuesta de Seguridad Física y del Entorno, se plantea un **modelo mixto de implementación**, conformado por responsables internos de Sauter Infomax S.A. y el acompañamiento periódico de un tercero especializado en seguridad de la información.

La selección de este modelo responde a que la organización posee una estructura aproximada de 15 a 18 colaboradores y actualmente no cuenta con un área interna exclusiva de auditoría o seguridad de la información que pueda asumir de manera independiente la implementación, evaluación y seguimiento de los controles propuestos. Por esta razón, no se considera conveniente trasladar esta responsabilidad a Recursos Humanos, debido a que sus funciones se relacionan principalmente con la gestión del personal y las actividades de capacitación y concientización.

Internamente, la **Administración** actuará como responsable de la coordinación organizacional de la propuesta, aprobación de políticas y procedimientos, asignación de recursos y seguimiento de las acciones de mejora. El área de **Soporte Técnico** será responsable de la ejecución y mantenimiento de los controles relacionados con infraestructura, equipos tecnológicos, monitoreo y condiciones físicas y ambientales.

Recursos Humanos tendrá una participación de apoyo, limitada principalmente a la coordinación de las actividades de capacitación, concientización y conservación de los registros correspondientes. Por tanto, esta área no tendrá bajo su responsabilidad la evaluación independiente del cumplimiento de los controles.

Como complemento del equipo interno, se recomienda la contratación de un **proveedor externo especializado en seguridad de la información**, cuya función será brindar acompañamiento técnico durante la implementación y realizar evaluaciones independientes sobre el cumplimiento y eficacia de los controles. Entre sus funciones se contemplan la revisión de la documentación generada, validación de evidencias, revisión de la matriz de riesgos y de la Declaración de Aplicabilidad (SoA), identificación de desviaciones y emisión de recomendaciones de mejora.

Durante los cuatro meses contemplados en la hoja de ruta de implementación, se propone que el tercero especializado realice una **revisión inicial**, una **revisión intermedia** y una **revisión final**, de manera que pueda verificarse progresivamente la correcta aplicación de la propuesta. Posteriormente, una vez estabilizados los controles, se recomienda efectuar una evaluación externa con una **frecuencia anual**, o extraordinariamente cuando se presenten cambios significativos en infraestructura, riesgos, procesos o controles.

De esta manera, la organización mantiene internamente la responsabilidad sobre la ejecución cotidiana de los controles, mientras que la evaluación especializada se realiza con mayor independencia, evitando asignar funciones de auditoría a áreas que participan directamente en la operación.

Tabla 26 Ejecución cotidiana de los controles

Integrante	**Tipo**	**Función principal**	**Frecuencia**
Administración	Interno	Coordinar implementación, aprobar documentos, asignar recursos y revisar resultados	Mensual
Soporte Técnico	Interno	Implementar y mantener controles técnicos, físicos y ambientales	Permanente
Recursos Humanos	Interno / apoyo	Coordinar capacitación y conservar evidencias de formación	Trimestral
Colaboradores	Interno	Cumplir procedimientos y reportar incidentes	Permanente

Tercero especializado	Externo	Acompañar, revisar evidencias, evaluar controles y emitir recomendaciones	Inicial, intermedia y final durante implementación; posteriormente anual

Fuente: Elaboración propia, 2026.

Matriz RACI del SGSI

La matriz RACI permite definir claramente los roles y responsabilidades dentro del SGSI. Las siglas corresponden a: R (Responsible – ejecuta), A (Accountable – responsable final), C (Consulted – consultado), I (Informed – informado).

Actividad	Administración	Soporte Técnico	Colaboradores	Recursos Humanos	Proveedor externo
Elaboración y revisión de políticas de seguridad	A/R	C	I	C	I
Control de acceso físico	A	R	I	I	I
Monitoreo de instalaciones	C	R	I	I	I
Gestión de incidentes físicos	A	R	C	I	I
Protección de equipos tecnológicos	C	A/R	I	I	I
Capacitación y concientización de seguridad	A	C	I	R	I
Manejo y almacenamiento de información física	A	C	R	I	I
Seguimiento de indicadores	A/R	C	I	I	C
Revisión y actualización de procedimientos	A	C	I	I	C
Evaluación y actualización de riesgos	A	R	C	I	C
Revisión y actualización del SoA	A/R	C	I	I	C

Evaluación independiente de los controles	C	C	I	I	A/R

Fuente: Elaboración propia, 2026

Cronograma de propuesta de implementación de controles de seguridad física y del entorno dentro del marco de un SGSI alineado con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Con el propósito de organizar las actividades relacionadas con la implementación progresiva propuesta de implementación de controles de seguridad física y del entorno dentro del marco de un SGSI alineado con las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022., se establece el siguiente cronograma de trabajo a cuatro meses. Al final de cada mes se indica el hito crítico verificable que confirma el avance del proceso.

Tabla 27 Cronograma

Actividad	**Responsable**	**Mes 1**	**Mes 2**	**Mes 3**	**Mes 4**	**Hito crítico al cierre del mes**
Diagnóstico de seguridad física	Administración	X				Mes 1: Informe de diagnóstico con brechas identificadas
Evaluación de riesgos y SoA	Administración / Soporte	X	X			Mes 2: Matriz de riesgos y SoA aprobados
Definición del alcance del SGSI	Administración	X				Mes 1: Documento de alcance firmado
Elaboración de políticas	Administración		X			Mes 2: Política de seguridad física aprobada

Desarrollo de procedimientos documentados	Administración / Soporte		X	X		Mes 3: Cinco procedimientos documentados y aprobados
Implementación de controles físicos	Soporte técnico			X	X	Mes 4: Controles físicos operativos verificados
Capacitación del personal	RRHH / Administración			X	X	Mes 4: ≥90% del personal capacitado
Implementación de monitoreo y vigilancia	Soporte técnico			X	X	Mes 4: Sistema de monitoreo operativo con bitácoras activas
Seguimiento de indicadores KPI	Administración				X	Mes 4: Primer informe de KPI generado
Revisión interna y auditoría inicial	Administración				X	Mes 4: Informe de revisión interna con acciones de mejora

Fuente: Elaboración propia, 2026.

Conclusión de la Propuesta

La propuesta de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) orientada a la seguridad física y del entorno en Sauter Infomax S.A. constituye una respuesta técnica, metodológica y documentalmente fundamentada a los hallazgos identificados en el diagnóstico del Capítulo IV, que evidenciaron la ausencia de políticas formales, controles de acceso no estructurados, procedimientos no documentados y mecanismos insuficientes de seguimiento y monitoreo.

En relación con el cumplimiento de los objetivos específicos, el Capítulo V aporta los siguientes entregables: respecto al OE2, se definió el contexto organizacional, se identificaron las partes interesadas conforme a la Cláusula 4.2, se delimitó el alcance bajo la Cláusula 4.3, se clasificaron los activos por nivel de criticidad y se estableció la relación entre activos y controles de protección. Respecto al OE3, se elaboraron la Política de Seguridad Física y del Entorno y cinco procedimientos documentados: Control de Acceso Físico, Seguridad Ambiental, Monitoreo y Vigilancia Física, Manejo y Almacenamiento de Información Física, y Gestión y Reporte de Incidentes. Respecto al OE4, se desarrollaron la Matriz de Riesgos con metodología Probabilidad × Impacto, la Declaración de Aplicabilidad (SoA) con trazabilidad Control → Procedimiento → Evidencia, y la Matriz RACI con roles y responsabilidades definidos. Respecto al OE5, se establecieron el Plan de Acción PHVA con hitos verificables, el Plan de Capacitación con contenido programático detallado, los Indicadores de Desempeño con umbrales y responsables, y el Cronograma de Implementación a cuatro meses con hitos críticos mensuales.

El aporte concreto para Sauter Infomax S.A. radica en que la organización pasa de una gestión empírica de la seguridad a contar con un conjunto estructurado de políticas, procedimientos y mecanismos de evaluación que fortalecen la protección de sus activos físicos, tecnológicos y documentales, reducen la exposición a riesgos identificados y promueven una cultura organizacional orientada a la prevención.

Finalmente, es importante reconocer las limitaciones explícitas de esta propuesta: su alcance está acotado a la seguridad física y del entorno, no constituye la implementación completa de un SGSI certificado bajo la norma ISO/IEC 27001:2022, y la validación empírica de los controles propuestos queda pendiente de ejecución y pilotaje por parte de la organización. No obstante, los elementos desarrollados representan una base sólida para que Sauter Infomax S.A. avance progresivamente hacia niveles más altos de madurez en la gestión de la seguridad de la información.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Conclusiones

A partir del desarrollo de la presente investigación, orientada a la propuesta de implementación de la seguridad física y del entorno en la empresa Sauter Infomax S.A., conforme a la norma ISO/IEC 27001:2022, se establecen las siguientes conclusiones en correspondencia con cada uno de los objetivos específicos planteados:

En relación con el primer objetivo específico, referido al análisis de la situación actual de la seguridad física y del entorno, se concluye que la empresa Sauter Infomax S.A. no cuenta con mecanismos formales de protección de sus activos físicos y tecnológicos. A través de la aplicación del análisis FODA, el cuestionario, la entrevista y la guía de observación, se identificaron brechas significativas tales como la ausencia de un registro formal de visitantes, la inexistencia de áreas restringidas debidamente delimitadas y la falta de procedimientos documentados para la gestión de incidentes físicos. Estas debilidades incrementan la exposición de la organización a riesgos relacionados con accesos no autorizados, daños ambientales y pérdida de información, evidenciando la necesidad urgente de implementar controles alineados con la norma ISO/IEC 27001:2022.

En cuanto al segundo objetivo específico, orientado a determinar los requerimientos normativos, el alcance y los elementos críticos del SGSI, se concluye que fue posible establecer un alcance claro del sistema, delimitando los activos, procesos, infraestructura y responsabilidades que forman parte del ámbito de aplicación de la propuesta. La identificación de las partes interesadas, la elaboración del mapa de cobertura y el desarrollo de la Declaración de Aplicabilidad (SoA) permitieron vincular de manera trazable cada control de la norma ISO/IEC 27002:2022 con los procedimientos diseñados, garantizando coherencia normativa y pertinencia organizacional en la propuesta.

Respecto al tercer objetivo específico, relativo a la elaboración de la política y los procedimientos documentados de seguridad física y del entorno, se concluye que fue posible desarrollar una política institucional y cinco procedimientos documentados que abordan el control de acceso físico, la seguridad ambiental, el monitoreo y vigilancia, el manejo y almacenamiento de

información física, y la gestión y reporte de incidentes. Estos instrumentos se encuentran alineados con los controles del dominio 7 de la norma ISO/IEC 27002:2022 y constituyen la base operativa del SGSI propuesto, proporcionando a la organización lineamientos claros, medibles y aplicables para la protección de sus activos.

En lo que concierne al cuarto objetivo específico, vinculado al desarrollo de instrumentos investigativos y de apoyo técnico, se concluye que la construcción de la matriz de riesgos, la Declaración de Aplicabilidad, la matriz RACI, los indicadores de desempeño con umbrales y los cuadros comparativos permitieron respaldar de manera sólida la propuesta. Estos instrumentos facilitaron la identificación de vulnerabilidades, la selección justificada de controles y la definición de responsabilidades, contribuyendo a que la propuesta cuente con una base técnica y metodológica coherente con las exigencias de la norma ISO/IEC 27001:2022.

Finalmente, en relación con el quinto objetivo específico, concerniente al plan de acción y mejora continua, se concluye que el diseño del plan basado en el ciclo PHVA, acompañado del cronograma de implementación, los indicadores de desempeño y el programa de capacitación, dota a la organización de una hoja de ruta estructurada para la implementación progresiva y sostenible del SGSI. Este enfoque garantiza que los controles no sean aplicados de manera aislada, sino integrados dentro de un sistema de gestión que promueve la evaluación continua, la corrección oportuna de desviaciones y la mejora permanente de la seguridad física y del entorno.

Recomendaciones

Con base en los hallazgos obtenidos y en las conclusiones derivadas de la investigación, se plantean las siguientes recomendaciones dirigidas a la empresa Sauter Infomax S.A., en correspondencia con cada uno de los objetivos específicos del estudio:

En atención al primer objetivo específico, se recomienda que la empresa adopte el diagnóstico realizado como punto de partida formal para la gestión de la seguridad, estableciendo un proceso periódico de revisión del contexto organizacional, no menor a una vez por año, que permita identificar nuevas brechas, cambios en el entorno operativo y variaciones en el perfil de riesgos. Para ello, se sugiere mantener actualizados los instrumentos de diagnóstico utilizados en

esta investigación, en particular el análisis FODA y la guía de observación, incorporándolos como herramientas permanentes dentro del sistema de gestión.

En relación con el segundo objetivo específico, se recomienda que la dirección de la empresa formalice y apruebe oficialmente el alcance del SGSI definido en esta propuesta, garantizando que todos los colaboradores conozcan los límites del sistema, los activos incluidos y las responsabilidades asociadas. Asimismo, se sugiere revisar la Declaración de Aplicabilidad al menos una vez al año o ante cambios significativos en la infraestructura, los procesos o el entorno normativo, con el fin de mantener la trazabilidad entre los riesgos identificados y los controles implementados.

Respecto al tercer objetivo específico, se recomienda que la empresa proceda a la implementación efectiva de la política de seguridad física y del entorno y los cinco procedimientos documentados desarrollados en esta investigación, comenzando por aquellos que atienden los riesgos de mayor criticidad identificados en la matriz de riesgos, tales como el control de acceso físico y el monitoreo de instalaciones. Se sugiere que cada procedimiento sea socializado con el personal mediante sesiones de capacitación, que se asignen responsables formales para su ejecución y que se definan registros de cumplimiento que permitan evidenciar su aplicación ante futuras revisiones o auditorías.

En cuanto al cuarto objetivo específico, se recomienda que la organización adopte los instrumentos metodológicos desarrollados en esta investigación como herramientas de gestión permanente, incorporando la matriz de riesgos, la matriz RACI y los indicadores de desempeño dentro de sus procesos de revisión periódica. Se sugiere además designar un responsable interno, preferiblemente del área técnica o administrativa, que sea el encargado de mantener actualizados estos instrumentos y de reportar los resultados a la gerencia, asegurando así la continuidad del sistema y la toma de decisiones basada en información objetiva.

Finalmente, en correspondencia con el quinto objetivo específico, se recomienda que la empresa implemente el plan de acción propuesto respetando el cronograma definido, priorizando las actividades del primer mes relacionadas con el diagnóstico formal, la aprobación del alcance y la definición de políticas. Se sugiere que la gerencia asuma un rol activo en el seguimiento del plan, revisando mensualmente los indicadores de desempeño establecidos y tomando acciones correctivas ante cualquier desviación detectada. A mediano plazo, se recomienda considerar la

ejecución de una auditoría interna del SGSI y, como meta organizacional de largo plazo, evaluar la posibilidad de avanzar hacia la certificación bajo la norma ISO/IEC 27001:2022, lo cual fortalecería la imagen institucional, incrementaría la confianza de los clientes y posicionaría a Sauter Infomax S.A. como una organización comprometida con la gestión responsable de la información.

REFERENCIAS

Asamblea Legislativa de la República de Costa Rica. (2011). *Ley N.º 8968: Protección de la persona frente al tratamiento de sus datos personales.*

Calder, A. (2019). *Implementing ISO/IEC 27001:2013: A practical guide to information security management* (4.ª ed.). IT Governance Publishing.

Calder, A. (2019). *ISO/IEC 27001:2013: A pocket guide* (3rd ed.). IT Governance Publishing.

Delta Protect. (2022, 14 de junio). ¿Qué es la norma ISO 27001 y para qué sirve? https://www.deltaprotect.com/blog/que-es-iso-27001

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2018). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education.

Hernández Sampieri, R., & Mendoza Torres, C. P. (2023). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta* (2.ª ed.). McGraw-Hill Education.

INCIBE-CERT. (2021, 21 de julio). El punto en el que seguridad y ciberseguridad convergen. Blog de INCIBE. https://www.incibe.es/incibe-cert/blog/el-punto-el-seguridad-y-ciberseguridad-convergen

Innevo. (2022, 28 de junio). Evaluación de riesgos según ISO 27001. https://innevo.com/blog/evaluacion-de-riesgos-iso27001

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

Kendall, K. E., & Kendall, J. E. (2011). *Análisis y diseño de sistemas* (8.ª ed.). Pearson Educación.

Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16.ª ed.). Pearson Education.

NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Versión 1.1). National Institute of Standards and Technology.

Organización Internacional de Normalización. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO. https://www.iso.org/standard/27001.html

PiraniRisk. (2025). Etapas de una auditoría interna. https://www.piranirisk.com/es/blog/etapas-y-fases-de-la-auditoria-interna

Real Academia Española. (s.f.). Negocio. En *Diccionario de la lengua española*. https://dle.rae.es/negocio

Wallarm. (s.f.). Definición de la tríada de la CIA: ejemplos de confidencialidad, integridad y disponibilidad. https://lab.wallarm.com/what/definicion-de-la-triada-de-la-cia-ejemplos-de-confidencialidad-integridad-y-disponibilidad/

ANEXOS

Anexo 1 Cuestionario

En el marco de una investigación sobre Propuesta de implementación de controles de seguridad física y del entorno basados en la norma ISO/IEC 27001:2022 en la empresa Sauter Infomax S.A., le invitamos a completar este cuestionario. Su participación es de gran importancia para comprender cómo el tema en estudio influye en la actividad de la organización.

Este cuestionario es confidencial. Sus respuestas solo se utilizarán con fines académicos y no serán compartidas con otras personas. Completar el cuestionario tomará aproximadamente 10 minutos.

1. ¿Conoce usted si la empresa cuenta con medidas de seguridad física para proteger las instalaciones y los equipos?

☐ Sí

☐ No

☐ No estoy seguro(a)

2. ¿Considera que el acceso a las instalaciones de la empresa está adecuadamente controlado?

☐ Totalmente de acuerdo

☐ De acuerdo

☐ Neutral

☐ En desacuerdo

☐ Totalmente en desacuerdo

3. ¿Las áreas donde se encuentra información o equipos importantes tienen algún tipo de restricción de acceso?

☐ Sí

☐ No

☐ No lo sé

4. ¿Ha recibido capacitación o información sobre normas de seguridad dentro de la empresa?

☐ Sí

☐ No

5. ¿Considera que existen riesgos físicos que podrían afectar la seguridad de los equipos o la información de la empresa?

☐ Sí

☐ No

☐ No estoy seguro(a)

6. ¿En la empresa existen controles para proteger los equipos tecnológicos (computadoras, servidores, dispositivos)?

☐ Sí

☐ No

☐ No lo sé

7. ¿Cree usted que las condiciones del entorno (electricidad, temperatura, espacio físico) son adecuadas para proteger los equipos y la información?

☐ Totalmente de acuerdo

☐ De acuerdo

☐ Neutral

☐ En desacuerdo

☐ Totalmente en desacuerdo

8. ¿En caso de presentarse un incidente de seguridad física (robo, acceso no autorizado, daño a equipos), sabe a quién reportarlo?

☐ Sí

☐ No

9. ¿Considera importante que la empresa implemente procedimientos documentados de seguridad física y control de acceso?

☐ Muy importante

☐ Importante

☐ Poco importante

☐ Nada importante

10. ¿Cree que mejorar la seguridad física ayudaría a proteger mejor la información y los activos de la empresa?

☐ Sí

☐ No

☐ No estoy seguro(a)

11. ¿Considera que la empresa debería implementar controles adicionales como cámaras, registro de visitantes o control de credenciales?

☐ Totalmente de acuerdo

☐ De acuerdo

☐ Neutral

☐ En desacuerdo

☐ Totalmente en desacuerdo

12. En general, ¿cómo evaluaría el nivel actual de seguridad física dentro de la empresa?

☐ Muy alto

☐ Alto

☐ Medio

☐ Bajo

☐ Muy bajo

Anexo 2 Entrevista

Entidad:	**Sauter Infomax S.A**
Nombre del entrevistado:	

Puesto del entrevistado:	
Nombre del estudiante:	**Mariana Chinchilla Murillo.**
Fecha de la entrevista:	
Lugar o medio de la entrevista:	

Preguntas

1. ¿Cómo describiría actualmente las medidas de seguridad física implementadas en la empresa para proteger las instalaciones y los equipos?

2. ¿Qué controles existen actualmente para regular el acceso de personas a las instalaciones o a las áreas donde se encuentran equipos o información importante?

3. Desde su perspectiva, ¿cuáles considera que son los principales riesgos físicos o ambientales que podrían afectar la seguridad de los activos de la empresa?

4. ¿La empresa cuenta con procedimientos o políticas documentadas relacionadas con la seguridad física o el control de accesos?

5. ¿Qué tipo de controles se aplican para proteger los equipos tecnológicos y la infraestructura física de la empresa?

6. ¿Cómo se gestionan actualmente los incidentes relacionados con seguridad física, como accesos no autorizados, pérdidas de equipos o daños en la infraestructura?

7. ¿Se realizan capacitaciones o acciones de concientización al personal sobre seguridad de la información y protección de activos?

8. ¿Considera que la empresa cuenta con las condiciones ambientales adecuadas (electricidad, ventilación, espacio físico) para proteger los equipos tecnológicos?

9. Desde su experiencia, ¿qué aspectos considera que deberían mejorarse para fortalecer la seguridad física y del entorno dentro de la empresa?

10. ¿Considera que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 podría beneficiar a la organización? ¿Por qué?

La guía de entrevista se aplicará a un colaborador con conocimiento del funcionamiento organizacional y de los procesos relacionados con la seguridad de la información dentro de la empresa Sauter Infomax S.A. El objetivo es obtener información cualitativa que permita comprender la situación actual de la seguridad física y del entorno, así como identificar posibles oportunidades de mejora dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

Anexo 3 Guía de observación

Entidad:	**Sauter Infomax S.A**
Dirección física de la entidad:	**San José centro**
Fecha de la actividad de observación:	
Nombre del estudiante:	**Mariana Chinchilla Murillos**

o	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
	Existencia de control de acceso físico a las instalaciones de la empresa				
1	Registro o control de ingreso de visitantes				
2	Protección física de equipos tecnológicos (computadoras, servidores, impresoras)				

o	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
3	Existencia de áreas restringidas para personal autorizado				
4	Protección contra riesgos ambientales (temperatura, humedad, polvo)				
5	Condiciones adecuadas de infraestructura (orden, espacio, ventilación)				

o	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
6	Existencia de sistemas de vigilancia o monitoreo (cámaras, supervisión)				
7	Condiciones de seguridad eléctrica y protección de equipos				
8	Existencia de controles para evitar acceso no autorizado a equipos				

o	Aspectos por observar	Cumple	No Cumple	Oportunidad de mejora	Detalle de Observación
9	Ubicación segura de equipos críticos o información sensible				

Anexo 4 Bitácora de control de acceso físico

N.°	Fecha	Nombre de la persona	Área de ingreso	Hora de entrada	Hora de salida	Motivo del ingreso	Autorizado por	Observaciones

Responsable del registro: Administración / responsable del control de acceso.

Frecuencia: Cada vez que se produzca un ingreso a un área de acceso restringido.

Anexo 5 Registro de visitantes

Objetivo: Mantener un registro de las personas externas que ingresan a las instalaciones y permitir la trazabilidad de su permanencia.

N.°	Fecha	Nombre del visitante	Empresa / institución	Persona que visita	Motivo de visita	Hora de ingreso	Hora de salida	Identificación verificada	Observaciones
								☐ Sí ☐ No	

Responsable del registro: Administración / recepción.

Frecuencia: Cada vez que ingrese una persona externa a las instalaciones.

Anexo 6 Formato de reporte de incidentes de Seguridad Física y del Entorno

Objetivo: Documentar los incidentes relacionados con la Seguridad Física y del Entorno y facilitar su atención, seguimiento y cierre.

Dato requerido	Información
N.° de incidente	
Fecha del incidente	
Hora del incidente	
Área / ubicación	
Persona que reporta	
Tipo de incidente	☐ Acceso ☐ Robo ☐ Daño ☐ Ambiental ☐ Eléctrico ☐ Otro
Activo o recurso afectado	
Descripción del incidente	
Acción inmediata realizada	
Responsable de atención	
Fecha y hora de atención	
Causa identificada	

Acción correctiva propuesta	
Estado	☐ Abierto ☐ En proceso ☐ Cerrado
Fecha de cierre	
Observaciones	

Firma del responsable: _____

Revisado por: _____

Fecha de revisión: ____ / ____ / _____

Frecuencia: Cada vez que se presente un incidente relacionado con la Seguridad Física y del Entorno.

Anexo 7 Lista de verificación de controles de Seguridad Física y del Entorno

Objetivo: Facilitar la revisión periódica del cumplimiento y funcionamiento de los controles implementados.

Fecha de revisión: ____ / ____ / _____

Responsable de la revisión: _____

N.°	Aspecto a verificar	Cumple	No cumple	N/A	Evidencia / observación	Acción requerida
1	Las áreas restringidas cuentan con mecanismos de control de acceso.	☐	☐	☐		
2	Se mantiene actualizado el registro de visitantes.	☐	☐	☐		
3	Los equipos críticos se encuentran protegidos físicamente.	☐	☐	☐		
4	Las cámaras de vigilancia se encuentran operativas.	☐	☐	☐		

5	Los registros de acceso se encuentran disponibles y actualizados.	☐	☐	☐		
6	Los equipos cuentan con mantenimiento preventivo vigente.	☐	☐	☐		
7	Se mantienen condiciones ambientales adecuadas en las áreas críticas.	☐	☐	☐		
8	La documentación física sensible se encuentra almacenada de forma segura.	☐	☐	☐		
9	Los incidentes detectados se encuentran registrados.	☐	☐	☐		
10	Las acciones correctivas identificadas cuentan con seguimiento.					

Anexo 8 Registro de mantenimiento preventivo

Objetivo: Mantener evidencia de las actividades de mantenimiento realizadas sobre los equipos y activos relacionados con la Seguridad Física y del Entorno.

N.°	**Fecha**	**Activo / equipo**	**Código de activo**	**Ubicación**	**Tipo de mantenimiento**	**Actividad realizada**	**Resultado**	**Responsable**	**Próxima revisión**
					☐ Preventivo ☐ Correctivo				

					☐ Preventivo ☐ Correctivo				
					☐ Preventivo ☐ Correctivo				
					☐ Preventivo ☐ Correctivo				
					☐ Preventivo ☐ Correctivo				

Anexo 9 Registro de capacitación y concientización

Objetivo: Mantener evidencia de las actividades de capacitación y concientización relacionadas con la Seguridad Física y del Entorno.

Tema de la capacitación: _____

Fecha: ____ / ____ / _____

Responsable / facilitador: _____

Objetivo de la capacitación:

_____

_____

N.°	Nombre del colaborador	Área	Asistencia	Evaluación realizada	Resultado	Firma
			☐ Sí ☐ No	☐ Sí ☐ No		
			☐ Sí ☐ No	☐ Sí ☐ No		
			☐ Sí ☐ No	☐ Sí ☐ No		
			☐ Sí ☐ No	☐ Sí ☐ No		
			☐ Sí ☐ No	☐ Sí ☐ No		

Cantidad de colaboradores programados: _____

Cantidad de colaboradores capacitados: _____

Porcentaje de participación: _____ %

Observaciones / acciones de seguimiento:

_____

_____

Responsable del registro: Recursos Humanos / Administración.