



UNIVERSIDAD SANTO TOMÁS
PRIMER CLAUSTRO UNIVERSITARIO DE COLOMBIA
T U N J A

TÍTULO INVESTIGACIÓN

Guía práctica para la implementación de ISO/IEC 27001

PROPONENTE(S)

Samuel Ricardo Bermúdez Núñez

DIRECTOR

Martha Susana Contreras Ortiz

Tunja

Fecha de presentación (20 de agosto de 2026)

CONTENIDO

1. FICHA TÉCNICA DE LA INVESTIGACIÓN	4
2. PLANTEAMIENTO DEL PROBLEMA	5
3. JUSTIFICACIÓN	7
4. OBJETIVOS.....	9
4.1 Objetivo General	9
4.2 Objetivos específicos	9
5. METODOLOGÍA	10
5.1 Metodología.....	10
6. ENTREGABLES	14
7. RESULTADOS.....	16
7.1 Objetivo 1	16
7.2 Resultado objetivo específico numero dos	25
7.2.1 Procedimiento para la identificación de los factores críticos.....	26
7.2.2 Criterios utilizados para determinar los factores críticos	26
7.2.3 Elaboración de la matriz final	28
7.2.4 Resultado del Objetivo Específico 2: Evaluación y Priorización de Controles (Anexo A)	29
8. Guia de implementación.....	34
8.1 Introducción a la guía de implementación	34
8.2 Requisitos para la implementación.....	34
8.3 Contexto de la organización.....	36
8.3.1Identificación del Contexto Organizacional	36
8.3.2 Identificación de Partes Interesadas.....	37
8.3.3Definición del Alcance del SGSI	39
8.4 Principales controles de seguridad	39
8.4.1 Roles y responsabilidades	50
8.5 Planificación del SGSI (Cláusula 6).....	50
8.5.1Identificación de Activos de Información.....	51

8.5.2 Evaluación de riesgos	52
8.5.3 Tratamiento de Riesgos.....	53
8.5.4 Declaración de Aplicabilidad (SoA).....	54
8.6 Apoyo (Cláusula 7)	54
8.6.1 Recursos del SGSI	54
8.6.2 Competencia.....	55
8.6.3 Concienciación y Capacitación	56
8.6.4 Gestión de la Comunicación	57
8.6.5 Control de la Información Documentada.....	57
8.7 Operación y Ejecución del SGSI (Cláusula 8)	58
8.8 Implementación de Controles del Anexo A (ISO/IEC 27001:2022)	58
8.9 Evaluación del Desempeño del SGSI (Cláusula 9).....	59
8.9.1 Auditoría Interna del SGSI	60
8.9.2 Revisión por la Dirección	63
8.9.3 Mejora Continua y Gestión de No Conformidades (Cláusula 10)	63
<u>9. CONCLUSIONES.....</u>	<u>65</u>
<u>10 REFERENCIAS</u>	<u>67</u>

1. FICHA TÉCNICA DE LA INVESTIGACIÓN

Título	Guía práctica para la implementación de ISO/IEC 27001
Nombre Estudiante (s)	Samuel Ricardo Bermúdez Núñez
Correo electrónico estudiante (s)	Samuel.bermudez@usantoto.edu.co
Director / codirector	Martha susana contreras
Línea de investigación	☒ Ingeniería del software ☐ Inteligencia Artificial ☐ Transformación Digital
Duración	4 meses
Palabras claves	ISO 27001, Auditoria, implementación de controles de sistemas, hallazgos de inconsistencias de software

2. PLANTEAMIENTO DEL PROBLEMA

Varias organizaciones a nivel mundial, se evidencian dificultades relacionadas con la ausencia de una gestión adecuada de la seguridad de la información, situación que se ve afectada por la falta de procesos alineados con los estándares internacionales establecidos en la norma ISO/IEC 27001. A nivel nacional, esta problemática se propicia en las pequeñas y medianas empresas del sector, donde la adopción de esquemas formales de ciberseguridad suele no ser tomada en cuenta por limitaciones presupuestales o falta de personal especializado en la materia. Esta vulnerabilidad aumenta el riesgo frente a posibles incidentes de seguridad que ponen en jaque la confidencialidad, integridad y disponibilidad de los activos de información, llevando a cabo impactos negativos en la continuidad operativa, la protección de datos sensibles y la confianza de clientes y aliados estratégicos (Chai & Zolkipli, 2021).

La ausencia de lineamientos para la identificación y gestión de riesgos, junto con la limitada implementación de controles técnicos y organizacionales, hace mucho más difícil el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). Debido a esto, persiste una brecha respecto a la capacidad de las organizaciones para prevenir, detectar y responder de manera eficiente ante posibles amenazas o incidentes de seguridad de la información (Alassaf & Alkhalifah, 2021). A pesar de que la literatura reciente aborda ampliamente la importancia de la ciberseguridad, existe aún un gran vacío en la caracterización detallada de brechas frente a la actualización de la norma ISO/IEC 27001:2022.

Por lo anterior, resulta de suma importancia analizar la aplicabilidad de la norma ISO/IEC 27001:2022, con el fin de identificar brechas en los procesos actuales de gestión de la seguridad de la información y establecer lineamientos que ayuden al fortalecimiento de los controles existentes. Esto ayudará a orientar a las organizaciones hacia un modelo de gestión más elaborado, promoviendo la mejora continua y el desarrollo de una cultura organizacional

enfocada en la protección de los activos de información (Annarelli et al., 2021).

En este marco, surge la siguiente pregunta de investigación: ¿De qué manera el análisis de aplicabilidad y brechas frente a los requisitos de la norma ISO/IEC 27001:2022 permite establecer lineamientos para el fortalecimiento de la gestión de la seguridad de la información en las organizaciones?

3. JUSTIFICACIÓN

En el contexto tecnológico actual, definido por el incremento en las ciberamenazas y la acelerada transformación digital de las organizaciones, el resguardo de los activos de información se ha convertido en un pilar estratégico. Sin embargo, existen vacíos significativos respecto a la realización de marcos internacionales actualizados en entornos empresariales concretos. En este escenario concreto, la elaboración del presente análisis sobre la norma ISO/IEC 27001:2022 da una respuesta a una necesidad sectorial real, que desemboca de las carencias en la gestión estructurada de la seguridad de la información. La ausencia de procesos establecidos incrementa de manera considerable la exposición a incidentes que comprometen la continuidad operativa, la confianza institucional y la custodia de datos sensibles (Alassaf & Alkhalifah, 2021).

Gracias a una perspectiva académica y disciplinar, esta investigación justifica su desarrollo al sintetizar y sistematizar la aplicación práctica del estándar ISO/IEC 27001:2022 en el contexto organizacional. El trabajo da un valor al conocimiento mediante la identificación analítica de brechas de seguridad, la evaluación de controles actualizados (incluidos los nuevos controles del Anexo A) y la propuesta de lineamientos conceptuales que tienen como fin la mitigación del riesgo. De este modo, la monografía no solo tiene como fin estructurar un modelo de prevención de amenazas, sino que a su vez establece bases teóricas y metodológicas para impulsar procesos de mejora continua y respaldar la toma de decisiones informadas (Andersson et al., 2022).

El conocimiento resultado en este estudio da como beneficio directamente a profesionales del área de la seguridad de la información, auditores de sistemas dentro del sector productivo, ofreciéndoles un marco de referencia analítico para diagnosticar y fortalecer sus empresas. Asimismo, sirve como fuente de consulta para la comunidad académica interesada en la gestión

de la ciberseguridad.

Finalmente, el alcance de esta monografía tiene como fin un estudio de revisión y caracterización analítica basado en la literatura científica reciente y en la estructura formal del estándar ISO/IEC 27001:2022, disciplinariamente en la gestión de la seguridad de la información y enfocado en organizaciones en proceso de adopción o actualización de dicho marco normativo.

4. OBJETIVOS

4.1 Objetivo General

Revisar la aplicabilidad de la ISO/IEC 27001:2022 en organizaciones con el propósito de diseñar una guía práctica de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), mediante revisión de literatura y estudio de los controles especificados en la norma.

4.2 Objetivos específicos

- Caracterizar los enfoques y factores críticos de implementación de la ISO/IEC 27001:2022, para sustentar propuestas de mejora, mediante revisión sistemática de literatura y análisis comparativo.
- Evaluar los controles del Anexo A de la ISO/IEC 27001:2022 para priorizar su implementación en organizaciones, mediante el análisis de costo, complejidad e impacto.
- Diseñar una guía práctica de implementación de la ISO/IEC 27001:2022 para orientar la adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) en organizaciones, mediante la integración de resultados del diagnóstico y el análisis teórico.

5. METODOLOGÍA

5.1 Metodología

Enfoque de la Investigación

El presente trabajo entrega una investigación de enfoque cualitativo con alcance descriptivo y analítico. Su fundamento es la revisión sistemática y estructurada de literatura científica, técnica y normativa para analizar la aplicabilidad de la norma ISO/IEC 27001:2022. Desde el punto de vista cualitativo permite clasificar, evaluar y sintetizar evidencia suministrada de bases de datos especializadas con el fin de diagnosticar brechas de seguridad, estudiar casos reales de adopción normativa y diseñar una guía práctica de implementación.

Tipo de Investigación

Se delimita dentro de la investigación aplicada. Su fin central no se limita a la descripción teórica, sino a la generación de un trabajo práctico: una guía de implementación guiada a la identificación de brechas y al diseño de controles de seguridad en entornos organizacionales, con sustento en la evaluación de la factibilidad técnica y operativa.

Método de Investigación y Fases Metodológicas

El desarrollo del estudio integra la metodología de revisión sistemática de literatura (adaptando los lineamientos de la declaración PRISMA) con el ciclo de mejora continua

Fase 1: Planear (Definición y Búsqueda Sistemática)

Delimitación y Criterios de Búsqueda: Se contextualiza las ecuaciones de búsqueda utilizando operadores booleanos en bases de datos académicas e indexadas: *IEEE Xplore*, *Scopus*, *ScienceDirect*, *Redalyc* y *Google Scholar*.

Criterios de Selección:

- Artículos científicos, conferencias y normas técnicas publicadas entre 2020 y 2026.
- Estudios enfocados en la implementación, diagnóstico o análisis de brechas de la norma ISO/IEC 27001 (versiones 2013 y 2022).

Criterios de Exclusión:

- Documentos sin revisión o de fuentes no confiables.
- Artículos con acceso restringido o parcial.
- Investigaciones desactualizadas o no alineadas con la gestión de seguridad de la información.

Cadenas de búsqueda

- ("ISO/IEC 27001" OR "ISO 27001") AND ("gap analysis" OR "compliance gap" OR "security gaps" OR "vulnerabilit*") AND ("information security management system" OR "ISMS")
- ("ISO/IEC 27001" OR "ISO 27001") AND ("critical success factors" OR "implementation factors" OR "barriers" OR "challenges" OR "organizational culture") AND ("information security management" OR "ISMS implementation")
- ("ISO/IEC 27001:2022" OR "Annex A controls") AND ("control prioritization" OR "risk treatment" OR "cost-benefit") AND ("information security controls")
- ("ISO/IEC 27001" OR "ISO 27001:2022") AND ("implementation" OR "adoption" OR "certification") AND ("information security management system" OR "ISMS")

Fase 2: Hacer (Análisis Técnico y Selección)

- **Sistematización y Filtrado:** Aplicación de PRISMA para la selección de artículos (identificación, cribado, elegibilidad e inclusión).
- **Análisis Comparativo del Anexo A (ISO/IEC 27001:2022):** Evaluación de los 93 controles establecido en las 4 nuevas categorías (Organizacionales, Personales, Físicos y Tecnológicos), analizando su complejidad, costo y valor agregado para el diseño de la guía de implementación.

Fase 3: Verificar

- **Criterios de Evaluación:** Claridad, coherencia normativa, aplicabilidad en entornos empresariales y utilidad práctica

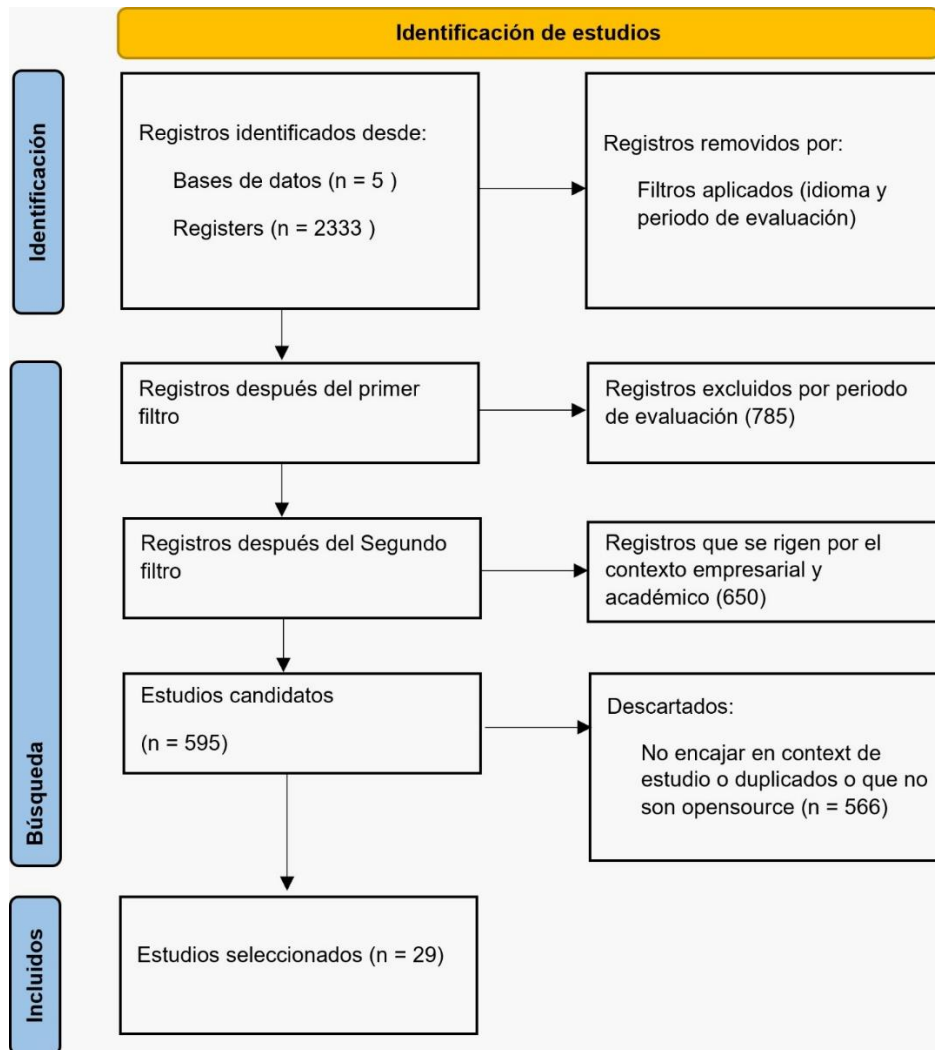
Fase 4: Actuar (Síntesis, Ajustes y Formulación Final)

- **Consolidación de Hallazgos:** Revisión por parte de director.
- **Aporte Final:** Redacción del documento definitivo de la guía de implementación.

Diagrama de Flujo de Selección de Fuentes (Adaptación PRISMA)

El siguiente esquema detalla el proceso de filtrado y trazabilidad bibliográfica para la revisión sistemática:

Figura 1. Diagrama de flujo de la revisión sistemática en PRISMA



Según la aplicación de la metodología se logró la selección de 29 estudios que encajan en el contexto de la investigación

6, ENTREGABLES

Con el propósito de garantizar la trazabilidad y verificación de los resultados de la monografía, en la Tabla 1. Matriz de trazabilidad de objetivos, entregables y medios de verificación se presenta la relación entre cada objetivo específico, las actividades asociadas, los entregables esperados y los medios de verificación correspondientes, permitiendo evidenciar de manera concreta el cumplimiento de cada fase del proceso investigativo.

Tabla 1. Matriz de trazabilidad de objetivos, entregables y medios de verificación

Objetivo específico	Fase	Actividades principales	Entregable	Medio de verificación
OE1. Caracterizar los enfoques y factores críticos de implementación de la ISO/IEC 27001:2022	Planear	Definición de criterios de búsqueda y selección; consulta de literatura en Google Scholar, IEEE Xplore, Scopus y ScienceDirect; selección y revisión de los estudios; extracción de información sobre enfoques, factores de éxito, dificultades y sostenibilidad; agrupación y categorización de factores; cálculo de frecuencia de aparición; valoración del nivel de influencia; comparación de resultados determinación de los factores críticos.	Matriz de hallazgos de la búsqueda sistemática	Matriz validada por el director
		Búsqueda y exclusión de términos en las bases de datos		
		Análisis de los estudios seleccionados		

Objetivo específico	Fase	Actividades principales	Entregable	Medio de verificación
OE2 Evaluar los controles del Anexo A de la ISO/IEC 27001:2022e}	Hacer y verificar	Estudio de la norma ISO 27001 e identificación de los factores críticos ubicados en el Anexo A Definición de influencia de cada factor a partir de los hallazgos de la literatura	Matriz de caracterización y priorización de factores críticos de implementación de ISO/IEC 27001:2022, acompañada del análisis comparativo de	Matriz diligenciada
OE3 Diseñar una guía práctica de implementación de la ISO/IEC 27001:2022	Actuar	Diseño de la estructura de la guía para la implementación de la norma Integración de brechas factores críticos y controles Construcción de la guía	Guía práctica de implementación	Documento aprobado por el director

7. RESULTADOS

7.1 Objetivo 1

Según el primer objetivo específico, orientado a caracterizar los enfoques y factores críticos de implementación de la ISO/IEC 27001:2022, para sustentar propuestas de mejora, mediante la revisión documental y la aplicación de una matriz de diagnóstico, se trabajó en un proceso compuesto por seis etapas. Primero, se realizó una búsqueda bibliográfica relacionada con la norma ISO/IEC 27001:2022, la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI), las brechas de seguridad, las dificultades y las experiencias de aquellas implementaciones. Como resultado de esa búsqueda, se seleccionaron 29 estudios en los cuales se hallaba información relevante para el propósito de la investigación.

Seguidamente, se llevó a cabo una revisión individual de cada uno de los 29 estudios seleccionados, con el fin de identificar los principales problemas reportados por los autores encontrados. En esta etapa se analizó específicamente qué situaciones presentaban deficiencias en los procesos, controles, políticas o prácticas relacionadas con la seguridad de la información. A partir de esta revisión se marcó una relación entre cada documento y el hallazgo identificado, siguiendo la estructura artículo /hallazgo /brecha. Es de suma importancia aclarar que las brechas no fueron descubiertas directamente en las organizaciones por medio de una auditoría, fueron extraídas e identificadas gracias a los hallazgos reportados en los estudios analizados. De esta forma, cuando en un artículo se evidenció una inconsistencia, deficiencia o incumplimiento relacionado con la seguridad de

la información, este hallazgo fue considerado como una brecha para efectos del estudio.

Identificadas las brechas, se procedió a ver su relación con la ISO/IEC 27001:2022, buscando determinar con qué requisito de la norma se encontraba relacionada cada una. Para esta clasificación se tuvieron en cuenta las cláusulas 4 a 10 de la norma, pertenecientes al contexto de la organización, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora, así como está establecido en el Anexo A, específicamente A.5 Controles organizacionales, A.6 Controles de personas, A.7 Controles físicos y A.8 Controles tecnológicos. Esta relación ayudo a contextualizar cada brecha dentro de los componentes de la norma y establecer qué aspectos de un SGSI podrían verse en peligro.

Se determinó la criticidad de cada brecha, con el fin de establecer su nivel de importancia dentro del proceso de implementación y gestión de la seguridad de la información. Para esto se utilizó una escala de tres niveles: alta, media-alta y media. La asignación de la criticidad se otorgó considerando el impacto potencial que cada brecha podría llegar a tener sobre la implementación efectiva de un SGSI, debido a esto, aquellas deficiencias con mayor capacidad de afectar la seguridad de la información, el cumplimiento de los requisitos de la norma o el funcionamiento correcto del sistema fueron consideradas de mayor criticidad.

Por último, toda la información recopilada y analizada fue plasmada en una matriz de diagnóstico, en la cual se anexaron los estudios revisados, los hallazgos identificados, las brechas derivadas de estos hallazgos, su correspondiente relación con las cláusulas 4 a 10 o

Esta matriz ayudó a organizar y visualizar de manera ordenada los resultados obtenidos de la revisión documental y formó el instrumento utilizado para realizar el diagnóstico del estado de la seguridad de la información frente a los lineamientos establecidos por la norma

El nivel crítico se caracterizó a partir del análisis explicado en la Tabla 2

Tabla 1 Matriz documentada de las brechas de seguridad

#	Autor/año	Hallazgo del estudio	Criterio para identificar la brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
1	Wibowo & Aji (2024)	La documentación de los controles no es correcta	Se sustrajo el problema documental dado por los autores y se contrastó con los controles organizacionales relacionados	Brecha: documentación inadecuada de los controles	Google Scholar	A.5 Organizacionales	Alta
2	Jevelin & Faza (2022)	El SGSI de la empresa está en una etapa muy temprana de desarrollo	Se identificó como brecha la diferencia entre el estado de desarrollo descrito y la implementación integral requerida por el SGSI	Brecha: desarrollo muy temprano del SGSI	Google Scholar	Cláusulas 4–10	Alta
3	Ramadhan Sopiah (2022)	Se hallaron problemas en activos y presencia de virus que comprometen la información	Se tomaron los problemas tecnológicos descritos y se relacionaron con los controles destinados a proteger los	Brecha: carencias en protección de activos y amenazas tecnológicas	Google Scholar	A.8 Tecnológicos	Alta

#	Autor/año	Hallazgo del estudio	Criterio para la brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
			activos y la información				
4	Hernández et al. (2024)	No hay evidencia de una gestión de riesgos	Se localizó la ausencia mencionada en el estudio y se contrastó con los requisitos de gestión de riesgos	Brecha: ausencia de una gestión de riesgos	Google Scholar	A.5 / Cláusula 6	Alta
5	Abeykoon (2024)	La cultura organizacional impacta directamente en la implementación del SGSI	Se localizó el factor organizacional identificado por el estudio y se relacionó con los aspectos de personas y cultura necesarios para el SGSI	Lección: la cultura organizacional debe tomarse como referencia en la implementación	Google Scholar	A.6 Personas	Media-Alta
6	Al-Amiri et al. (2024)	Es de suma importancia realizar cambios frente a nuevas tecnologías	Se identificó la necesidad de adaptación señalada por el estudio y se relacionó con los controles tecnológicos	Lección: la implementación final debe contemplar la actualización tecnológica	Google Scholar	A.8 Tecnológicos	Media
7	Niemeläinen et al. (2024)	Distribución incorrecta de recursos	Se tomó la deficiencia en distribución de recursos como evidencia de una asignación inadecuada para las actividades de seguridad	Brecha: asignación inadecuada de recursos	IEEE XPLORE	Cláusula 7 Soporte	Media
8	Domínguez et al. (2023)	El personal no está lo suficientemente capacitado	Se contrastó la insuficiencia de capacitación	Brecha: pobre capacitación del personal	IEEE XPLORE	A.6 Personas	Alta

#	Autor/año	Hallazgo del estudio	Criterio para identificar la brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
			reportada con los controles relacionados con las personas y competencias				
9	Domínguez al. (2023b)	Identificación de factores organizacionales	Se captaron los factores organizacionales identificados por los autores como elementos que pueden afectar la implementación	Lección: los factores organizacionales deben considerarse en el SGSI	IEEE XPLORE	A.5 / A.6	Media-Alta
10	Wijayarathna (2022))	Es de suma importancia la participación de la alta dirección para la toma de decisiones y el rumbo del SGSI	Se identificó la participación directiva como elemento determinante señalado en el estudio y se relacionó con liderazgo	Lección: el liderazgo de la alta dirección es necesario para orientar el SGSI	Google Scholar	Cláusula Liderazgo 5	Alta
11	Tanadi et al. (2021)	Las auditorías externas ayudan en la mejora del SGSI y adopción de controles	Se tomó la relación entre auditoría y mejora señalada por los autores como evidencia de la importancia de evaluar el SGSI	Lección: las auditorías contribuyen a la evaluación y mejora del SGSI	Scopus	Cláusula Evaluación 9	Media
12	Angelini et al. (2022)	Se hallaron brechas en diferentes accesos y necesidad de actualizar políticas	Se relacionaron los problemas de acceso y políticas descritos con los controles de	Brecha: deficiencias en controles de acceso y actualización de políticas	IEEE XPLORE	A.5 / A.8	Alta

#	Autor/año	Hallazgo del estudio	Criterio para identificar brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
			acceso y organizacionales				
13	Culot et (2021)	Se hallaron problemas de implementación y factores contextuales de la empresa	Se captó la dificultad de implementación reportada y se relacionó con los factores organizacionales que condicionan la adopción	Brecha: contratiempos de implementación asociadas al contexto organizacional	Scopus / ScienceDirect	A.5 Organizacionales	Media
14	Ayinoluwa (2024)	Los factores organizacionales tienen bastante peso en el cumplimiento y adopción de estándares	Se sustrajo la influencia organizacional identificada por el estudio como elemento que debe considerarse en la implementación	Lección: la gobernanza y los factores organizacionales influyen en la adopción del estándar	Google Scholar / Scopus	A.5 / Gobernanza	Alta
15	Ryanto & Tundjung sari (2024)	Se detectó una posible fuga de datos y necesidad de fortalecer las políticas	Se relacionó el riesgo de fuga y la necesidad de fortalecer políticas con controles organizacionales y tecnológicos	Brecha: debilidades en protección de la información y políticas de seguridad	Google Scholar / Scopus	A.5 / A.8	Alta
16	López-Vasco et al. (2025)	Para implementar es de suma importancia tener una estructura de lo que se va a realizar	Se captó la necesidad de estructuración identificada por los autores y se relacionó con el establecimiento y planificación del SGSI	Brecha: pobre estructura definida para la implementación	IEEE XPLORE	Cláusulas 4–10	Alta
17	Chávez et al.	Es crítico proteger los datos de los clientes	Se vió la protección de datos como	Lección: la protección de los datos de los	IEEE XPLORE	A.8 Tecnológicos	Alta

#	Autor/año	Hallazgo del estudio	Criterio para la brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
	(2024)		necesidad de seguridad y se relacionó con los controles tecnológicos	clientes debe ser un elemento prioritario de los controles de seguridad			
18	Arumdiya & Rudianto (2025)	Se hallaron fallas en capacitación que pueden generar errores graves	Se captó la deficiencia de capacitación reportada y se comparó con los controles relacionados con personas	Brecha: falencias en capacitación del personal	IEEE XPLORE	A.6 Personas	Alta
19	Kamil et (2023)	Se necesita conocimiento organizacional y no solamente técnico	Se identificó la necesidad de conocimientos organizacionales dada por el estudio como complemento de las capacidades técnicas	Lección: la implementación requiere de conocimiento organizacional además del conocimiento técnico	ScienceDirect / Scopus	A.6 Personas	Media-Alta
20	Confluence IEEE Study (2024)	Se estipula elaborar metodologías de riesgo para la implementación del SGSI	Se captó la recomendación explícita del estudio sobre metodologías de riesgo y se relacionó con la planificación del tratamiento de riesgos	Lección: es crítico establecer una metodología de gestión de riesgos	IEEE XPLORE	Cláusula 6 / A.5	Alta
21	Financial Institution ISO Study (2024)	Se necesita una mejor integración de las normas ISO y mayor seguridad en la implementación	Se identificó como necesidad la integración de los marcos normativos mencionada por el estudio	Lección: la integración de normas y marcos puede fortalecer la implementación	IEEE XPLORE	A.5 Gobernanza	media-Alta
22		Se detectó fallas en políticas, backups y	Se separaron los problemas	Brecha: carencias en	Scopus	A.8 Tecnológicos	Alta

#	Autor/año	Hallazgo del estudio	Criterio para identificar brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
	Suorsa & (2023)	Hacking	identificados y se relacionaron con los controles tecnológicos correspondientes	políticas, copias de seguridad y registro de eventos			
23	Shen (2023)	Se encontraron fallas de configuración que pueden generar fuga de datos	Se captó la relación entre configuración incorrecta y fuga de información identificada en el estudio	Brecha: configuraciones muy deficientes en los controles de acceso/protección	Google Scholar	A.8 Tecnológicos	Alta
24	Ahmed et al. (2025)	Se da una conexión fuerte entre ISO 27001, COBIT y COSO	Se captó la recomendación de integración de marcos como una lección para la gobernanza de seguridad	Lección: integración de marcos de gestión para fortalecer la gobernanza	Scopus	A.5 Gobernanza	media
25	Alharbi et al. (2023)	Se analizó falta de políticas de acceso y privacidad en dispositivos personales	Se contrastaron las carencias de acceso y privacidad reportadas con los controles tecnológicos correspondientes	Brecha: políticas insuficientes para acceso y privacidad en dispositivos personales	Scopus	A.8 Tecnológicos	Alta
26	Fujs et al. (2025)	Existe oposición para seleccionar controles relevantes	Se captó la dificultad identificada por los practicantes como evidencia de un problema en la selección y aplicabilidad de controles	Brecha: carencia para determinar los controles pertinentes	ScienceDirect	A.5 / A.8	media
27	Shekawat et al. (2023)	Se halló malware cifrado capaz de	Se captó la amenaza tecnológica	Brecha: limitaciones de los controles	Google Scholar	A.8 Tecnológicos	Alta

#	Autor/año	Hallazgo del estudio	Criterio para la brecha	Brechas y lecciones	Base de datos	Anexo relacionado	Nivel crítico
		evadir antivirus tradicionales	identificada y se relacionó con la necesidad de controles de protección tecnológica	tradicionales frente a amenazas avanzadas			
28	Assolin et al. (2025)	Se encontraron fallas de acceso no autorizado y ausencia de respuestas automáticas	Se tomaron ambos hallazgos y se contrastaron con controles de acceso y respuesta ante incidentes	Brecha: deficiencias en control de acceso y respuesta ante incidentes	Google Scholar	A.8 Tecnológicos	Alta
29	Domínguez-Domínguez et al. (2023)	Se detectó que las capacitaciones son demasiado débiles	Se contrastó la debilidad de las capacitaciones reportada con los controles relacionados con competencias y personas	Brecha: capacitación insuficiente para el personal	Google Scholar	A.6 / Cláusula 5	A.6 / Cláusula 5

Criterio de extracción de brechas y lecciones:

Para cada estudio se identificó los hallazgos, problemas, necesidades o recomendaciones expresados por los autores. Seguidamente, estos elementos fueron comparados con los requisitos de las cláusulas 4 a 10 y los controles del Anexo A de la ISO/IEC 27001:2022.

Cuando el hallazgo evidenció una ausencia, deficiencia o incumplimiento respecto del requisito o control relacionado, se clasificó como brecha.

Cuando el estudio presentó una recomendación, factor crítico o aspecto que debía considerarse para una implementación adecuada, se clasificó como lección. Finalmente, se registró el requisito o control ISO relacionado como evidencia de la correspondencia realizada.

Figura 2 Distribución de brechas encontradas en la literatura



Los resultados muestran un alto índice de brechas en controles tecnológicos (34%) y organizacionales (31%), lo que evidencia que los desafíos más recurrentes en la literatura se relacionan con controles técnicos, gobernanza y políticas de seguridad.

7.2 Resultado objetivo específico numero dos

El segundo objetivo específico estuvo orientado a evaluar los controles del Anexo A de la ISO/IEC 27001:2022 para priorizar su implementación en organizaciones, mediante el análisis de costo, complejidad e impacto, con el propósito de sustentar propuestas de mejora mediante una revisión sistemática de literatura y un análisis comparativo con la norma. Para dar respuesta a este objetivo, se estableció un proceso de revisión y análisis de estudios académicos y documentos relacionados con la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI), con el fin de identificar elementos que tienen incidencia en el éxito, las dificultades y la sostenibilidad de la implementación de la norma ISO/IEC 27001:2022, En este sentido, diferentes investigaciones han

identificado como factores relevantes las políticas de seguridad, el apoyo de la alta dirección, la evaluación de riesgos, la conciencia de seguridad y la cultura de seguridad de la información (Chen & Hai, 2024).

7.2.1 Procedimiento para la identificación de los factores críticos

Se realizó la lectura y extracción de la información relevante de los documentos seleccionados, teniendo en cuenta ítems relacionados con los factores que favorecen la implementación, los factores que dificultan el proceso, los elementos asociados con el éxito y la sostenibilidad del SGSI, las dificultades de carácter organizacional, humano, técnico y económico, la gestión de riesgos, así como las políticas, controles y procesos de mejora continua. A partir de esta revisión fue posible identificar y agrupar los diferentes factores mencionados en los estudios, buscando establecer cuáles se presentan de manera recurrente y cuáles tienen una influencia significativa sobre la implementación y funcionamiento de un SGSI basado en ISO/IEC 27001:2022. Esta forma de análisis es coherente con investigaciones que han utilizado la identificación y agrupación de factores para determinar aquellos elementos que pueden contribuir al desempeño de la gestión de seguridad de la información (Chen & Hai, 2024; Zammani & Razali, 2016).

7.2.2 Criterios utilizados para determinar los factores críticos

Identificados y agrupados los factores hallados en la literatura, se establecieron dos criterios de análisis para determinar cuáles podrían considerarse factores críticos: la tasa de aparición y el nivel

de influencia. El primer criterio corresponde a la tasa de aparición, entendida como el número de estudios en los cuales se halló cada factor. Para ver su representación dentro del conjunto de documentos analizados, se calculó el porcentaje de frecuencia relativa mediante la siguiente expresión (Rietveld et al., 2022):

$$\text{Frecuencia (\%)} = (\text{Número de estudios donde aparece el factor} / \text{Número total de estudios analizados}) \times 100$$

Este cálculo ayudó a establecer qué factores tienen una mayor recurrencia dentro de la literatura revisada. Sin embargo, la frecuencia por sí sola no es suficiente para determinar la criticidad de un factor, debido a que un elemento puede aparecer en varios estudios sin necesariamente dar una influencia significativa sobre la implementación del SGSI.

Como segundo criterio se consideró el nivel de influencia, mediante un análisis cualitativo de la importancia que los autores de los estudios atribuyen a cada factor y de la manera en que este puede dañar el éxito, la implementación del SGSI. Por esto, se estableció una escala de valoración que permitió clasificar los factores gracias al grado de influencia identificado en la literatura. El conjunto de la frecuencia de aparición y el nivel de influencia permitió realizar un análisis comparativo de los factores identificados, diferenciando aquellos que presentan una presencia frecuente y una influencia significativa de aquellos cuya aparición o impacto es menor. De esta forma, los factores seleccionados como críticos se basan en la evidencia obtenida de los estudios analizados y no únicamente en una apreciación de los investigadores, dando una base para formular propuestas de mejora relacionadas

con la implementación de la ISO/IEC 27001:2022.

Tabla 2 Matriz de impacto crítico

Nivel	Crítico
Muy alta	El factor afecta directamente el éxito, sostenibilidad o capacidad de implementación del SGSI.
Alta	El factor tiene una incidencia significativa sobre la implementación o funcionamiento del SGSI.
Media-alta	El factor tiene una incidencia importante, aunque depende de otros elementos organizacionales o técnicos.
Media	El factor contribuye a la implementación, pero su influencia es secundaria.
Bajo	El factor tiene una incidencia limitada o indirecta.

7.2.3 Elaboración de la matriz final

Tabla 3 Matriz de indicador de factores críticos

Factor crítico	Tipo	Frecuencia en literatura	Nivel de influencia	Definición
Compromiso de la alta dirección	Organizacional	Alta	Muy alta	Determina asignación de recursos, liderazgo y sostenibilidad del SGSI
Cultura de seguridad	Organizacional	Alta	Alta	Favorece cumplimiento y adopción de controles
Capacitación del personal	Humano	Alta	Alta	

Factor crítico	Tipo	Frecuencia en literatura	Nivel de influencia	Definición
				Reduce errores humanos y fortalece respuesta ante incidentes
Gestión de riesgos	Estratégico	Alta	Muy Alta	Base para selección de controles y tratamiento del riesgo
Recursos	Organizacional	Media	Alta	Permite soporte técnico y operativo del SGSI
Políticas	Normativo	Alta	Muy Alta	Facilita alineación con requisitos de la norma

7.2.4 Resultado del Objetivo Específico 2: Evaluación y Priorización de Controles (Anexo A)

Procedimiento y Selección de Controles

Se examinaron los controles del Anexo A de la norma ISO/IEC 27001:2022 con el fin de definir su orden de implementación. La selección no se otorgó de manera aislada, se vincularon las brechas y factores críticos hallados en los Objetivos 1 y 2 con las cuatro categorías del Anexo A (Organizacionales, Personales, Físicos y Tecnológicos). A partir de esto, se filtraron los controles con mayor utilidad práctica, evaluándose mediante una escala ordinal para calcular un puntaje de priorización final.

Criterios de Valoración

La priorización se fundamentó en tres factores clave:

- **Costo:** Mide la inversión económica requerida (Bajo: recursos existentes; Medio: inversión moderada; Alto: presupuesto elevado o terceros).
- **Complejidad:** Evalúa la dificultad técnica y operativa de adopción (Baja: ajustes sencillos; Media: cambios en procesos; Alta: reestructuración técnica o experta).

Tabla 4 Matriz costo complejidad

Nivel	Valor para priorización
Bajo	3
Medio	2
Alto	1

- **Impacto:** Determina el grado del riesgo y protección de la información (Bajo: contribución puntual; Medio: mejora sustancial; Alto: reducción crítica de vulnerabilidades).

Tabla 5 Matriz de Impacto

Nivel	Valor para priorización
Bajo	1
Medio	2
Alto	3

Método de Priorización de Controles

El puntaje final de prioridad se obtuvo mediante la suma de los tres criterios evaluados: **Puntaje de prioridad = Impacto + Costo + Complejidad**. La utilización de múltiples criterios para evaluar y priorizar controles de seguridad permite considerar simultáneamente aspectos relacionados con el impacto de las amenazas, los recursos requeridos y las condiciones de implementación, facilitando

una selección estructurada de los controles que deben ser atendidos prioritariamente (Almorsy et al., 2018).

- Impacto: 1 a 3 puntos.
- Costo: 1 a 3 puntos, utilizando valoración inversa.
- Complejidad: 1 a 3 puntos, utilizando valoración inversa.

Tabla 6 Matriz de Prioridad

Puntaje	Prioridad
8-9	Alta
6-7	Media
3-5	Bajo

Para asegurar una escala coherente, cada variable se valoró entre 1 y 3 puntos, aplicando una valoración inversa en Costo y Complejidad (donde 3 representa menor costo/complejidad y 1 representa mayor costo/complejidad). De este modo, la escala total resultante varía entre 3 (mínimo) y 9 (máximo) puntos.

Para obtener el puntaje de priorización de cada control se sumaron los valores asignados a costo, nivel de dificultad e impacto, de acuerdo con las escalas establecidas. En el caso de Políticas de seguridad, se asignaron 3 puntos por costo bajo, 3 puntos por dificultad baja y 3 puntos por impacto alto, obteniendo un total de 9 puntos ($3 + 3 + 3$), correspondiente a una prioridad alta.

Para Propiedad intelectual, se asignaron 3 puntos por costo bajo, 3 puntos por dificultad baja y 3 puntos por impacto muy alto, para un total de 9 puntos ($3 + 3 + 3$), clasificado como prioridad alta.

En Capacitación, el costo medio obtuvo 2 puntos, la dificultad media 2 puntos y el impacto alto 3 puntos, alcanzando 7 puntos ($2 + 2 + 3$), correspondiente a una prioridad media.

Para Control de accesos, el costo alto obtuvo 1 punto, la dificultad alta 1 punto y el impacto muy alto 3

puntos, obteniendo 5 puntos (1 + 1 + 3), clasificado como prioridad baja.

En Copias de seguridad, se asignaron 2 puntos por costo medio, 2 puntos por dificultad media y 3 puntos por impacto alto, obteniendo 7 puntos (2 + 2 + 3), correspondiente a una prioridad media.

Para Protección contra malware, se asignaron 2 puntos por costo medio, 2 puntos por dificultad media y 3 puntos por impacto alto, obteniendo 7 puntos (2 + 2 + 3), correspondiente a una prioridad media.

Finalmente, en Acceso físico, se asignaron 3 puntos por costo bajo, 3 puntos por dificultad baja y 2 puntos por impacto medio, obteniendo 8 puntos (3 + 3 + 2), correspondiente a una prioridad alta.

La aplicación de los criterios permitió construir una matriz para los controles seleccionados del Anexo A de la ISO/IEC 27001:2022.

Tabla 7 Matriz de evaluación y priorización de controles

Control	Subgrupo	Costo	Nivel de dificultad	Impacto
Políticas de seguridad	Organizacional	Bajo	Bajo	Alto
Propiedad intelectual	Organizacional	Bajo	Bajo	Muy alto
Capacitación	Personas	Medio	Medio	Alto
Control de accesos	Tecnológico	Alto	Alto	Muy alto
Copias de seguridad	Tecnológico	Medio	Medio	Alto
Protección contra malware	Tecnológico	Medio	Medio	Alto

Control	Subgrupo	Costo	Nivel de dificultad	Impacto
Acceso físico	Físico	Bajo	Bajo	Medio

8. Guía de implementación

8.1 Introducción a la guía de implementación

La presente guía tiene como fin dar a las organizaciones tecnológicas una ruta estructurada para implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con base en los requisitos de la norma ISO/IEC 27001:2022. La guía está diseñada para que pueda ser utilizada por organizaciones de diferentes sectores, adaptando sus actividades, documentos, responsables y controles con respecto a su contexto, procesos, activos, riesgos y necesidades particulares (International Organization for Standardization [ISO], 2022).

La guía se construye a partir de los resultados dados en el análisis documental y de los factores críticos identificados durante la investigación. Por esta eso, no se limita a dar los requisitos de la norma, sino que establece qué debe hacer la organización, qué documento o registro debe generar, quién debería ser responsable, qué evidencia debe conservar y qué resultado se espera obtener en cada etapa.

La implementación se da de acuerdo con las cláusulas 4 a 10 de ISO/IEC 27001:2022 y se lleva a cabo con la selección e implementación de los controles aplicables del Anexo A. La norma tiene 93 controles distribuidos en cuatro grupos: controles organizacionales, de personas, físicos y tecnológicos. Estos controles deberían ser analizados por la organización a partir de las necesidades y resultados de tratamiento de riesgos, y su selección debe quedar justificada en la Declaración de Aplicabilidad.

8.2 Requisitos para la implementación

La empresa debe establecer las condiciones necesarias para empezar la implementación de la guía.

En esta etapa se debe definir quién dirigirá el proceso, qué recursos estarán disponibles y cuál será el alcance del SGSI, teniendo en cuenta el contexto de la organización, las necesidades de las partes

interesadas y los requisitos aplicables (International Organization for Standardization [ISO], 2022).

La dirección debe designar un responsable y proporcionar los recursos necesarios para desarrollar las actividades. Además, debe establecerse un cronograma de implementación y determinar las áreas, procesos, sedes, sistemas y servicios que serán considerados inicialmente, de acuerdo con el contexto de la organización y el alcance definido para el SGSI (International Organization for Standardization [ISO], 2022). Se tiene que designar:

Actividades

- Designar un responsable del SGSI.
- Definir el equipo de implementación.
- Obtener el compromiso formal de la alta dirección.
- Definir recursos humanos, tecnológicos y económicos.
- Establecer un cronograma de implementación.
- Determinar inicialmente los procesos y áreas que serán analizados.
- Realizar un diagnóstico inicial del estado de seguridad de la organización.

Documentos y registros

- Acta de inicio del proyecto SGSI.
- Designación del responsable del SGSI.
- Matriz de roles y responsabilidades.
- Cronograma de implementación.
- Diagnóstico inicial.
- Registro de recursos asignados.

8.3 Contexto de la organización

Se realiza un diagnóstico inicial de la empresa tecnológica a evaluarse con el objetivo de identificar el estado actual de la seguridad de la información y detectar brechas existentes., para darse una idea se debe verificar si se cuenta con alguna documentación de base, por ejemplo, si se tiene política de seguridad, se revisará a profundidad estos documentos y se decidirá si la información está muy desactualizada o sirve para empezar la implementación. Los auditores ayudarán en el proceso de implementación, si no se cuentan con uno se puede hacer una auditoría interna dentro de la empresa, pero siempre es recomendable que lo haga alguien que no tenga interés de por medio con la empresa.

Esta etapa corresponde principalmente a la cláusula 4 de ISO/IEC 27001:2022. Su finalidad es comprender la organización, identificar los factores que pueden afectar al SGSI, determinar las partes interesadas y establecer claramente los límites del sistema. La cláusula 4 comprende el contexto, las partes interesadas, el alcance y el establecimiento del SGSI.

8.3.1 Identificación del Contexto Organizacional

La empresa debe determinar los factores internos y externos que resulten pertinentes para su fin y que afecten su capacidad para alcanzar los resultados en el SGSI. Este diagnóstico inicial permite relacionar la estrategia de ciberseguridad con la realidad operativa, estratégica y presupuestal de la empresa, facilitando que las acciones de seguridad respondan a los objetivos y necesidades reales de la organización (Silva et al., 2020).

Para realizar un análisis integral del entorno, se evalúan dos dimensiones clave:

- **Factores Internos:** tiene en cuenta la estructura organizacional, dimensión de la empresa y la

complejidad de sus procesos críticos de negocio. A su vez, analiza la infraestructura tecnológica desplegada, el nivel de madurez en sus operaciones y la disponibilidad de recursos económicos destinados a la gestión de riesgos.

- **Factores Externos:** Engloba las exigencias del entorno tecnológico y de mercado, incluyendo la aparición de nuevas amenazas a la seguridad, la evolución digital y la alta dependencia de terceros de servicios. De esta manera, contempla el cumplimiento de requisitos legales y contractuales aplicables, las expectativas de privacidad de los clientes y las condiciones del contexto socioeconómico.

Tabla 8 Matriz de contexto de la organización

Factor	Tipo	Descripción	Impacto
Dependencia tecnológica	Interno o	La operación depende de sistemas informáticos	Alto
Proveedores externos	Externo o	Se utilizan servicios tecnológicos de terceros	Medio
Legislación aplicable	Externo o	Existen obligaciones legales sobre información	Alto

Tómese la anterior matriz como un ejemplo práctico

8.3.1 Identificación de Partes Interesadas

La organización debe determinar las partes interesadas para el SGSI, teniendo en cuenta sus necesidades y expectativas en materia de seguridad de la información. Además, debe contemplar las exigencias operativas, contractuales, legales y reglamentarias del entorno institucional, de manera que los objetivos y medidas de seguridad respondan a las necesidades de las partes interesadas y al contexto en el que opera la organización (Kamil et al., 2023).

Las partes interesadas se organizan en cuatro grupos estratégicos:

- **Partes Internas:** Comprende al personal de la organización en todos sus

niveles operativos, accionistas y órganos de gobierno corporativo, cuyas expectativas se centran en la protección de la reputación, la continuidad del negocio y el cumplimiento de las responsabilidades laborales en entornos seguros.

- **Clientes y Socios Comerciales:** Abarca a los usuarios directos de los servicios y aliados estratégicos que exigen garantías de confidencialidad, privacidad de datos y disponibilidad en el procesamiento de sus transacciones o activos de información.
- **Proveedores y Terceros Tecnológicos:** Incluye a los proveedores de infraestructura, servicios en la nube, soporte técnico y consultorías externas, con quienes se deben definir acuerdos de nivel de servicio (SLA) y requisitos claros de seguridad en la cadena de suministro.
- **Entidades Gubernamentales y Regulatorias:** Engloba a los organismos de control, autoridades fiscales y entes reguladores del sector, ante los cuales la organización debe demostrar el cumplimiento estricto del marco legal aplicable y de las normativas de protección de datos personales.

Tabla 9 Matriz de partes interesadas según la norma

Parte interesada	Necesidad	Requisito	Impacto sobre la seguridad
Clientes	Protección de información	Confidencialidad	Alto
Empleados	Acceso a sistemas	Disponibilidad	Medio
Entidad regulatoria	Cumplimiento legal	Protección de datos	Alto

8.3.3 Definición del Alcance del SGSI

Según lo establecido en la Cláusula 4.3 de la norma ISO/IEC 27001:2022, la organización debe delimitar de forma clara los límites físicos, operativos y tecnológicos donde se aplicará el Sistema de Gestión de Seguridad de la Información. La definición del alcance evita brechas en la protección de los datos y facilita que los esfuerzos de ciberseguridad se concentren en las áreas donde residen los activos más críticos.

Para estructurar la cobertura del SGSI, la organización debe precisar los siguientes elementos:

- **Delimitación Operativa y Humana:** Especifica los procesos clave del negocio, los servicios de préstamo y los colaboradores que interactúan con la información bajo el perímetro del sistema.
- **Perímetro Tecnológico e Información:** Determina los sistemas de información, las tecnologías de soporte y las bases de datos o documentación de contenido sensible que quedan cubiertas bajo los controles de seguridad.
- **Límites Físicos y de Terceros:** Define las sedes, ubicaciones físicas en la nube donde operan los sistemas, además de las interfaces y puntos de contacto con proveedores o socios externos que acceden a la red o procesan datos de la entidad.

8.4 Principales controles de seguridad

Para hablar de controles, antes debemos mencionar a los activos, ya que estos corresponden a los recursos físicos o virtuales que tienen valor para la organización, tales como computadores, servidores, bases de datos, aplicaciones o código fuente. Los controles son medidas destinadas a proteger estos activos frente a amenazas y riesgos que puedan afectar la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, en el caso de un servidor físico, uno de los controles que puede utilizarse es el control de acceso, mediante el cual se restringe el ingreso únicamente al personal autorizado (Suorsa & Helo, 2024).

Teniendo eso en consideración, se enumeraron de forma concisa los controles más importantes que se deben tener en cuenta a la hora de realizar la guía de implementación. La cantidad y selección de controles depende de los activos con los que cuenta la empresa, así como de los riesgos identificados, las necesidades de protección y las características particulares de la organización (Fujs et al., 2025).

Política de seguridad de la información

Objetivo

La política de seguridad de la información constituye el documento rector que formaliza el compromiso organizacional con la protección de los activos de información. Se trata de un instrumento normativo de alto nivel que establece los principios, objetivos y responsabilidades que orientan el comportamiento de todos los actores dentro de la organización en materia de seguridad. Su función principal no es prescribir procedimientos técnicos detallados, sino proporcionar un marco de referencia coherente que permita alinear las prácticas operativas con los requisitos legales, regulatorios y estratégicos de la entidad (Alqahtani et al., 2023). Para ser efectiva, esta política debe ser comunicada de forma activa a todo el personal, revisada periódicamente y aprobada formalmente por la alta dirección, garantizando así su legitimidad y vigencia en el tiempo.

Procedimientos básicos

1. Redactar y debatir la alta gerencia cada punto de la política si no omitir.
2. Revisar y aprobar debidamente por alta gerencia.
3. Socializar el contenido con todo el personal.

4. Revisar una vez al año como mínimo.
5. Actualizar cuando cambien procesos de la política.

Evidencia

- Documento de política
- Lista de aprobación
- Registro de socialización

Control de acceso

Objetivo

Se define como el conjunto de mecanismos técnicos y administrativos mediante los cuales una organización regula quién puede interactuar con sus recursos de información, en qué condiciones y con qué nivel de privilegios. Su fundamento radica en el principio de mínimo privilegio, que establece que cada usuario o proceso debe contar exclusivamente con los permisos estrictamente necesarios para el desempeño de sus funciones, evitando así la acumulación de derechos que puedan ser explotados de manera indebida (Horne et al., 2022). El modelo más extendido en entornos organizacionales es el Control de Acceso Basado en Roles (RBAC, por sus siglas en inglés), el cual asigna permisos en función del perfil funcional del usuario, simplificando la gestión de identidades y reduciendo la superficie de ataque ante amenazas tanto externas como internas.

Procedimiento básico

1. crear usuarios según solicitud aprobada.
2. asignar permisos por rol.
3. Se deben exigir contraseñas seguras para el acceso al sistema.

4. Implementar MFA cuando aplique.
5. Erradicar accesos a personal que salga de la empresa.
6. Revisar permisos cada mes.

Evidencia

- Matriz de usuarios
- Roles y permisos
- Solicitudes de acceso
- Registro de bajas de usuarios

Copias de seguridad

Objetivo

Constituyen un mecanismo fundamental para garantizar la disponibilidad y la recuperabilidad de la información ante eventos disruptivos como fallos de hardware, ataques de ransomware, errores humanos o desastres naturales. Desde la perspectiva de la gestión de la continuidad del negocio, una estrategia de respaldo eficaz debe contemplar la periodicidad de las copias, los medios de almacenamiento utilizados, la segregación física o lógica de las copias respecto al sistema original y la verificación periódica de los procesos de restauración (Warkentin & Orgeron, 2020). La ausencia de una política de backups estructurada representa una de las vulnerabilidades más críticas que enfrentan las organizaciones, ya que puede derivar en pérdidas irreversibles de información ante incidentes que de otro modo serían recuperables.

Procedimiento básico

1. Se debe identificar información crítica.
2. Definir frecuencia en la cual se harán las copias.
3. los backup se realizan de forma automática.
4. Guardar copia en nube o servidor alternativo.
5. restauración mensual.
6. Registrar resultados.

Evidencia

- Política de backup
- Logs de respaldo
- Evidencia de restauración

Protección contra malware

Objetivo

El malware es una categoría amplia de software diseñado con propósitos maliciosos que abarca virus, troyanos, ransomware, spyware y otras variantes capaces de comprometer la confidencialidad, integridad y disponibilidad de los sistemas de información. La protección frente a este tipo de amenazas implica una estrategia de defensa en profundidad que combina herramientas tecnológicas como antivirus, sistemas de detección de intrusiones y filtros de contenido— con medidas organizacionales orientadas a la concienciación del personal, dado que muchos vectores de entrada

del malware explotan el comportamiento humano a través de técnicas de ingeniería social y phishing (Syafitri et al., 2022). La actualización continua de las firmas y los mecanismos de detección, junto con la segmentación de redes, son considerados controles esenciales para mitigar la propagación de este tipo de amenazas dentro del entorno corporativo.

Procedimiento básico

1. Se debe instalar antivirus corporativo.
2. Configurar escaneo automático.
3. Mantener las firmas actualizadas.
4. Bloquear software sin autorización.
5. Reportar alertas sospechosas.

Evidencia

- Antivirus
- Reporte de actualizaciones
- Historial de amenazas detectadas

Gestión de logs

Objetivo

La gestión de registros de eventos, o logs, consiste en la recolección, almacenamiento, correlación y análisis sistemático de los datos generados por los sistemas, aplicaciones y dispositivos de red de una organización. Esta función es central para la detección temprana de incidentes de seguridad, ya que permite identificar patrones de comportamiento anómalo que podrían indicar actividades maliciosas en curso. Los sistemas de Gestión de Información y Eventos de Seguridad (SIEM)

automatizan este proceso al centralizar los logs provenientes de múltiples fuentes y aplicar reglas de correlación que transforman grandes volúmenes de datos en alertas accionables para los equipos de seguridad (González-Granadillo et al., 2021). Adicionalmente, la conservación adecuada de estos registros es un requisito de cumplimiento en numerosos marcos regulatorios y normativos, incluyendo la propia ISO/IEC 27001:2022.

Procedimiento básico

1. Registrar inicios de sesión.
2. Registrar intentos fallidos.
3. Registrar cambios de configuración.
4. Registrar accesos administrativos.
5. Proteger logs contra modificación.
6. Revisarlos semanalmente.

Evidencia

- Logs del sistema
- Reportes SIEM
- Bitácora de revisión

Acceso físico

Objetivo

La seguridad de acceso físico hace referencia al conjunto de controles y barreras tangibles que una

organización implementa para restringir el ingreso a sus instalaciones, centros de datos, salas de servidores y cualquier área que albergue activos de información críticos. A diferencia de los controles lógicos —que operan en el ámbito digital—, los controles físicos actúan sobre el entorno material y comprenden elementos como sistemas de vigilancia por video, tarjetas de acceso, biometría, registros de visitantes y vigilancia presencial. La norma ISO/IEC 27001:2022 contempla explícitamente estos controles dentro de su Anexo A, reconociendo que una brecha en la seguridad física puede anular por completo la eficacia de cualquier medida tecnológica implementada, ya que el acceso no autorizado a las instalaciones puede derivar en robo, sabotaje o exfiltración directa de información (Annarelli et al., 2021).

Procedimiento básico

1. Ingreso a áreas críticas con credencial.
2. Usar cerraduras, tarjetas o biometría.
3. Registro de visitantes.
4. Monitorear con cámaras las 24 horas.
5. Registro de ingreso y salida de equipos.
6. Mantener áreas seguras cerradas.

Evidencia

- Registro de visitantes
- Bitácora de ingreso
- Grabaciones CCTV

Capacitación del personal

Objetivo

La formación en seguridad de la información es reconocida en la literatura especializada como uno de los controles de mayor impacto dentro de cualquier SGSI, dada la centralidad del factor humano en la mayoría de los incidentes documentados. Un programa de capacitación efectivo no puede limitarse a sesiones informativas genéricas; por el contrario, debe diseñarse de manera diferenciada según los roles y responsabilidades de cada grupo de usuarios, abordando escenarios prácticos relevantes para su contexto laboral. Zhang et al. (2021) proponen un marco de análisis costo-beneficio para los programas de concienciación en ciberseguridad, concluyendo que las organizaciones que invierten en formación continua y personalizada reportan una reducción estadísticamente significativa en la frecuencia y el impacto de los incidentes relacionados con el comportamiento humano. La capacitación, por tanto, no debe concebirse como un evento puntual sino como un proceso sistemático y sostenido de desarrollo de competencias en seguridad.

Procedimiento básico

1. Programar capacitaciones mensuales.
2. El phishing, contraseñas y buenas prácticas debe tenerse en claro .
3. hacer test para evaluar conocimientos.
4. Registrar asistencia.
5. Reforzar al personal con bajo desempeño.
6. Actualizar contenidos.

Evidencia

- Cronograma
- Lista de asistencia
- Resultados de evaluaciones

Propiedad intelectual

Objetivo

La propiedad intelectual del software engloba los derechos legales que protegen las creaciones digitales de sus autores o titulares frente a su reproducción, distribución o uso no autorizado. En el contexto de la seguridad de la información, la gestión de estos derechos es un control organizacional de doble dimensión: por un lado, implica garantizar que el software utilizado dentro de la organización cuente con las licencias correspondientes, evitando así exposiciones legales y el uso de versiones no soportadas que pueden contener vulnerabilidades conocidas; por otro lado, supone proteger el software desarrollado internamente como un activo estratégico frente a accesos no autorizados y posible

exfiltración (Alassaf & Alkhalifah, 2021). El uso de software sin licencia incrementa significativamente la superficie de riesgo, ya que estas versiones no reciben actualizaciones de seguridad ni parches correctivos por parte de sus fabricantes.

Procedimiento básico

1. Identificar activos protegidos.

2. Clasificar información confidencial.
3. Firmar acuerdos NDA.
4. Restringir copias y descargas.
5. Registrar licencias y derechos.
6. Monitorear el uso indebido.

Evidencia

- Registro de licencias
- Inventario documental
- Bitácora de incidentes

8.4.1 Roles y responsabilidades

Se establece quién es el encargado en la toma de decisiones, quién administra el SGSI, quién es responsable de los riesgos y quién ejecuta los controles (Biswas, 2022).

Tabla 10 Matriz roles y responsabilidades

Actividad	Dirección	Responsable SGSI	T	Empleado
Aprobar política	A	R	C	I
Gestionar riesgos	A	R	C	C
Implementar controles	I	A	R	C
Capacitación	A	R	C	R

A — Autoridad: Es la persona o rol que rinde cuentas por el resultado, tiene la última palabra y aprueba la actividad. Solo debe haber una "A" por cada tarea.

R — Responsable: Es quien ejecuta o realiza operativamente la tarea

C — Consultado: Es a quien se le pide criterio técnico, datos o asesoría antes o durante la ejecución de la actividad.

I — Informado: Es a quien únicamente se le notifica o mantiene al tanto sobre los avances o resultados finales.

8.5 Planificación del SGSI (Cláusula 6)

Esta fase constituye una fase estratégica dentro del proceso de implementación, pues permite prever escenarios de amenaza, adelantar sus consecuencias sobre el negocio y establecer las salvaguardas necesarias para mitigar la vulnerabilidad institucional.

En alineación con la Cláusula 6 de la norma ISO/IEC 27001:2022, este componente contempla tres ejes fundamentales:

- **Gestión de riesgos y oportunidades:** Mecanismos para abordar de forma proactiva las

incertidumbres que puedan afectar el desempeño del SGSI.

- **Evaluación y tratamiento del riesgo:** Criterios metodológicos para identificar, analizar, valorar y responder ante las vulnerabilidades de los activos de información.
- **Objetivos de seguridad y planificación:** Definición de metas medibles, alineadas con las políticas de la organización, junto con las acciones, recursos y cronogramas requeridos para su logro.

8.5.1 Identificación de Activos de Información

Antes de proceder con la evaluación de riesgos dentro del SGSI, es fundamental confeccionar un inventario exhaustivo de los activos de información de la organización. Este proceso no solo es la infraestructura tangible, sino que abarca la totalidad de los recursos, datos y servicios que poseen valor estratégico u operativo.

Para estructurar de forma correcta este inventario, los activos deben clasificarse en cuatro dimensiones principales:

- **Activos de Información y Datos:** entiende el conocimiento crítico de la organización, incluyendo la información de clientes, registros de empleados, estados financieros, bases de datos y copias de seguridad (*backups*), además de credenciales de acceso y documentación formal.
- **Infraestructura y Equipamiento Físico:** Engloba el soporte material donde se almacena o la información, como servidores, computadores de escritorio, portátiles, equipos de red y dispositivos físicos ubicados en las instalaciones.
- **Sistemas y Aplicaciones:** es el conjunto de software corporativo, aplicaciones internas,

- Servicios e Redes:** Abarca la infraestructura de telecomunicaciones, enlaces de red y servicios informáticos necesarios para mantener la disponibilidad y conectividad del entorno tecnológico.

8.5.2 Evaluación de riesgos

La organización debe establecer una metodología de evaluación de riesgos que ayude a obtener resultados consistentes. ISO/IEC 27001 no obliga a utilizar solo una metodología específica; la organización puede definir la que resulte mejor siempre que cumpla los requisitos de evaluación y tratamiento establecidos (Advisera, 2024).

Una metodología sencilla para la guía puede utilizar:

Tabla 11 Matriz de impacto

Impacto	Valor
baja	1
medio	2
alto	3

Tabla 12 Matriz de Resultado

Resultado	Nivel
1-2	bajo
3-4	medio
6-9	alto

Tabla 13 Matriz de probabilidad

Probabilidad	Valor
baja	1
medio	2
alto	3

De acuerdo con cada tabla se hallará el resultado final

8.5.3 Tratamiento de Riesgos

la organización debe determinar la estrategia de respuesta que se adecue mejor para cada uno, seleccionando las medidas que permitan llevar la exposición a un nivel aceptable según su apetito de riesgo.

Para abordar estas incertidumbres, se aplican cuatro opciones principales de tratamiento:

- **Evitar el riesgo:** Consiste en tomar la decisión de suspender, modificar o no iniciar la actividad o proceso que genera la amenaza, eliminando por completo la fuente que expone a la organización.
- **Mitigar el riesgo:** activa la selección e implementación de controles técnicos, organizacionales o físicos (alineados con el Anexo A de la norma) para disminuir la probabilidad de ocurrencia o minimizar el impacto de un posible incidente.
- **Compartir o transferir el riesgo:** Se especializa en trasladar de manera parcial o total la responsabilidad económica o de gestión a un tercero mediante contratos de servicios.
- **Aceptar el riesgo:** Corresponde a la decisión formal de asumir el riesgo remanente sin aplicar medidas adicionales, siempre que su impacto se encuentre dentro de los límites preestablecidos y aprobados por la alta dirección.

Para finalizar, este proceso se consolida mediante la elaboración de un Plan de Tratamiento de Riesgos, un documento que consolida los controles seleccionados asigna responsables, define las fechas límite de ejecución y especifica los recursos técnicos y financieros para garantizar la efectividad de las salvaguardas propuestas.

8.5.4 Declaración de Aplicabilidad (SoA)

La organización debe analizar verificar los controles del Anexo A y llegar a la conclusión de cuáles son necesarios para tratar sus riesgos. Además, se debe justificar las inclusiones y exclusiones y establecer el estado de implementación.

Tabla 14 matriz declaración de aplicabilidad

Control	Aplicable	Justificación	Estado	Evidencia
a.5.x	Si	Riego identificado	implementado	Política x
a.6.x				
a.7.x				
a.8.x				

8.6 Apoyo (Cláusula 7)

Esta fase contempla la previsión de las capacidades organizacionales para la sostenibilidad del SGSI. En alineación con la Cláusula 7 de la norma ISO/IEC 27001:2022, afirma la disponibilidad de la infraestructura técnica y económica requerida, además de la asignación de personal competente y concientizado sobre sus responsabilidades en la protección de la información.

También, abarca la gestión del conocimiento técnico de la organización y el control riguroso de la información documentada (políticas, procedimientos y registros), asegurando que los documentos del sistema se encuentren debidamente elaborados, identificados, actualizados y accesibles para las partes interesadas.

8.6.1 Recursos del SGSI

La organización debe determinar y comunicar las capacidades necesarias para su establecimiento, implementación, mantenimiento y mejora continua.

Esta asignación se consolida a través de seis factores fundamentales:

- **Talento Humano:** Asignación de personal con roles y responsabilidades definidos para la administración, monitoreo y auditoría del SGSI.
- **Presupuesto:** Aprobación de términos financieros dedicados a la adquisición de tecnología, licenciamiento, servicios especializados, auditorías y contingencias operativas.
- **Infraestructura Física y Tecnológica:** Aseguramiento de instalaciones seguras, centros de procesamiento de datos, equipos de red y servidores con las condiciones de contingencia necesarias.
- **Herramientas de Seguridad:** Despliegue de soluciones especializadas para la protección de la información, ya sea como antivirus corporativos, sistemas de prevención de intrusos (IPS/IDS), cifrado y gestión centralizada de registros (*logs*).
- **Servicios Externos y Proveedores:** Contratación de consultorías especializadas, soporte técnico de terceros, plataformas en la nube y servicios administrados de ciberseguridad.

8.6.2 Competencia

La organización debe examinar y corroborar qué conocimientos necesita el personal que desempeña funciones relacionadas con seguridad.

Tabla 15 Matriz de competencias.

Cargo	Competencia requerida	Competencia actual	Necesidad de capacitación
Administrador TI	gestión de accesos	media	si
Responsable SGSI	ISO 27001	Alta	no

Explicar

8.6.3 Concienciación y Capacitación

La efectividad de un SGSI resulta del comportamiento del factor humano. Por esto, la organización debe garantizar que el personal, sin importar su rol o tipo de contratación, comprenda sus responsabilidades operativas y los riesgos al manejo de la información.

Esta gestión se fomenta mediante el Programa de Concienciación y Capacitación, un instrumento metodológico con base en fortalecer la cultura de seguridad institucional a través de dos factores principales:

- **Módulos Temáticos de Formación:** Abarcan temas críticos de prevención operativa como la creación y custodia de contraseñas seguras, la detección de ataques de *phishing* e ingeniería social, las pautas para el manejo correcto de información sensible, la política de uso aceptable de recursos informáticos y dispositivos, y el procedimiento formal para el reporte oportuno de incidentes de seguridad.
- **Mecanismos de Control y Evidencias Auditables:** Garantizar la trazabilidad del programa por medio de auditorías a través del registro sistemático de listas de asistencia a capacitaciones, material didáctico, evaluaciones de conocimiento, certificados y métricas derivadas del seguimiento a campañas de concienciación.

8.6.4 Gestión de la Comunicación

La organización debe armar un esquema formal de comunicación interna y externa. En cumplimiento de los requisitos de la norma, esta herramienta se define mediante la matriz de comunicación, la cual determina con claridad:

- **Qué se comunica:** políticas, alertas de seguridad, incidentes de alto impacto o cambios normativos.
- **A quién se comunica:** personal interno, partes interesadas, clientes, proveedores, autoridades reguladoras o medios de comunicación.
- **Cuando se comunica:** Oportunidad y frecuencia del mensaje, ya sea de forma periódica (campañas, boletines) o coyuntural (activación de protocolos ante incidentes).
- **Cómo se comunica:** Canales oficiales habilitados, como correo institucional, intranet, comunicados formales o reuniones operativas.
- **Quién comunica:** Roles y voceros autorizados dentro de la estructura de gobierno del SGSI para emitir información oficial.

8.6.5 Control de la Información Documentada

De acuerdo con la Cláusula 7.5 de la norma ISO/IEC 27001:2022, la organización debe armar un procedimiento para el control documental que regule el ciclo de vida de las políticas, procedimientos, instructivos y registros del SGSI, asegurando su confidencialidad, integridad, disponibilidad y trazabilidad.

Se formaliza mediante el Procedimiento de Control Documental, el cual pone como estándar la elaboración, aprobación, almacenamiento, distribución y disposición final de los documentos mediante el seguimiento de nueve atributos clave:

- **Estructura y Clasificación:** Asignación de código único, nombre descriptivo, versión vigente y fecha de emisión o actualización.
- **Responsabilidad y Autoridad:** Identificación clara del elaborador o responsable del contenido

y del aprobador designado dentro del SGSI.

- **Estado y Control de Cambios:** Indicación del estado del documento (borrador, aprobado, obsoleto) junto con el historial de modificaciones que sustenta sus revisiones.
- **Disposición y Acceso:** Definición de la ubicación centralizada de almacenamiento (física o digital) y el control de permisos para asegurar su consulta y evitar el uso involuntario de versiones obsoletas.

8.7 Operación y Ejecución del SGSI (Cláusula 8)

Esta fase representa la acción en marcha de las actividades elaboradas en la etapa de planificación (Cláusula 6) y la ejecución del Plan de Tratamiento de Riesgos. Atraves de la operación, la organización despliega los procesos, políticas y procedimientos diseñados para controlar los riesgos de seguridad de la información identificados.

8.8 Implementación de Controles del Anexo A (ISO/IEC 27001:2022)

La selección y distribución de los controles de seguridad deben corresponder a las prioridades definidas en el Plan de Tratamiento de Riesgos y a la Declaración de Aplicabilidad (SoA). Gracias a esto con la actualización del estándar, los controles se estructuran en cuatro dominios clave:

- **A.5 Controles Organizacionales:** Define la estructura de gobierno de la seguridad de la información. Abarca la formulación de políticas, asignación de roles y responsabilidades, gestión de activos, seguridad en la cadena de suministro y proveedores, gestión de incidentes, continuidad del negocio y cumplimiento legal o normativo.
- **A.6 Controles de Personas:** Enfocado en la gestión del factor humano a lo largo del ciclo de vida laboral. Comprende la definición de responsabilidades contractuales, procesos de concienciación y capacitación continua, gestión de cambios en el personal (ingresos,

traslados, desvinculaciones) y mecanismos para el reporte oportuno de eventos de seguridad.

- **A.7 Controles Físicos:** Dirigido a la protección perimetral y ambiental de las instalaciones. Incluye el establecimiento de áreas seguras, control de acceso físico a centros de datos, protección de equipos e infraestructura tecnológica, y medidas de salvaguarda frente a amenazas ambientales o desastres naturales
- **A.8 Controles Tecnológicos:** Enfocado en la seguridad técnica de la infraestructura de TI. Contempla mecanismos de autenticación y control de acceso lógico, protección contra código malicioso (*antimalware*), gestión de copias de seguridad, registro y monitoreo de eventos (*logs/SIEM*), seguridad en redes y telecomunicaciones, gestión de vulnerabilidades técnicas, uso de criptografía y prácticas de desarrollo seguro de software.

8.9 Evaluación del Desempeño del SGSI (Cláusula 9)

Una vez dada la fase operativa, la organización debe verificar la suspicacia del Sistema de Gestión de Seguridad de la Información frente a sus objetivos dispuestos. En cumplimiento de la Cláusula 9 de la norma ISO/IEC 27001:2022, este factor establece los mecanismos institucionales para medir la salud del SGSI, hallar desviaciones operativas y asegurar la alineación estratégica del sistema con las metas del negocio.

Esta etapa de supervisión y control se estructura a través de tres componentes metodológicos:

- **Seguimiento, Medición, Análisis y Evaluación:** Definición de métricas e indicadores clave de desempeño (KPI) para reconocer la efectividad de los controles implementados, la recurrencia de incidentes y el nivel de cumplimiento de los objetivos de seguridad.
- **Auditoría Interna:** Evaluaciones periódicas e independientes para ver si el SGSI cumple con los requisitos propios de la organización y con los estándares de la norma ISO/IEC 27001, asegurando la recolección de evidencias auditables.

- **Revisión por la Dirección:** Evaluación formal por parte de la alta dirección en base al estado del sistema, analizando los resultados de auditorías, el cumplimiento de objetivos, la retroalimentación de las partes interesadas y ajustar prioridades estratégicas.

8.9.1 Auditoría Interna del SGSI

De acuerdo con los requisitos del numeral 9.2 de la norma ISO/IEC 27001:2022, la organización debe establecer e implementar un cronograma de auditorías internas periódicas. Este proceso permite evaluar de manera objetiva si el SGSI cumple con las directrices internas, abarca las exigencias de la norma y se mantiene eficaz.

Para estructurar la trazabilidad y ejecución de las auditorías, se gestiona un flujo de seis documentos fundamentales:

- **Gestión y Planificación Operativa:** formalizar el *Programa de Auditoría* (planificación anual de evaluaciones) junto con el *Plan de Auditoría* específico para cada ciclo.
- **Herramientas de Ejecución y Levantamiento:** Se utiliza la *Lista de Verificación* para guiar el trabajo de y verificar el cumplimiento de cada requisito.
- **Resultados y Respuesta Organizacional:** Generar el *Informe de Auditoría* con los hallazgos encontrados, el *Registro de Hallazgos / No Conformidades* y el *Plan de Acciones Correctivas*.

Tómese como plantilla el siguiente documento elaborado por el ingeniero Henry Guio, profesor de la Universidad Santo Tomás seccional Tunja

ALCANCE
RECURSOS
MÉTODOS
EQUIPO DE AUDITORES
LIDER:

ACOMPañANTE(S)
):

OBSERVADOR(RE
S):

CONFIDENCIALIDAD

CRITERIOS

IDENTIFICACIÓN DE RIESGOS	
RIESGO	CONTROL DEL RIESGO
Inasistencia de los auditores	
Inasistencia de los auditados	
Orden público	
Prolongación de la auditoría	
Conflictos	
Competencias de los auditores	
Adaptación a la reestructuración del SGC	
Dificultades o problemas con las herramientas tecnológicas (Microsoft teams, google meet, zoom, internet, página web)	

CALENDARIO DE AUDITORÍAS							
SEDE SECCIONAL	/	AUDITOR	PROCESO	LÍDER DEL PROCESO	FECHA		
					DD	MM	AA
							HORA

SEGUIMIENTO

FECHA DE SEGUIMIENTO

PROCESO	RESPONSABLE	DD	MM	AA	OBSERVACIONES
---------	-------------	----	----	----	---------------

Desarroll					
o de					
Software					

APROBÓ:

F

I

R

M

A

:

N

O

M

B

R

E

:

FECHA:

8.9.2 Revisión por la Dirección

En cumplimiento de la Cláusula 9.3 de la norma, la alta dirección tiene que examinar el desempeño del SGSI para tener su conveniencia, adecuación y eficacia continuas. Este análisis estratégico se basa en el Acta o Informe de Revisión por la Dirección, el cual tiene que traer a discusión insumos clave como los resultados de auditorías, métricas de indicadores (KPIs), incidentes registrados y el estado actual de los riesgos. Asu vez, se evalúan los cambios en el contexto de la organización (Advisera, 2024).

8.9.3 Mejora Continua y Gestión de No Conformidades (Cláusula 10)

Se consolida mediante la aplicación de la mejora continua (Cláusula 10), Asegurando que las fallas del sistema se transformen en oportunidades de fortalecimiento organizacional (AES Tech, 2026).

Si existe una no conformidad, la organización ejecuta un procedimiento estructurado de nueve pasos:

Detección y Registro: Identificación formal de la desviación y documentación del evento en el registro de incidencias del SGSI.

Análisis Causa Raíz: Evaluación analítica para determinar la causa subyacente que originó el fallo, evitando soluciones meramente superficiales.

Planificación y Asignación: Definición de la acción correctiva correspondiente, asignando un responsable directo de ejecución y fijando un plazo límite de cumplimiento.

Ejecución y Verificación: Puesta en marcha de las medidas correctivas, comprobación posterior de su efectividad práctica y registro del cierre formal de la no

conformidad

9. CONCLUSIONES

El cumplimiento de los objetivos específicos ayudó a construir una secuencia metodológica seria para abordar la implementación de la ISO/IEC 27001:2022 A través de una visión documental y práctica.

El primer objetivo se alcanzó mediante la revisión bibliográfica y la matriz diagnóstica construida a partir de 29 estudios, lo que ayudó a identificar y clasificar brechas de seguridad según la relación con las cláusulas de la norma y los dominios del Anexo A.

El segundo objetivo permitió caracterizar los factores compuestos con la implementación a través del análisis comparativo de la literatura, hallando elementos relacionados con el compromiso de la dirección, la gestión de riesgos, las políticas, la capacitación y la cultura de seguridad.

El tercer objetivo ayudó a trasladar estos hallazgos hacia la evaluación de controles del Anexo A mediante criterios de costo, dificultad e impacto. Por último, estos resultados sirvieron como sustento para el diseño de la guía práctica, por lo que los objetivos no fueron abordados de manera única, sino como etapas sucesivas de una misma propuesta.

- La revisión de la literatura permitió consolidar que las dificultades de implementación de un SGSI no dependen únicamente de la adopción de controles tecnológicos. Los estudios analizados mostraron la importancia de factores organizacionales y humanos, la asignación de recursos, la gestión de riesgos, la capacitación y la existencia de políticas de seguridad. Esta evidencia permitió orientar la propuesta hacia una implementación integral de la ISO/IEC 27001:2022.
- La matriz diagnóstica formó un mecanismo para transformar la información desordenada de la literatura en evidencia comparable y útil para la toma de decisiones. La clasificación de las brechas a través de las cláusulas de la ISO/IEC 27001:2022 y los factores del Anexo A permitió identificar patrones repitentes y establecer una relación entre las dificultades en los estudios y las necesidades que deben ser tomadas en cuenta durante la implementación de un SGSI. Este resultado constituye una síntesis de la evidencia documental analizada y da una base para guiar procesos de diagnóstico en organizaciones que pretendan adoptar la norma.
- La evaluación de los controles dio a entender que la priorización de la implementación requiere considerar el impacto esperado y las condiciones necesarias para adoptar cada control. La incorporación de criterios de costo, dificultad e impacto ayudó a diferenciar controles que

pueden abordarse inicialmente de aquellos que necesitan mayores capacidades técnicas, económicas u organizacionales. Esta visión evita plantear la implementación del Anexo A como una actividad uniforme y permite dar una estrategia general, aspecto especialmente relevante para organizaciones que cuentan con recursos limitados.

- La principal contribución de la investigación se da en la integración de los resultados bibliográficos, el análisis de factores críticos y la evaluación de estos en una guía práctica de implementación de la ISO/IEC 27001:2022. Esta guía no se limita a listar los requisitos de la norma, sino que los transforma en actividades aplicables, procedimientos y evidencias que pueden orientar el diagnóstico inicial. De esta manera, la investigación aporta un instrumento de orientación dirigido principalmente a organizaciones que requieren una ruta estructurada para iniciar o fortalecer la implementación de un SGSI.
- La guía propuesta adquiere un valor adicional al relacionar los controles con acciones de implementación. Los procedimientos desarrollados para aspectos como políticas de seguridad, control de accesos, protección contra malware, gestión de registros y seguridad física ayudan a pasar de la identificación de una necesidad de seguridad a una actividad verificable mediante evidencias. Esta función favorece la aplicabilidad de la propuesta, por esto permite que una organización no solo identifique qué debe controlar, sino que también disponga de una referencia sobre cómo iniciar su implementación y qué elementos puede utilizar para demostrarla.

10 REFERENCIAS

- Abeykoonge, K. (2024). *Organizational culture influence on ISO 27001 implementation*. ResearchGate. <https://www.researchgate.net/publication/391181885>
- Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9, 44928–44949. <https://doi.org/10.1109/ACCESS.2021.3066383>
- Advisera. (2024). *ISO 27001 clause 9.3 – Management review*. 27001Academy. <https://advisera.com/iso27001/clause-9-3-management-review/>
- Advisera. (2024). *ISO 27001 risk assessment & risk treatment: The complete guide*. 27001Academy. <https://advisera.com/27001academy/iso-27001-risk-assessment-treatment-management/>
- Al-Amiri, A., et al. (2024). *Adoption of new technologies in university environments and its impact on information security*. Al-Kut College Journal. https://js.alkutcollege.edu.iq/article_24703.html
- Alassaf, N., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. *IEEE Access*, 9, 162687–162705. <https://doi.org/10.1109/ACCESS.2021.3132574>
- Aljuaid, T. A. A. M., Abdul Wahab, A. W., & Idris, M. Y. I. (2023). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment: State of the art and future directions. *Applied Sciences*, 13(14), 8048. <https://doi.org/10.3390/app13148048>
- Almorsy, M., Grundy, J., & Müller, I. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security*, 77, 565–577. <https://doi.org/10.1016/j.cose.2018.05.009>
- Andersson, A., Hedström, K., & Karlsson, F. (2022). Standardizing information security: A structurational analysis. *Information & Management*, 59(3), 103623. <https://doi.org/10.1016/j.im.2022.103623>
- Angelini, M., et al. (2022). *Security gaps and policy updates in IT companies*. arXiv. <https://arxiv.org/abs/2207.03269>
- Annarelli, A., Battistella, C., & Nonino, F. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal*, 33(7), 76–105. <https://doi.org/10.1108/TQM-09-2020-0202>
- Arumdiya, R., & Rudianto, R. (2025). *Training deficiencies and their impact on information security management systems*. ResearchGate. <https://www.researchgate.net/publication/394151106>
- Assolin, J., Kreutz, D., & Bertholdo, L. M. (2025). IoTedu: Access control, detection, and automatic incident response in academic IoT networks. arXiv. <https://doi.org/10.48550/arXiv.2512.09934>
- AES Tech. (2026). *ISO 27001: Clause 10 – Improvement*. AES Tech. [Consultar fuente](#)

Ayinoluwa, O. (2024). *Organizational factors affecting governance and ISO standards adoption*. ResearchGate. <https://www.researchgate.net/publication/380129833>

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118–131. <https://ora.ox.ac.uk/objects/uuid:cfed4907-d32a-4450-b075-ad37477b10d8>
Biswas, P. (2022, diciembre 8). *ISO 27001:2022 A.5.2 Information security roles and responsibilities*. PRETESH BISWAS. <https://preteshbiswas.com/2022/12/08/a-5-2-information-security-roles-and-responsibilities/>

Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education*, 8(2), 34–42. <https://doi.org/10.37134/jictie.vol8.2.4.2021>

Chávez, D., et al. (2024). *Information security in internet service companies*. IEEE. <https://www.researchgate.net/publication/379162806>

Chen, H., & Hai, Y. (2024). Exploring the critical success factors of information security management: A mixed-method approach. *Information and Computer Security*, 32(5), 545–572. <https://doi.org/10.1108/ICS-03-2023-0034>

Culot, G., Nassimbeni, G., Orzes, G., & Sartor, M. (2021). Behind the definition of ISO 27001 information security management systems: A literature review. *Computers & Security*, 103, 102192. <https://doi.org/10.1016/j.cose.2021.102192>

Confluence IEEE Study. (2024). *Risk methodologies for ISMS implementation*. IEEE Xplore. <https://ieeexplore.ieee.org/document/10463392>

Domínguez, J., et al. (2023). *Organizational factors in ISO 27001 implementation*. arXiv. <https://arxiv.org/abs/2306.11050>

Domínguez, J., et al. (2023b). *Organizational challenges in ISO implementation*. EasyChair. <https://easychair.org/publications/preprint/wS2G>

Domínguez-Domínguez, J., López, A., & Martínez, F. (2023). *Organizational leadership and security awareness gaps in higher education institutions*. arXiv. <https://arxiv.org/abs/2306.11050>

Financial Institution ISO Study. (2024). *ISO 27001 integration in banking sector*. IEEE Xplore. <https://ieeexplore.ieee.org/document/10569415>

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2025). Implementing and integrating security controls: A practitioners' perspective. *Computers & Security*, 156, 104516. <https://doi.org/10.1016/j.cose.2025.104516>

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 4759. <https://doi.org/10.3390/s21144759>

Hernandez, L., Pranolo, A., & Wibawa, A. P. (2024). Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis: Case study: Higher education institution. *Transactions on Energy Systems and Engineering*

Applications, 5(2), 1–20. <https://doi.org/10.32397/tesea.vol5.n2.635>

Horne, C. A., Maynard, S. B., & Ahmad, A. (2022). A survey on empirical security analysis of access-control systems: A real-world perspective. *ACM Computing Surveys*, 55(6), 1–36. <https://doi.org/10.1145/3533703>

International Organization for Standardization. (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. <https://www.iso.org/standard/27001.html>

Jevelin, R., & Faza, M. (2023). *Early stages of ISMS implementation in private organizations*. *Journal of Information Systems and Informatics*. <https://journal-isi.org/index.php/isi/article/view/572>

Kamil, M., Hallikainen, P., et al. (2023). *Organizational knowledge and ISO 27001 adoption challenges*. *Information Systems and e-Business Management*. <https://doi.org/10.1007/s10257-023-00646-y>

Kamil, Y., Lund, S., & Islam, M. S. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and e-Business Management*, 21, 699–722. <https://doi.org/10.1007/s10257-023-00646-y>

López-Vasco, J., et al. (2025). *Structured approaches for ISO 27001 implementation in technology companies*. IEEE. <https://www.researchgate.net/publication/390369079>

Niemeläinen, T., et al. (2024). *Resource allocation issues in technology companies*. arXiv. <https://arxiv.org/abs/2409.19029>

Ramadhan, A., & Sopiah, S. (2024). *Security breaches in transportation sector organizations*. UNESA Journal. <https://ejournal.unesa.ac.id/index.php/jdbim/article/view/65912>

Reuben-Owoh, B., & Haig, E. (2025). A systematic review of voluntary cybersecurity standards and frameworks. *International Journal of Information Security*, 24, Article 206. <https://doi.org/10.1007/s10207-025-01121-0>

Rietveld, J., Slob, E., & van Kalmthout, R. (2022). What drives the growth of start-up firms? A tool for mapping the state-of-the-art of the empirical literature. *Journal of Business Venturing Insights*, 18, e00345. <https://doi.org/10.1016/j.jbvi.2022.e00345>

Ryanto, R., & Tundjungsari, V. (2024). *Data leakage risks in banking institutions*. ResearchGate. <https://www.researchgate.net/publication/383041040>

Shekhawat, A. S., Di Troia, F., & Stamp, M. (2019). Feature analysis of encrypted malicious traffic. *Expert Systems with Applications*, 125, 130–141. <https://doi.org/10.1016/j.eswa.2019.01.064>

Shen, B. (2023). *A survey of access control misconfiguration detection techniques*. arXiv. <https://doi.org/10.48550/arXiv.2304.07704>

Silva, E. M., Abreu, A., & Pires, G. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, 99, 102030. <https://doi.org/10.1016/j.cose.2020.102030>

Suorsa, M., & Helo, P. (2024). Information security failures identified and measured: ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis. *Information Security Journal: A*

Global Perspective, 33(3), 285–306. <https://doi.org/10.1080/19393555.2023.2270984>

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. *IEEE Access*, 10, 39325–39343. <https://doi.org/10.1109/ACCESS.2022.3164739>

Tanadi, T., et al. (2021). *External audits and ISMS continuous improvement in ISO 27001 certified organizations*. Reaksi. <https://journals.ums.ac.id/index.php/reaksi/article/view/15146>

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess ransomware risks. *International Journal of Information Management*, 52, 102090. <https://doi.org/10.1016/j.ijinfomgt.2020.102090>

Wibowo, A., & Aji, P. (2024). *ISMS implementation in healthtech organizations*. IJCS. <https://www.ijcs.net/ijcs/index.php/ijcs/article/view/4166>

Wijayarathne, W. (2022). *ISO 27001 implementation in laboratory environments*. ResearchGate. <https://www.researchgate.net/publication/372523436>

Zammani, M., & Razali, R. (2016). An empirical study of information security management success factors. *International Journal on Advanced Science, Engineering and Information Technology*, 6(6), 904–913. <https://doi.org/10.18517/ijaseit.6.6.1371>

Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management & Data Systems*, 121(3), 613–636. <https://doi.org/10.1108/IMDS-06-2020-0321>