Benemérita Universidad Autónoma de Puebla

Facultad de Ciencias de la Computación

T E S I S

“ISO 27001: UNA PROPUESTA DE GUÍA PARA SU IMPLEMENTACIÓN”

Presenta: *Luis Alberto Ramirez Roque*

Para obtener el grado de: Licenciatura en Ciencias de la Computación

Director/Asesor: *DR. Rafael de la Rosa Flores*

Puebla, Pue., Noviembre 2025

Contenido

Capítulo 1: Introducción

1.1 Introducción

Hoy en día se libra una guerra que no se anuncia con sirenas ni se desata con bombas, al contrario, se desarrolla en silencio, oculta en líneas de código y en redes invisibles. En este conflicto los soldados no visten uniformes ni armas de fuego, sino que sus herramientas son teclados y sus armas son el conocimiento para adentrarse en cualquier sistema. Este escenario de una guerra mundial silenciosa, se reconfigura la importancia de la seguridad de la información en la era digital (Castillo del Río, 2025b).

Ahora la protección sistemática de la información se ha convertido en un eje estratégico de las organizaciones públicas y privadas. En este contexto, la norma ISO/IEC 27001:2022 proporciona un marco sólido, flexible y reconocido a nivel mundial para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) (Parolin, 2022).

Por lo tanto, el presente documento tiene como objetivo principal servir como guía técnica y práctica para la implementación gradual y sostenible de un SGSI, basado en las etapas del ciclo PDCA (Planificar–Hacer–Verificar–Actuar) (ISO/IEC, 2022, cláusula 10.2). Para ello, la propuesta se basa tanto en los lineamientos normativos de la ISO/IEC 27001 como en buenas prácticas internacionales, en documentación de soporte especializado y en experiencias aplicadas en diversos contextos organizacionales.

Cada sección tiene definiciones operacionales, pasos en orden secuencial, criterios de aceptación, indicadores clave de desempeño y de riesgo (KPI/KRI) y recomendaciones técnicas que permiten su inmediata aplicación.

De esta manera, el lector obtendrá herramientas concretas para el diseño, implantación y mantenimiento de un SGSI alineado a los objetivos estratégicos de la organización. El enfoque busca unir rigor académico y efectividad operativa, lo que incluye elementos documentales, organizativos, tecnológicos y culturales.

Esta propuesta es escalable y modular; además, resulta adaptable a diferentes tamaños de organización, modular, con un análisis de contexto y trazabilidad de controles, e integración de tecnologías emergentes como parte del ciclo de mejora continua.

Sin embargo, al ser una norma ampliamente reconocida y utilizada a nivel mundial, su especificación técnica a veces se encuentra opaca y acorde a muchos usos de las organizaciones que no cuentan con el presupuesto necesario para su aplicación. Son muchas las pequeñas y medianas empresas (PYMES) que enfrentan la falta de capacidades como la disponibilidad de consultores, alto costo de consultorías, falta de capacidades o la falta de documentos guía, en su lengua y su contexto (Valencia Duque & Orozco Alzate, 2017). Con objeto de reducir esa brecha, se brinda una oferta asequible, aplicada y sensible al contexto real de estas organizaciones.

En síntesis, el presente documento se ofrece como un aporte que tiene como fin reducir las barreras de entrada a la norma ISO/IEC 27001:2022, así como también ofrecer claridad metodológica en su implementación, y sobre todo contribuir al fortalecimiento de la cultura de seguridad de la información en las organizaciones que lo adopten. (Parolin, 2022).

Para lograr este objetivo, el documento se estructura de la siguiente manera:

Capítulo 1: Introducción: Aborda la necesidad de proteger la información y presenta una guía práctica para implementar un SGSI basado en ISO 27001:2022 y PDCA, pensada para organizaciones con recursos limitados.

Capítulo 2: Marco Teórico: Explica los fundamentos de la seguridad de la información (tríada CIA, gestión de riesgos) y la evolución de ISO 27001 hasta la versión 2022. Define los SGSI y el ciclo PDCA.

Capítulo 3: Estado del Arte: Analiza las tendencias y riesgos en ciberseguridad, destacando las dificultades de adopción de ISO 27001 en PYMES y la necesidad de enfoques accesibles.

Capítulo 4: Metodología de la Investigación: Detalla el problema de la complejidad de ISO 27001 para PYMES, justifica la investigación y establece el objetivo de crear una guía metodológica cualitativa y propositiva.

Capítulo 5: Metodología de Implementación de ISO/IEC 27001: Presenta un modelo de implementación del SGSI siguiendo el ciclo PDCA (Planificar, Implementar, Operar, Monitorear y Mejorar Continuamente) con base en ISO 27001:2022.

Capítulo 6: Propuesta de guía y recursos para la implementación de ISO/IEC 27001:2022: Describe la guía metodológica propuesta, incluyendo fases prácticas para el análisis de riesgos, el establecimiento del alcance, la creación de políticas, la implementación de controles y la gestión de incidentes y auditorías.

Capítulo 7: Conclusiones y Recomendaciones: Resume el logro de los objetivos con una guía metodológica escalable y accesible como principal aporte. Aborda las consecuencias prácticas, limitaciones y futuras líneas de investigación para la mejora continua del SGSI.

Capítulo 2: Marco Teórico

2.1 Fundamentos de seguridad de la información

La seguridad de la información, disciplina que se encarga de proteger los activos de información contra diversas amenazas, con la finalidad de garantizar la continuidad del negocio, reducir los riesgos y elevar el retorno de inversión (PMG-SSI, 2024). Esta disciplina ha ido evolucionando desde un enfoque meramente técnico hacia una perspectiva integral que toma en cuenta aspectos organizacionales, humanos y estratégicos.

2.1.1 Principios fundamentales

La seguridad de la información se fundamenta en tres pilares fundamentales que son los que conforman la conocida tríada CIA, la cual abarca: confidencialidad, integridad y disponibilidad.

Confidencialidad: Asegura la protección contra el acceso no autorizado a la información. Se lleva a cabo mediante controles de acceso, métodos de cifrado, clasificación de información y convenios de confidencialidad. Por ejemplo, el cifrado AES-256 resguarda los datos/información/activos delicados durante su transmisión, mientras que los sistemas de autenticación de múltiples factores impiden accesos no autorizados (PMG-SSI, 2024).

Integridad: Es la encargada de que la información no haya sido alterada/modificada de manera no permitida, manteniendo su exactitud y totalidad. Los procedimientos más utilizados comprenden funciones hash criptográficas (como SHA-256), firmas/claves digitales, verificación de datos, controles de acceso granulares y detectar modificaciones no autorizadas en archivos críticos (PMG-SSI, 2024).

Disponibilidad: Garantiza que la información/datos y los sistemas estén disponibles cuando los usuarios autorizados lo requieran. Esto se logra llevar a cabo gracias a arquitecturas redundantes, balanceadores de carga, planes de recuperación para desastres, respaldos regulares y monitoreo o un seguimiento constante. Las estrategias comprenden la implementación de alta disponibilidad (99.9%) y la definición de tiempos de recuperación objetivos (RTO) (Gartner, 2023).

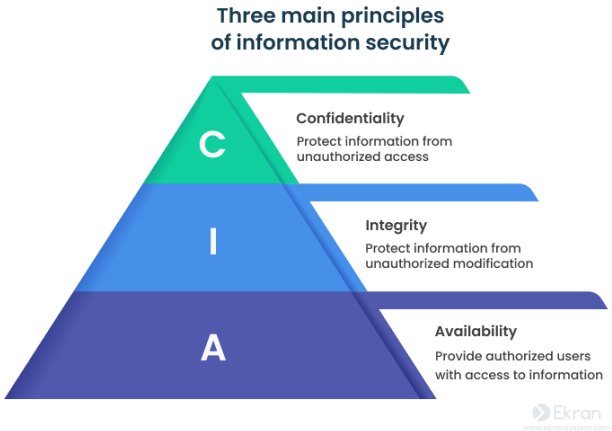

Figura 1: Representación gráfica de la Tríada CIA, los tres pilares fundamentales de la seguridad de la información. Adaptado de The InfoSec Guide to the 10 Types of Information Security Controls (Ohayon, 2024).

- **Confidencialidad**: Implica la protección de la información frente a accesos no autorizados, asegurando que únicamente el personal autorizado pueda consultarla, tal como se observa en la Figura 1.
- **Integridad**: Consiste en prevenir modificaciones no autorizadas en los datos, esto asegura su exactitud, coherencia y fiabilidad como se observa en la Figura 1.

- **Disponibilidad**: Garantiza el acceso oportuno y continuo a los sistemas y datos por parte de los usuarios autorizados, mediante mecanismos como respaldos, redundancia y balanceo de carga, tal como se observa en la Figura 1.

La Norma ISO/IEC 27001:2022 está especializada en la Tríada CIA (Confidencialidad, Integridad y Disponibilidad) como sus pilares fundamentales (Parolin, 2022). Sin embargo, la práctica de la seguridad de la información se ha ampliado para abordar a los vectores de cuales son más susceptibles de ataques. Por lo cual es crucial que se reconozca que la autenticación y la autorización son elementos de igual importancia, ya que estos son los garantizados en verificar la identidad y el control de acceso, el cual es un enfoque que refleja una visión más moderna y proactiva de la seguridad. (Auth0, n.d.).

- Autenticación: Determina la identidad del usuario. (Auth0, n.d.).
- Autorización: Determina qué nivel de acceso tiene el usuario. (Auth0, n.d.).

2.1.2 Amenazas y vulnerabilidades

Amenazas de seguridad: Situaciones, sucesos, eventos o acciones de individuos que tienen la capacidad de perjudicar a los activos de información. Se clasifican en función de su procedencia (naturales, humanas, ambientales, tecnológicas) o su intención (intencionadas, accidentales, ambientales). Las principales amenazas actuales con más relevancia en el ENISA Threat Landscape 2023 comprenden ransomware, phishing, ataques DDoS, amenazas internas y ataques a la cadena de suministro (ENISA, 2023).

Vulnerabilidades: Debilidades o deficiencias que pueden ser explotadas/aprovechadas por diversas amenazas para determinar un riesgo. Se clasifican en: técnicas (problemas de software, configuraciones inseguras), físicas (acceso no autorizado a instalaciones),

organizacionales (políticas inadecuadas o insuficientes, ausencia de procedimientos) y humanas (propensos a ingeniería social, ausencia de conocimientos) (OWASP, 2021).

Relación Entre Amenazas-Vulnerabilidades: El riesgo se origina de cruzar las amenazas potenciales con las vulnerabilidades actuales, considerando el posible efecto sobre los activos (OWASP, 2021). Esta relación se expresa a través de la fórmula básica adaptada de la norma ISO 27005 esto para incluir la vulnerabilidad de manera explicita:

Riesgo = Amenaza × Vulnerabilidad × Impacto

Como se muestra en la Figura 2, este modelo facilita la cuantificación y priorización de los riesgos para una administración efectiva de la seguridad.

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Figura 2: Matriz de evaluación y priorización de riesgos de ciberseguridad. Matriz de evaluación de riesgos de ciberseguridad. Adaptado de ¡Fácil y sencillo! Análisis de riesgos en 6 pasos (Incibe, 2017).

2.1.3 Gestión de riesgos

La gestión de riesgos es un procedimiento sistemático que facilita la identificación, análisis, evaluación y manejo de riesgos relacionados con los activos de información, ofreciendo el fundamento para la elección e implementación de controles adecuados (ISOTools, 2017).

Proceso de gestión de riesgos: La norma ISO 27005 dicta pautas que constituyen el establecimiento del contexto, valoración del riesgo (identificación, análisis y evaluación), tratamiento (minimizar, transferir, prevenir o aprobar), la comunicación y consulta constante, además del monitoreo y revisión regular. Este proceso iterativo asegura que la gestión de riesgos evolucione con el ambiente organizacional (ISOTools, 2017).

Metodologías de gestión de riesgos: Se conocen varias metodologías como ISO 27005, NIST SP 800-30, OCTAVE, MAGERIT y FAIR. La elección de la metodología adecuada se basa en elementos como el tamaño y la complejidad de la organización, requerimientos regulatorios particulares y el nivel de madurez en seguridad de la información (NIST, 2012).

Integración con ISO 27001: La gestión de riesgos es el núcleo central de la ISO 27001. La cláusula 6 exige que las entidades establezcan un procedimiento estructurado de evaluación de riesgos, detecten y examinen los riesgos de seguridad, seleccionen alternativas de tratamiento y controles apropiados, y elaboren un plan de tratamiento autorizado por los dueños (NIST, 2012).

2.2 Evolución de la norma ISO 27001

En términos de evolución, la ISO 27001 ha sufrido un cambio considerable desde sus comienzos hasta llegar a ser conocida como el estándar internacional más prestigioso para la

gestión de seguridad de la información, ajustándose de manera constante a las amenazas ascendentes y requerimientos de las organizaciones.

2.2.1 Antecedentes históricos

BS 7799 (1995): La primera aparición fue la norma británica BS 7799, publicada por el British Standards Institute (BSI), el cual fue el primer precedente y proporcionó las primeras recomendaciones organizadas para las mejores prácticas en seguridad de la información en el sector empresarial (López, s. f.-c).

BS 7799-1 y BS 7799-2 (1999): De manera estratégica, la norma BS 7799 se fragmentó en dos partes: BS 7799-1 como norma de buenas prácticas informativas y BS 7799-2 con especificaciones técnicas para un SGSI, consolidándose como el primer estándar de certificación internacional (López, s. f.-c).

ISO/IEC 17799 (2000): Tanto la Organización Internacional de Normalización (ISO) como la Comisión Electrotécnica Internacional (IEC) establecieron BS 7799-1 como norma global, proporcionando recomendaciones y sugerencia a nivel global reconocidas para gestión de seguridad de la información (López, s. f.-c).

ISO/IEC 27001:2005: En 2005 se conoció como el nacimiento formal de la ISO 27001, especificando por primera vez requisitos específicos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar constante un SGSI (Parolin, 2022).

2.2.2 Evolución hacia ISO 27001:2013

La revisión de 2013 significó un gran cambio, sincronizando la norma con la Estructura de Alto Nivel (HLS) definida por ISO para todos los estándares de sistemas de gestión (Ed, 2013). Las modificaciones más relevantes comprendieron los siguientes puntos:

Estructura de alto nivel: La implantación de un marco común y consistente para todos los estándares de sistemas de gestión ISO, promoviendo la integración organizacional.

Enfoque basado en riesgos reforzado: Mayor interés en la detección proactiva de riesgos, evaluación sistemática y la evaluación constante del rendimiento del SGSI.

Reorganización de controles: Evolución del Anexo A, pasando de 11 secciones con 133 controles particulares a 14 secciones con 114 mejor estructurados y optimizados.

Flexibilidad documental mejorada: Disminución considerable de documentos prescriptivos, lo que permite una mayor adaptabilidad en la organización.

Enfoque en contexto organizacional: Principal interés en el entendimiento profundo del entorno organizacional y las demandas de los interesados relevantes.

2.2.3 ISO 27001:2022 - La versión vigente

En octubre de 2022, ISO puso en circulación la versión más actualizada y sofisticada. Esta actualización conserva la estructura de alto nivel y los requisitos fundamentales establecidos; sin embargo, introduce modificaciones innovadoras, principalmente en el Anexo A (Parolin, 2022):

Reorganización radical de controles: La aplicación de 4 cláusulas fundamentales (controles organizacionales, de personas, físicos y tecnológicos) en sustitución de las 14 secciones previas, simplifica de gran manera la comprensión y su uso.

Optimización cuantitativa: Disminución estratégica de 114 a 93 controles, a través de la combinación inteligente y la reestructuración de controles previos para incrementar la eficiencia operacional.

Controles emergentes: Incorporación de nuevos controles particulares para enfrentar tecnologías y riesgos actuales, que incluyen seguridad en computación en la nube, gestión de privacidad de datos y prevención avanzada de fugas de información.

Atributos descriptivos para controles: Incluir la información adicional del tipo de control, características de seguridad específicas y conceptos avanzados de ciberseguridad pertinentes.

Como se muestra en la Figura 3, la evolución de BS 7799 de 1995 a la normativa ISO/IEC 27001:2022 refleja un proceso de maduración técnica que consolida a la norma como el referente internacional en gestión de la seguridad de la información (López, s. f.-c; Parolin, 2022).

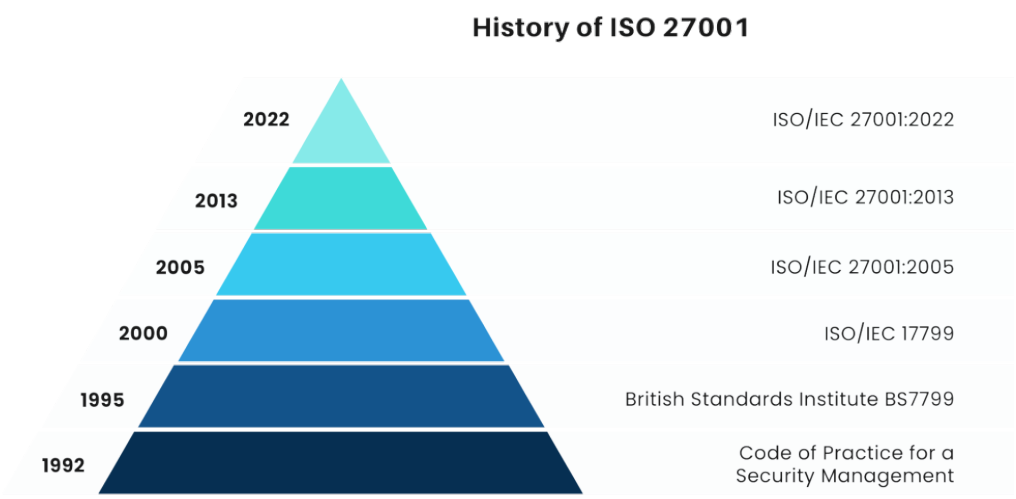

Figura 3: Línea de tiempo evolutiva de los estándares ISO/IEC 27001. Adaptado de How ISO/IEC 27001 Certification Enhances an Organization's Cybersecurity: A Comprehensive Guide (Microtek Learning, 2024)

2.2.4 La familia de normas ISO 27000

ISO 27001 es el pilar de una familia integral de estándares interconectados para seguridad de la información (ISOTools, 2015). Los estándares complementarios clave incluyen:

- **ISO/IEC 27000**: Proporciona visión general conceptual y vocabulario técnico especializado.
- **ISO/IEC 27002**: Código detallado de prácticas para implementación de controles de seguridad.
- **ISO/IEC 27003**: Orientación práctica específica para implementación efectiva de SGSI.
- **ISO/IEC 27004**: Directrices especializadas para medición, monitoreo y evaluación de desempeño.
- **ISO/IEC 27005**: Directrices comprehensivas para gestión avanzada de riesgos de seguridad.
- **ISO/IEC 27701**: Extensión especializada para gestión de información de privacidad y protección de datos.
- **ISO/IEC 27017/27018**: Directrices específicas para servicios en computación en nube y protección de datos personales.
- **ISO/IEC 27031**: Directrices para continuidad de servicios de tecnologías de información y comunicación.
- **ISO/IEC 27035**: Marco estructurado para gestión integral de incidentes de seguridad.

La arquitectura coherente de esta familia ofrece un enfoque holístico y sistemático para la seguridad de la información, permitiendo a las organizaciones seleccionar y combinar estándares específicos relevantes para su contexto operacional particular (ISOTools, 2015).

2.3 Sistemas de Gestión de Seguridad de la Información (SGSI)

Un SGSI representa el método sistemático y estructurado para establecer, implementar, operar, monitorear, revisar, mantener y mejorar de manera sustancial la seguridad de la información en el entorno organizacional (NQA, 2023).

2.3.1 Definición y objetivos

Definición formal: De acuerdo con la norma ISO 27001, un SGSI es "el componente del sistema de gestión general de una organización, fundamentado en un enfoque de riesgo empresarial, diseñado para establecer, implementar, operar, monitorear, revisar, mantener y potenciar la seguridad de la información de manera sistemática y organizada" (Parolin, 2022).

Objetivos estratégicos principales:

- Protección completa de activos esenciales de la información de la organización.
- Manejo sistemático y proactivo de riesgos de seguridad.
- Cumplimiento estricto de requisitos normativos y regulatorios pertinentes.
- Implementación de mejora constante en los procesos de seguridad.
- Fortalecimiento de la resiliencia organizacional ante amenazas.

Valor estratégico organizacional: Un SGSI debe ser entendido como un instrumento esencial que aporta valor palpable a la organización (NQA, 2023), vinculando de manera satisfactoria la seguridad de la información con objetivos de negocio, mejorando la toma de

decisiones ejecutivas, incrementando el retorno de inversiones en seguridad y estableciendo un lenguaje común organizacional para gestión de riesgos.

2.3.2 Componentes fundamentales

Estructura organizativa y liderazgo ejecutivo: Establecer claramente los roles y funciones para la junta directiva, el comité encargado de seguridad, los responsables de seguridad de la información, los encargados de los activos críticos y personal operativo general (NQA, 2023).

Políticas y procedimientos documentados: Marco documental integral que proporciona, que ofrece una, guía estratégica y acompañamiento operativo, desde políticas generales de alto nivel hasta procedimientos particulares detallados, instrucciones técnicas y registros de cumplimiento (NQA, 2023).

Gestión integral de riesgos: Metodología sistemática basada en riesgos que abarca un enfoque estructurado de evaluación, los activos críticos con un inventariado detallado, un análisis profundo de amenazas y vulnerabilidades, una valoración tanto cuantitativa como cualitativa de riesgos, tratamiento adecuado y personalizado de riesgos detectados y declaración formal de aplicabilidad (ISOTools, 2017).

Implementación efectiva de controles: Las medidas concretas y cuantificables, las cuales son necesarias para mitigar riesgos detectados, las cuales incluyen controles técnicos sofisticados, controles físicos sólidos, controles administrativos adecuados, y controles legales y normativos apropiados (ISOTools, 2017).

Medición, monitoreo y mejora continua: Sistema integral de métricas de seguridad, seguimiento continuo de efectividad de controles, auditorías internas regulares, revisiones

ejecutivas periódicas, administración proactiva de incumplimientos y configuración de medidas correctivas y preventivas (Parolin, 2022).

Gestión proactiva de incidentes: Habilidad organizacional para detectar de manera temprana, reportar eficientemente, evaluar adecuadamente, responder efectivamente, aprender sistemáticamente y mejorar continuamente a partir de incidentes de seguridad de la información (Parolin, 2022).

2.3.3 La implementación del ciclo PDCA en el SGSI

El ciclo PDCA (Planificar-Hacer-Verificar-Actuar) representa el modelo núcleo para la mejora continua, ampliamente implementado en sistemas de gestión más actuales (Parolin, 2022). Como se muestra en la Figura 4, este ciclo permite que las organizaciones mantengan un proceso dinámico de mejora constante para garantizar la eficacia del SGSI.

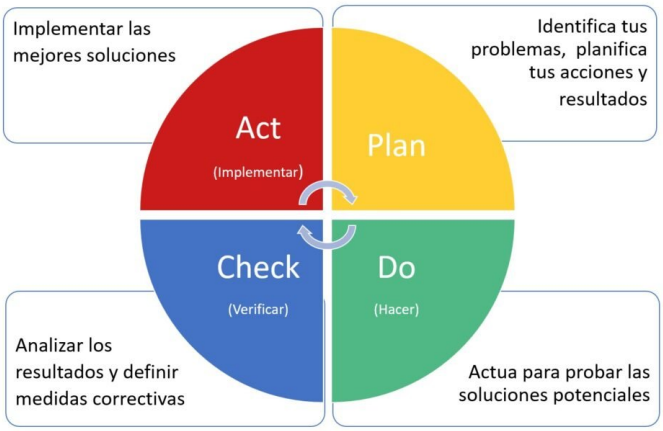

Figura 4: Diagrama del ciclo PDCA aplicado al SGSI. Adaptado de Implementa el ciclo Plan-Do-Check-Act para mejorar tu empresa (MDP Ajedrez, 2024).

Fase de Planificación (Plan): Esta fase establece cuáles son los fundamentos firmes del SGSI, especificando de manera clara, en el ámbito organizacional, política de seguridad de alto nivel, metodología sólida de evaluación de riesgos, y elección estratégica de controles adecuados (GlobalSuite Solutions, 2023).

Fase de Implementación (Do): En esta fase efectivamente se materializa lo planificado, poniendo en marcha el plan integral de gestión de riesgos, los controles escogidos y verificados, indicadores de rendimiento relevantes y programas integrales de formación y sensibilización (GlobalSuite Solutions, 2023).

Fase de Evaluación (Check): Esta fase es la encargada de verificar sistemáticamente si lo que se ha implementado cumple con las expectativas establecidas a través de seguimiento constante de indicadores, revisiones estructuradas reguladas, medición objetiva de eficacia de controles y auditorías internas rigurosas (GlobalSuite Solutions, 2023).

Fase de Mejora (Act): Esta fase se enfoca en la mejora sistemática continua, aplicando mejoras detectadas a través del análisis, acciones correctivas y preventivas apropiadas, y comunicación efectiva de resultados (GlobalSuite Solutions, 2023).

Como se muestra en la Figura 4, estas fases forman un ciclo dinámico e interconectado que impulsa la mejora continua del SGSI.

2.3.4 Beneficios y desafíos

Beneficios organizacionales clave (ISOTools, 2015):

***Operativos*:** Manejo más eficiente de riesgos de seguridad, disminución de incidentes de seguridad, mayor incremento en la resistencia de la organización ante amenazas emergentes y optimización de procesos operativos.

***Cumplimiento*:** El cumplimiento sistemático de los requisitos legales y normativas necesarias, muestra objetiva de la responsabilidad necesaria frente a auditorías e inspecciones regulatorias.

***Comerciales*:** La obtención de una notable ventaja competitiva sostenible, mejora significativa de la imagen corporativa y reputación de la empresa, acceso simplificado a nuevos mercados y oportunidades comerciales.

***Organizacionales*:** El aumento notable de sensibilización en seguridad, aclaración efectiva de las responsabilidades y roles, mejora sustancial en comunicación entre departamentos.

Desafíos contemporáneos comunes (ISOTools, 2015):

***Organizacionales*:** El mantenimiento y adquisición de un compromiso directivo mantenido, incorpora de manera eficaz la seguridad en la cultura de la organización y la administración adecuada de la resistencia al cambio.

***Técnicos*:** La adecuada selección de controles técnicos eficaces, balance óptimo entre una seguridad sólida y una usabilidad práctica, adaptación a tecnologías más recientes.

***Recursos*:** Es la parte destinada a recursos humanos y económicos adecuados, desarrollo constante de diferentes habilidades técnicas especializadas, justificación objetiva del rendimiento de la inversión.

***Implementación*:** La determinación adecuada del alcance de la organización, elaboración de la metodología de evaluación personalizada, generación de documentación efectiva y balanceada.

Capítulo 3: Estado del Arte

3.1 Tendencias globales en ciberseguridad

En los últimos años, se ha producido un cambio de panorama global de ciber acciones. Consideraciones de referencia como el Digital Defense Report 2023 de Microsoft indican que los ataques cibernéticos se han vuelto más frecuentes, organizados y sofisticados. Además, están más orientados a sectores críticos y organizaciones cuyos presupuestos de ciberseguridad suelen ser limitados (Microsoft Security, 2023). De acuerdo con el informe ENISA Threat Landscape 2023, los ataques más usados son el phishing dirigido, ransomware y la explotación de vulnerabilidades en servicios web (ENISA, 2023).

Este nivel de sofisticación refleja una profunda mutación de los atacantes, que ha evolucionado de ser un simple un simple explorador tecnológico a convertirse en un ciberdelincuente. Esta nueva realidad a convertido a los hackers en actores capaces de decidir el destino de las economías o alterar el equilibrio geopolítico global con unas cuantas líneas de código (Castillo del Rio, 2025b).

3.2 Principales riesgos identificados

Las diez amenazas más críticas para las aplicaciones web son el control de acceso débil, los fallos criptográficos y los errores de diseño de seguridad, entre otros (OWASP, 2021). Las vulnerabilidades constituyen un vector de ataque crítico y refuerzan la necesidad de adoptar soluciones estructuradas como las que establece la norma ISO/IEC 27001:2022 (Parolin, 2022).

La historia reciente ha demostrado que estos riesgos no solo son teóricos. En 2007, Estonia sufrió una serie de ataques de denegación de servicio (DDoS) los cuales lograron paralizar sus sistemas gubernamentales y bancarios. Unos años mas tarde, en 2015, la red eléctrica de Ucrania fue saboteada por un ciberataque que provoco apagones masivos, y mas

recientemente, un ataque que fue dirigido al oleoducto Colonial Pipeline en 2021 el cual paralizo el suministro de combustible en Estados Unidos, subrayando el impacto directo que un ataque digital puede tener sobre la infraestructura critica de una nación (Castillo del Rio, 2025a).

Dejando de lado las vulnerabilidades técnicas, uno de los riesgos mas persistentes seguirá siendo la explotación del factor humano. La ingeniería social, definida como el arte de manipular la percepción para obtener acceso alguno, esto convierte al usuario en el eslabón mas débil de la cadena de seguridad en una guerra psicológica en donde la confianza y la rutina son las mayores vulnerabilidades (Castillo del Rio, 2025b).

3.3 Enfoques de gestión y mitigación

IBM y NIST han promovido marcos de gestión de la amenaza que incluyen desde la evaluación del perfil de amenazas de forma continua al monitoreo activo y a los planes de recuperación (IBM, 2024), (NIST, 2012). Muchos de estos marcos están diseñados para grandes empresas con capacidades técnicas avanzadas.

3.4 Dificultades de adopción en contextos de bajos recursos

Un importante hallazgo del estado del arte es que la mayoría de las herramientas, guías y recursos que existen para la implementación ISO 27001:2022 no están pensados para PYME o entidades con capacidades limitadas.

Los documentos normativos oficiales y guías especializadas suelen tener barreras de acceso como lenguaje técnico, estructuras complejas, o no tener versiones que se adapten al contexto latinoamericano. Este hecho representa una gran limitación para la democratización del estándar. Investigaciones anteriores lo confirman. Esto último porque la mayoría de las pymes

tiene problemas con el costo del consultor, falta de personal técnico y escasa disponibilidad de documentación práctica en su idioma (Valencia Duque y Orozco Alzate, 2017).

3.5 Necesidad de enfoques prácticos y accesibles

Las regulaciones deben evolucionar hacia metódicas más adaptativas con herramientas listas para usar, plantillas y procesos estandarizados, (Gartner, 2023; World Economic Forum, 2023). Esta visión respalda que se sigan desarrollando propuestas como la que está en sus manos, que busca transformar estándares complejos en pasos viables y documentados en escenarios reales.

Capítulo 4: Metodología de la Investigación

4.1 Planteamiento del problema

Las organizaciones deben proteger esta información y los datos de la organización contra ataques cibernéticos. Pero hay un importante reto de proteger los datos de las amenazas de rápido crecimiento. Ahora no se trata solo de ataques individuales, sino de redes estructuradas de cibercriminales que buscan acceder u obtener información confidencial. El informe mundial 2023 en ciberseguridad —2023— por el grupo Gartner realizó un estudio sobre ese tema, confirmando que los ataques son cada vez más sofisticados y complejos (Gartner, 2023). Asimismo, las aplicaciones web (que pueden tener problemas por malas prácticas o ignorancia) continúan siendo vulneradas (OWASP, 2021).

Aparte de esto, el impacto global del problema, así como el panorama global de amenazas, muestra igualmente preocupantes patrones de amenazas que más afectan a aquellas organizaciones que menos recursos de protección tienen (ENISA, 2023). De hecho, el prestigioso Informe de Investigaciones de Fugas de Datos de Verizon de 2024 confirma esta tendencia, revelando que el elemento humano estuvo involucrado en el 68% de todas las brechas de seguridad analizadas" (Verizon, 2024).

Aparentemente, su dificultad de la implementación está aumentando, a pesar de su creciente respuesta como herramienta regulatoria. Las complicaciones son más que evidentes.

- **Complejidad técnica:** Las exigencias normativas resultan un reto importante para las distintas entidades sin formación especializada. (Valencia Duque & Orozco Alzate, 2017)
- **Falta de manuales:** No hay guías que apliquen el control de lo que habla la norma en un contexto organizacional. (Valencia Duque & Orozco Alzate, 2017).

- **Dificultad de adaptación:** El primer problema hace referencia a que, interpretar y adaptar lineamientos genéricos a la realidad concreta, no resulta fácil (IBM, 2024).
- **Falta de mantenimiento continuo:** La ineficacia que ocurre por falta de cuidado permanente en el sistema (ISOTools, 2017), (NIST, 2012). Muchas entidades no tienen procedimientos para que el sistema no pierda su efectividad.

Las principales economías, como la mexicana, están constituidas en su mayor parte por pequeñas y medianas empresas (pymes); un reto será esto. La situación actual demanda más que simplemente documentar técnicamente. En efecto, es necesario crear metodologías que conviertan los requisitos que surgen de la norma ISO 27001 en algo más sencillo y flexible a cada contexto organizacional (Parolin, 2022).

4.2 Justificación

La norma ISO 27001 es cada vez más necesaria con el auge exponencial del ciberdelito, que se calcula que alcanzará los 10,5 billones de dólares anuales en 2025 (Cybersecurity Ventures, 2020). La seguridad de la información deja de ser una práctica correcta y se convierte en una exigencia estratégica de supervivencia de la organización.

A pesar de que algunas organizaciones ya cuentan con algunos controles contemplados en la norma, han conseguido mejoras parciales en su gestión de seguridad (Andrea, P., & López, E. A. 2011). La complejidad del estándar, la restricción presupuestaria y la falta de guías prácticas de referencia son los principales obstáculos. Estas limitaciones sitúan a las organizaciones, especialmente a las pequeñas y medianas empresas (PYMES), por debajo de la línea de **ciber pobreza**, un umbral conceptual que define el nivel mínimo de recursos que una organización necesita para defenderse de manera efectiva de las ciber amenazas (Microsoft Digital Defense Report, 2023).

El marco regulatorio intensifica esta necesidad. En nuestro país y en el ámbito internacional, como el Reglamento General de Protección de Datos (GDPR), se han hecho leyes que impondrán sanciones a delincuentes y las multas son elevadas (Microsoft Security, 2023).

Cumplir con estos requisitos es una ventaja competitiva, ya que un porcentaje significativo de clientes escoge a sus proveedores por competencia a padecer una pérdida de datos. Tener la certificación ISO 27001 trae beneficios comerciales tangibles. Según el Panorama de amenazas de ENISA 2023, el 90% de las empresas que han sufrido ciberataques no contaban con sistemas de ciberseguridad formales. (ENISA, 2023)

La complejidad del estándar, la restricción presupuestaria y la falta de guías prácticas de referencia. Son los principales obstáculos. Esta investigación aborda dichas limitaciones a través de

- Un análisis documental extendido y exhaustivo.
- Herramientas y plantillas reutilizables.
- Estrategias de costo y beneficio para pymes.
- Un plan para mejorar continuamente, aun en un entorno de pocos recursos.

El propósito es empoderar a la ISO 27001 para que cumpla con su objetivo: facilitar su adopción más allá de las grandes empresas y en beneficio del ecosistema nacional de ciberseguridad.

4.3 Objetivos

4.3.1 Objetivo general

El objetivo general de la investigación es la de generar una guía metodológica para la implementación de la norma ISO/IEC 27001:2022. (Parolin, 2022). Esta guía servirá de ayuda a

la adopción práctica de la norma por parte de las entidades mexicanas, fortaleciendo sus Sistemas de Gestión de Seguridad de la Información (SGSI).

4.3.2 Objetivos específicos

1. Analizar los requisitos de la norma ISO 27001 y los principales obstáculos de implementación en México.
2. Diseñar un método organizado por etapas para simplificar el proceso de implementación.
3. Desarrollar herramientas, plantillas y recursos adaptables a diferentes tipos de organizaciones.
4. Establecer criterios para la evaluación y gestión de riesgos ajustados al entorno nacional.
5. Proponer estrategias de aplicación económicas para pequeñas y medianas empresas.

4.4 Alcance y limitaciones

4.4.1 Alcance

La investigación abarca.

- Requisitos asociados a la norma ISO 27001 y su aplicación.
- Creación de un proceso desde la evaluación inicial hasta el mantenimiento del SGSI.
- Creación de instrumentos, plantillas y recursos listos para usar.
- Ejemplos de la vida real de diferentes organizaciones en México.
- Controles de gestión, financieros y operativos.

4.4.2 Limitaciones

- La guía es un recurso complementario; no debe ser utilizada en sustitución del texto, oficial de la norma.
- No se recomienda usar software de uso comercial.

- No se debe considerar como asesoría jurídica.
- No certifica metodológicamente y con garantía total.
- Requerirán adaptaciones adicionales dependiendo del tipo de industria.

4.5 Diseño metodológico

La investigación actual es de carácter aplicado, cualitativo, con un diseño documental y propositivo. Se fundamenta en la revisión, análisis y sistematización de fuentes normativas, técnicas y académicas sobre lo que es el Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO/IEC 27001:2022 (Parolin, 2022).

La norma ISO 27001 (Parolin, 2022), informes de organismos internacionales (ENISA, 2023), artículos de revisión académica como (Valencia Duque & Orozco Alzate, 2017), guías de buenas prácticas como (ISOTools, 2017) y la reciente tendencia de (Gartner 2023) sobre ciberseguridad.

El fin pretendido fue el de reestructurar el conocimiento existente en una guía metodológica práctica, al ciclo PDCA (ISO/IEC, 2022, cláusula 10.2), que permita facilitar la adopción de la norma en las organizaciones mexicanas, especialmente en las pequeñas y medianas empresas. La guía fue construida como una propuesta estructurada, con herramientas, recursos, y ejemplos listos para aplicar.

Capítulo 5: Metodología de Implementación de ISO/IEC 27001

Habiendo establecido la metodología de investigación y los fundamentos teóricos, el siguiente paso es detallar cómo implementar un SGSI siguiendo el ciclo PDCA (Planificar-Hacer-Verificar-Actuar), comenzando con la fase de planificación, que sienta las bases para un sistema robusto y alineado con los objetivos organizacionales (ISO/IEC, 2022, cláusula 10.2).

En este capítulo se presenta un modelo basado en la norma ISO/IEC 27001:2022. Un conjunto de marcos regulatorios, casos, sugerencias prácticas y herramientas de apoyo para las diferentes organizaciones, para diferentes épocas y distintos niveles de madurez (Parolin, 2022). Se pretende dotar de unas pautas claras, secuenciales y útiles para cualquier entorno organizacional que alineen la seguridad de la información a los lineamientos estratégicos de las organizaciones, protegiendo sus activos más preciados y cumpliendo la normativa, ley y contrato que toquen.

5.1 Fase de planificación

La etapa inicial que se precisa para la implementación de un SGSI es la planificación. Ello implica la elaboración del análisis de situación, donde se recopiló y seleccionó la información relevante. La correcta ejecución de esta actividad permite prever las necesidades de seguridad, establecer el alcance del sistema, definir las políticas reactivas y seleccionar las mejores metodologías para atender los riesgos. Los actores de la entidad intervinieron al principio, lo que a la vez empieza a sentar las bases para una aplicación eficaz y duradera.

5.1.1 Obtención del compromiso de la alta dirección

El compromiso de alta dirección se considera un factor crítico de éxito en un SGSI. La voluntad política de llevar a cabo unas acciones se tiene que expresar no solamente en palabras,

sino, en acciones concretas que tengan que ver con el liderazgo, la afluencia de recursos y la toma de decisiones. Entre los principales roles de los actores de alta dirección.

1. Aprobación de la política de seguridad de la información.
2. Distribución del dinero, tecnología y personas por actividades.
3. Creación de roles estratégicos como el responsable del SGSI.
4. Verifica periódicamente las capacidades del sistema.

La integración de la seguridad de la información a los objetivos estratégicos de las organizaciones. De concreto, el liderazgo debe contribuir al mejoramiento continuo y la toma de conciencia en los niveles de jerarquía. De acuerdo con estudios recientes, si la alta dirección supervisa el sistema de gestión de seguridad de la información (SGSI), habrá menos incidentes y se mejorará la respuesta a las nuevas amenazas (ISO/IEC, 2022; Valencia Duque & Orozco Alzate, 2017).

Este compromiso va mas allá de una simple supervisión; implica entender la ciberseguridad como un componente estratégico de la organización. Los lideres de alto nivel (C-Level) deben ser los arquitectos, la pieza mas importante de una organización resiliente, capaces de fomentar una cultura donde la seguridad sea vista como una ventaja competitiva y no solamente como una carga. La capacidad de respuesta ante un incidente emana directamente de este liderazgo (Castillo del Rio, 2025a).

5.1.2 Definición del alcance del SGSI

Cuando ya se ha definido el compromiso, se realiza la definición del alcance del SGSI. En esta fase se establece el alcance organizacional, físico, tecnológico y funcional donde se

implementará el sistema. El rango debe estar claramente documentado e incluir las siguientes dimensiones.

- Funciones organizacionales involucradas (producción, soporte, TI, recursos humanos, contable, etc.).
- Recursos tecnológicos como infraestructuras físicas y software crítico en la nube.
- Sitios físicos (sede, oficina, centro de cómputo).
- Proveedores y socios estratégicos.
- Requisitos legales, regulatorios y contractuales que apliquen.

Un alcance mal redactado puede dar lugar a la exclusión de activos importantes, así como a un exceso de controles innecesarios. En consecuencia, la norma plantea que se aplique un enfoque modular que permita comenzar por las de mayor impacto y ampliarse con el tiempo (Parolin, 2022). Una manera de tener efectos inmediatos que juega a favor de la aceptación interna.

5.1.3 Establecimiento de la política de seguridad de la información

La política de seguridad de la información es el documento que define la visión, los objetivos y las directrices generales del SGSI. Debe contar con la autorización de la alta dirección y su difusión debe ser clara para todos los miembros de la organización. Una política efectiva debe contener.

- Compromiso institucional con la seguridad.
- Principios maestros y objetivos de alto nivel
- Relación con otras políticas internas.
- Mandatos generales de los trabajadores.

- Regularidad de verificación y encargado de su actualización.

También debe tener un lenguaje que pueda ser entendido por todos los públicos (INCIBE, 2021).

5.1.4 Metodología de evaluación de riesgos

La identificación, evaluación y tratamiento de riesgos es uno de los fundamentos de un SGSI. Es necesario definir una metodología de análisis que permita evaluar las amenazas y vulnerabilidades, valorar los activos y priorizar los riesgos según su criticidad. Esta metodología debe considerar.

- Criterios para valorar el impacto y la probabilidad de ocurrencia.
- Umbrales para determinar si el riesgo es aceptable o no
- Identificación de activos y categoría de estos.
- Identificar los riesgos y debilidades.
- Numérico, valorativo o puede ser mixto.

En función del sector, tamaño y recursos de la organización, se elegirá la metodología. En la siguiente tabla se comparan algunos enfoques comunes.

Tabla 5.1: Comparativa de metodologías de análisis de riesgos

Metodología	**Enfoque**	**Aplicabilidad**
ISO/IEC 27005	Mixto(valorativo/numérico)	Compatible con ISO 27001.
NIST SP 800-30	Valorativo	Recomendado para el sector público.
MAGERIT	Numérico	Usado por administraciones públicas.
OCTAVE	Valorativo	Ideal para organizaciones medianas.

Elaboración propia a partir de Estudio comparado de metodologías de análisis de riesgos para TI y Seguridad de la Información (Versión 01) (AGESIC, 2021).

5.1.5 Identificación de activos, amenazas y vulnerabilidades

El procedimiento del análisis de riesgos se inicia con la identificación de activos. Los activos primarios para tener en cuenta son la información, los procesos de negocio y los servicios críticos. Y los activos de soporte son la infraestructura, la red, el personal y las aplicaciones. Todo activo debe ser documentado, valorado y clasificado según su sensibilidad.

Luego se identifican las amenazas (naturales, técnicas, humanas, organizacionales) y las vulnerabilidades que pueden ser aprovechadas por ellas. Se llevan a cabo entrevistas, análisis de documentos, pruebas técnicas y revisiones de incidentes.

Se sugiere realizar una matriz de relación activa-amenaza-vulnerabilidad que permita identificar las relaciones más críticas para preparar estrategias de mitigación. Como se muestra en la Figura 5, este tipo de matriz facilita la visualización y priorización de riesgos al ilustrar la conexión entre activos, amenazas y vulnerabilidades. OWASP y ENISA ofrecen catálogos actualizados que pueden ser utilizados de referencia (ENISA, 2023), (OWASP, 2021).

Riesgo	Probabilidad	Impacto	Mitigación
Fraude Interno	Media	Alto	Auditorías internas, implementación de software de monitoreo
Fluctuaciones del mercado	Alta	Alto	Diversificación de inversiones, análisis de mercado continuo
Fallos tecnológicos	Baja	Alto	Actualizaciones constantes de software, copias de seguridad diarias.

Figura 5: Ejemplo de matriz de riesgos en el sector financiero. Matriz de riesgos: qué es, ejemplos y cómo crearla fácil (Pirani, 2022).

5.1.6 Desarrollo del plan de tratamiento de riesgos

Con base en los resultados del análisis de riesgo, se elabora un plan de tratamiento que define el modo de abordar los riesgos identificados. Este plan debe especificar.

- Identificación y evaluación de riesgos priorizados.
- Seleccionar la acción para el proyecto (mitigar, evitar, transferir o aceptar).
- Controles escogidos (del Anexo A de ISO/IEC 27001:2022).
- Señalizar los recursos y responsables asignados.
- Un calendario y sistema para medir la eficacia.

La forma en que se debe seleccionar la defensa en profundidad de los controles: un conjunto de medidas que son técnicas, organizacionales y físicas. Todas las decisiones sobre la aceptación de riesgos requerirán la aprobación explícita de la dirección. Igualmente, el proceso será documentado y auditable (Parolin, 2022); (Pérez, 2025).

5.2 Fase de implementación

Esta fase traduce los hechos y elementos en acciones. Mediante la puesta en marcha, se inician el control, las políticas, los recursos y los sistemas documentales previamente planificados, para que todo el marco del SGSI funcione conforme a los requerimientos establecidos. Esta etapa requiere coordinación, liderazgo técnico, capacidades de gestión del cambio y una comunicación que facilite la aceptación organizacional.

5.2.1 Elaboración de la Declaración de Aplicabilidad (SoA)

La SoA o Declaración de Aplicabilidad correspondiente es uno de los documentos clave requeridos como parte de la ISO/IEC 27001. Él identifica los controles del Anexo A seleccionados y su aplicabilidad y, además, indica cuáles están en implementación, cuáles están

relacionados con procedimientos existentes y su justificación. Su valor está en dar cuerpo a la estrategia de seguridad de forma concreta y operativa, así como en facilitar la auditoría, seguimiento interno y cumplimiento.

Es aconsejable hacerla por fases muy marcadas. Primera fase: revisión y análisis de controles del Anexo A. Segunda fase: decisión sobre su aplicabilidad en función de la situación. Tercera fase, documentación de las justificaciones. Cuarta fase, asignación de responsables. Y última fase, aprobación. La SoA debe mantenerse como un documento esencial y revisado periódicamente a través de análisis de riesgos o cambios organizacionales (Kruiskamp, 2025), (*ISO 27001: Controles Y Cómo Implementarlos Correctamente*, n.d.)

Lo recomendable es combinarla con herramientas de gestión de cumplimiento tipo GRC o plataformas documentales con control de versiones. Esto hace menos complicado su seguimiento y consulta para auditores y partes interesadas.

5.2.2 Desarrollo de la estructura documental

La documentación es el esqueleto del SGSI. Los controles no tienen una guía útil para su operación sin una organización bien definida. El desarrollo documental establece políticas, procedimientos, instructivos, registros y formularios a fin de homogeneizar el comportamiento de la organización en torno a la seguridad de la información.

Cada documento debe cumplir criterios de claridad, vigencia, aprobación, control de versiones y accesibilidad. Lo mejor es que haya una política de gestión documental. Esto establece responsables, frecuencias y condiciones de acceso. Así mismo, habrá que utilizar formatos estandarizados y similares

.

Ejemplo de jerarquía documental.

- Nivel 1: Políticas institucionales.
- Nivel 2: Procedimientos operativos.
- Nivel 3: Instrucciones técnicas y listas de verificación.
- Nivel 4: Formularios y registros que sirven de evidencia de cumplir.

La automatización de tareas de revisión, alertas de vencimiento y control de cambios por parte de un DMS (Sistemas de gestión de documentos) (NQA, 2023).

5.2.3 Implementación de controles seleccionados

Los controles deben implementarse teniendo en cuenta su dependencia con otros procesos y las implicaciones en la operación. La ejecución no debe ser simultánea de todos los controles, sino a través de un cronograma progresivo y validado.

Se recomienda aplicar fases como:

1. Detalles de cada control, incluyendo su descripción e intención, y requerimientos técnicos y operativos.
2. Pruebas piloto en áreas controladas para detectar impactos no previstos.
3. Evaluación de resultados y ajustes.
4. Despliegue progresivo por áreas funcionales.

Los controles técnicos como firewalls, autenticación de múltiples factores o cifrado de datos requieren que haya un especialista detrás. Y los controles administrativos, como una política o un procedimiento, requieren formación y gestión del cambio. En todos los casos es imprescindible documentar los resultados y retroalimentarlos para su mejora continua.

5.2.4 Gestión de recursos y competencias

La capacidad de las personas responsables implica que se implementen acciones. Por ello, la norma ISO 27001 exige que se identifiquen, proporcionen y evalúen los recursos necesarios.

Eso quiere decir que se definen los perfiles de esos roles clave (el oficial de seguridad, analista de riesgos, auditores internos), se mapean las competencias requeridas para cada uno y se diseña un plan de formación continua. La evaluación de competencias puede hacerse mediante examen, simulación, participación en incidentes y seguimiento.

Los recursos incluyen también los sistemas tecnológicos, las herramientas de gestión, el tiempo que se destina para desarrollar tareas del SGSI, el presupuesto para las auditorías y la formación y el apoyo organizacional que recibe de la alta dirección. Sin ellos, el sistema puede llegar a implementarse formalmente, pero no tener efectividad operativa. (Parolin, 2022).

5.2.5 Plan de comunicación y concientización

Debe existir una concientización y capacitación en seguridad de la información para establecer una cultura organizacional que contemple la protección de la información y el cumplimiento de las políticas del SGSI. El plan de comunicación ha de estructurarse en función de los públicos objetivos y mensajes diferenciados.

Elementos del plan.

- Objetivos de concientización.
- Audiencia (dirección, usuarios, TI, proveedores).
- Métodos como correos y vídeos internos.

- Frecuencia de las campañas.
- Medición de impacto (evaluaciones, cambios de comportamiento, incidentes reportados).

El programa va desde un boletín mensual hasta simulaciones de ataque y talleres prácticos (simulación de phishing). También deberían contemplarse las opiniones de los usuarios, mejoras sucesivas y visible apoyo institucional para mayor eficacia Instituto (INCIBE, 2021).

5.3 Fase de operación

La finalidad de la fase de operación es garantizar que las actividades y controles del SGSI que fueron definidos e implementados durante la fase de planificación se ejecuten efectivamente y de forma sostenible. Esta etapa representa el paso del diseño teórico a la práctica diaria; es decir, los procedimientos se integran a la cultura organizacional. El SGSI debe contar con un control permanente, con responsabilidades bien definidas, con documentación actualizada, con análisis de los resultados y con reacciones al desvío.

5.3.1 Operación conforme a procedimientos

Es momento de asegurarse de que los controles y la documentación se implementarán de manera orgánica en las actividades diarias. Esto se logra mediante.

- Definición de responsables por procesos y controles.
- Integrar los procedimientos en los flujos de trabajo normales.
- La formación permanente del personal que interviene.
- Supervisión permanente de tareas críticas.

Por ejemplo, todo proceso de gestión de cambios debe incluir una validación previa de seguridad cuando el cambio afecte infraestructura crítica o datos sensibles; de esta forma se evita introducir vulnerabilidades y se garantiza la continuidad operativa.

La integración puede realizarse con herramientas colaborativas, cheques de operaciones, mecanismos de validación automática (SIEM y DLP) y supervisión a través de KPI o dashboards de seguridad. El SGSI no debe ser un sistema paralelo en el que se carguen los arquitectos de negocio, sino ser parte del negocio, para evitar sobrecargas (NQA, 2023).

5.3.2 Gestión de incidentes de seguridad

La gestión de incidentes es uno de los procesos más visibles del SGSI, constituye una de las pruebas clave de eficacia. La norma ISO/IEC 27001 exige procedimientos documentales (Parolin, 2022).

1. Para la realización de los incidentes, deben prepararse en la programación informática, además de los útiles.
2. Identificación mediante alertas a medidos, monitoreos, reportes y/o terceros.
3. Aislamiento de sistemas para evitar su propagación.
4. Erradicación, eliminar de raíz la causa del incidente".
5. Recuperar los sistemas y datos impactados.
6. Revisar las causas y los controles fallidos para mejorar, de forma continua.

Los incidentes son sucesos que ocurren inesperadamente y que interrumpen la correcta operación de un sistema y que, como consecuencia, deben quedar debidamente registrados. para que un incidente se considere como tal se requiere la intervención de expertos para que el sistema o las operaciones puedan volver a su estado de normalidad. el incidente no debe ser

confundido con fallo, el cual es la causa. los informes de incidente deben incluir la fecha y la hora, la duración, los sistemas involucrados, el impacto que se haya podido producir, las acciones que se han realizado, las medidas quiénes han sido los responsables y las que se piensan poner en técnicas para el futuro. Las herramientas como SIEM, SOC o SOAR facilitan y mejoran los tiempos de respuesta en este proceso.

5.3.3 Control de documentos y registros

Se generan un gran número de documentos y registros en un SGSI que requieren un control que garantice la integridad, trazabilidad y disponibilidad de estos. ISO/IEC 27001 establece que todo documento debe.

- Identificados, versionados y aprobados por responsables.
- Ayudar a la gente disponible cuando te necesite.
- Debe ser revisado y actualizado con frecuencia.
- Proteger contra pérdida, acceso no autorizado y deterioro.

Los registros son evidencias del cumplimiento de actividades de acuerdo con el SGSI, y pueden tener los siguientes.

- Resultados de auditorías.
- Registros de incidentes.
- Informes de formación.
- Registros de acceso y actividades.

El uso de herramientas digitales para gestión documental como SharePoint, Confluence, Google Workspace o Alfresco e incluso DMS específicos, mejora el control, el cumplimiento normativo y la eficiencia operativa. (NQA, 2023)

5.4 Fase de Monitoreo y Mejora Continua

La fase de monitoreo y mejora continua es el elemento que permite asegurar la sostenibilidad del SGSI en el tiempo. Hay que asegurar que el sistema se mantenga al día ante un mundo cambiante, supervisar la eficacia de los controles, detectar desviaciones, aprender de los incidentes y crear retroalimentación. Esta fase corresponde a la etapa “Verificar” y “Actuar” del modelo PDCA (planificar, hacer, verificar y actuar) (ISO/IEC, 2022, cláusula 10.2). Es fundamental para la continuidad del negocio (BCP) y la organización y resiliencia de la organización ante nuevas amenazas o modificaciones en los objetivos del negocio.

5.4.1 Medición de la efectividad de controles

La medición objetiva mide si los controles se ejecutan como se tenía previsto. Debemos definir métricas que sean cuantificables, específicas y relevantes para cada control implantado. Estas métricas pueden incluir.

- Porcentaje de políticas de cumplimiento de acceso.
- Tiempo medio de detección y respuesta ante incidentes.
- Cantidad de fallas críticas resueltas.
- Usuarios capacitados en seguridad porcentaje.

El análisis de estos indicadores se puede realizar mediante dashboards, SIEM o plataformas GRC. Es importante que los resultados se interpreten en un contexto, ya sea interno o externo, metas establecidas y tendencias históricas (Initialize, 2023). Al realizar un monitoreo que se realiza mediante automatización, se logra minimizar el error humano y se acelera el análisis, lo que permite respuestas más proactivas.

5.4.2 Auditorías internas

Las auditorías internas permiten revisar sistemáticamente la conformidad y eficacia del SGSI. Deben ser realizadas por personal competente e independiente de los procesos auditados, con un enfoque basado en riesgos que contemple un programa anual fijado en función de las prioridades del negocio. Las auditorías deben contemplar.

- Revisar documentos ya sea un procedimiento o un registro.
- Charlas con los directivos y los operarios.
- Observación directa de procesos.
- Tests de cumplimiento y efectividad.

Los hallazgos se separan en no conformidades mayores, menores, observaciones y oportunidades de mejora. Cada hallazgo debe estar soportado por una evidencia y ligar a un plan de acción correctiva con plazos. La retroalimentación de las auditorías constituye un elemento clave en la mejora continua y la preparación para auditorías externas de certificación (Lucena, 2024).

5.4.3 Revisión por la dirección

La evaluación que lleva a cabo la Alta Dirección permite comprobar que el SGSI mantiene su adecuación, su eficacia y su alineación respecto a los objetivos del negocio. Esta revisión debe hacerse por lo menos una vez al año, e incluir.

- Fruto de auditorías internas y externas.
- Cumplir las metas de seguridad definidas.
- Alcanzar las propuestas de objetivos de seguridad.
- Retroalimentación de partes interesadas.

- Estado de acciones correctivas.
- Cambios al interior y exterior que impactan el SGSI.
- Sugerencias de mejora y decisiones estratégicas.

La reunión debe estar documentada y los acuerdos que se tomen deben ser implementados dentro del proceso de mejora. Este ejercicio refuerza el liderazgo de la empresa y propicia la visión del SGSI como parte del modelo de gestión integral (Parolin, 2022), (Drmunozcl, 2025).

5.4.4 Acciones correctivas y mejora continua

El SGSI debe ser capaz de aprender de sus errores. Acciones que se toman para eliminar la causa de la no conformidad detectada en una auditoría, en un incidente o en un monitoreo, para que no se repita.

El proceso para su gestión incluye:

- Identificar el problema y su causa raíz.
- Valoración del impacto y urgencia.
- Propuesta de medidas correctivas.
- Implementación y documentación.
- Verificación de efectividad.

La mejora continua es la aplicación sistemática de análisis de tendencia, ‘benchmarking’, lecciones aprendidas y oportunidades tecnológicas para mejorar progresivamente la seguridad en la organización. Los modelos como el ciclo PDCA, Six Sigma o Kaizen pueden adaptarse como metodologías compatibles (ISO/IEC, 2022, cláusula 10.2).

5.4.5 Evaluación continua del SGSI

Hay que evaluar la madurez de la SGSI como un sistema global, mayormente en relación con los fallos, su control y su corrección (véase la Figura 6). Es recomendable valorar los procesos mediante una escala de cinco niveles.

- Nivel Inicial – Prácticas ad-hoc y reactivas.
- Nivel Repetible - Para que el proceso se considere 'nivel repetible' los procedimientos básicos del proceso se encuentran documentados, aunque todavía existe dependencias a personas.
- Nivel Definido – Procesos formalizados, normalizados y comunicados en toda la organización.
- Nivel gestionado— Métricas e indicadores permite controlar y ajustar los procesos.
- Nivel de optimización - La mejora continua con retroalimentación y análisis de tendencias se designa como nivel de optimización.

Esta evaluación holística debe abarcar.

- El SGSI brinda soporte a los objetivos de negocio
- ¿Se están manejando los riesgos importantes?
- Se cumplen las metas de seguridad.
- Utilizan los recursos de forma óptima - Eficiencia
- ¿El sistema se adapta a los cambios en sostenibilidad?

Tal como se ilustra en la Figura 6, estas dimensiones se representan gráficamente mediante los cinco niveles de madurez del SGSI.

Herramientas prácticas para esta finalidad los modelos de madurez como CMMI, COOBIT e ISOTools, o bien, una evaluación ad hoc con la anterior escala. El SGSI puede medir su ROI en la reducción de incidentes, cumplimiento normativo, confianza del cliente y eficiencia operativa (*Niveles De Madurez De La Capacidad En La Evaluación De Riesgos - FasterCapital*, n.d.)

Figura 6: Los cinco niveles de madurez de la capacidad en la evaluación de riesgos. Adaptado *de* Niveles de madurez de la capacidad en la evaluación de riesgos (Niveles De Madurez De La Capacidad En La Evaluación De Riesgos - FasterCapital, n.d.).

Termina el ciclo, mejora continua que da a la organización capacidad de adaptación a amenazas emergentes, nuevas tecnologías y requisitos normativos en evolución**.**

Capítulo 6: Propuesta de Guía y Recursos para la Implementación de ISO/IEC 27001:2022

Con base en la norma ISO/IEC 27001:2022 se detalla en este capítulo el enfoque de desarrollo del SGSI, bajo el ciclo PHVA (planificar-hacer-verificar-actuar). Se busca dotar a la organización de un manual práctico, ordenado y coherente que facilite el cumplimiento de los requisitos normativos y que además fortalezca su capacidad de respuesta ante riesgos y amenazas emergentes (Parolin, 2022).

6.1 Fase 1 — Análisis de riesgos

6.1.1 Enfoque metodológico detallado

El análisis de riesgos es fundamental para el correcto funcionamiento del SGSI De acuerdo con ISO/IEC 27001:2022, este proceso tiene como objetivos identificar, evaluar y priorizar riesgos que afectan a la información, para tomar decisiones razonadas sobre los controles a implementar (Parolin, 2022).

El proceso comienza por identificar y clasificar cada activo. Es recomendable distinguir entre.

Activos primarios: información crítica, procesos y servicios que son esenciales para la misión de la organización.

Activos de soporte: los recursos que permiten operar esos activos primarios, incluyendo infraestructura tecnológica, aplicaciones, personal y proveedores.

Cada activo hay que registrarlo con datos clave, que son: responsable al que se le asigna, ubicación física o lógica, valor que tiene, y por última clasificación CIA: confidencialidad, integridad, disponibilidad. Esta clasificación hace fácil ver la importancia que tienen en los procesos de la organización, así como la priorización de su protección (Lucena, 2024).

El segundo paso es la identificación de amenazas. Es recomendable apoyarse en marcos de referencia consolidados, como lo menciona el informe Threat Landscape de ENISA (ENISA, 2023), o el OWASP Top 10 (OWASP, 2021). Las amenazas pueden ser técnicas (como un ataque de programa maligno “malware” o un ataque por explotación de vulnerabilidades), humanas (un error del personal que provoca una fuga o ingeniería social) u organizativas (por ejemplo, falta de políticas, procesos inadecuados).

La tercera actividad consiste en identificar las vulnerabilidades que pueden ser de tipo técnico, organizativo o humano. Las vulnerabilidades técnicas son sistemas obsoletos, configuraciones inseguras, etc. Las vulnerabilidades organizativas son la no existencia de procedimientos claros. Las vulnerabilidades humanas son aquellos que no están concienciados en la seguridad. Se utilizan CIS Benchmarks, los resultados de las pruebas de penetración y vulnerabilidades clasificadas de acuerdo con sus CVSS v4.0 (IBM, 2024) para detectarlas.

Cuando se valora los riesgos se califica cada riesgo con base en su impacto y probabilidad. El impacto incluye los efectos económicos, legales y de reputación de un incidente. Una estimación económica se calcula mediante la multiplicación del valor del activo por un porcentaje de afectación. La probabilidad se refiere a la frecuencia esperada y a la vulnerabilidad del activo frente a la amenaza. Finalmente, el nivel de riesgo se calcula multiplicando impacto por probabilidad, y se expresa en una matriz de riesgos que permite la priorización visual (ISOTools, 2017).

Categorización de riesgos por criterios de aceptación. Por ejemplo.

- **Riesgos bajos** que no necesitan más protección.
- **Riesgos medios** requieren mitigación o transferencia.

- **Los riesgos altos** exigen tratamientos o respuestas inmediatas.

La elección de controles y la guía para la estrategia de seguridad de la organización se derivan de este análisis.

6.1.2 Indicadores de Riesgo Clave (KRI)

La gestión de riesgos requiere mecanismos de medición y seguimiento continuo. Algunos ejemplos de indicadores clave son:

- La proporción de riesgos críticos que carecen de un plan de tratamiento aprobado.
- El porcentaje de riesgos revisados en los últimos períodos de evaluación.
- La evolución del número total de riesgos por categoría (técnicos, humanos, organizativos).

Estos indicadores deben revisarse con periodicidad definida (mensual, trimestral o semestral, según criticidad) y documentarse en los informes del SGSI (Vivas, 2025).

6.1.3 Clasificación de Información según su Criticidad

La clasificación de la información depende de su nivel de criticidad, es un paso fundamental en la gestión de riesgos dentro de un sistema de gestión de seguridad de la información (SGSI), ya que esto permite que los recursos y controles para proteger los activos se prioricen y sean mas sensibles para la organización. Según la norma ISO/IEC 27001:2022, las organizaciones deben identificar y deben clasificar sus activos de información esto para garantizar su confidencialidad, integridad y disponibilidad (Parolin, 2022). Alienado este proceso con el Anexo A, asegura que los datos se gestionen dependiendo su importancia estratégica y los riesgos que estos asocian.

6.1.4 Proceso de Clasificación de Información

La clasificación de información tiene que basarse en su impacto potencial en la organización en caso de que se vea comprometida. La guía propone un enfoque en tres niveles de criticidad, esto adaptado a un contexto aplicable a organizaciones de todos los tamaños, especialmente PYMES:

1. Confidencial: La información cuyo acceso no autorizado, modificación o su indisponibilidad puede causar un impacto grave en las diferentes operaciones, finanzas o la reputación de la organización. Estos ejemplos incluyen datos financieros, información de clientes, propiedad intelectual o secretos comerciales.
2. Interna: La información destinada al uso interno de la organización, cuya exposición esta limitada la cual no representa un riesgo crítico, pero estos requieren protección para evitar las interrupciones operativas. Estos ejemplos incluyen documentos de procesos internos, correos electrónicos corporativos o planes operativos.
3. Publica: La información la cual no requiere restricciones de acceso y la cual su distribución o divulgación no afecta a la organización. Estos ejemplos incluyen materiales promocionales o alguna información en sitios web públicos o comunicados oficiales.

6.1.5 Buenas prácticas recomendadas

Para garantizar que el análisis de riesgos sea completo y efectivo, se recomienda:

1. Mantener un inventario de activos actualizado y validado con las áreas responsables.

2. Realizar talleres participativos donde se revisen amenazas y vulnerabilidades de forma colaborativa.
3. Documentar con evidencias técnicas cada vulnerabilidad detectada.
4. Revaluar riesgos después de incidentes relevantes o cambios tecnológicos.
5. Alinear la clasificación de riesgos con el apetito de riesgo y los objetivos de la organización.

Estas prácticas refuerzan la fiabilidad del análisis y permiten que las decisiones de seguridad sean proporcionales a los riesgos identificados (Instituto Nacional de Ciberseguridad (INCIBE, 2021).

6.2 Fase 2 — Establecimiento del alcance.

6.2.1 Proceso detallado.

El alcance del SGSI pregunta qué estará sujeto a su gestión. Define los límites, activos y procesos, a ser gestionados. De acuerdo con la norma ISO/IEC 27001:2022, dicho alcance debe encontrarse documentado y ser un fiel reflejo del funcionamiento de la organización y de los intereses de las partes interesadas (Parolin, 2022).

El proceso se desarrolla en varias etapas.

1. **Análisis del contexto**: Se realiza con técnicas como PESTEL. Con esto podemos ver que hay elementos políticos, económicos, sociales, tecnológicos, ambientales y jurídicos que afectan la seguridad de la información.
2. **Modelado preliminar:** Herramientas como los diagramas SIPOC ayudan a representar el flujo de información y los actores involucrados en los críticos.

3. **Comprobación:** El alcance preliminar, que permite comprobar que esté incluida toda la propiedad de los activos con alto riesgo según el análisis de riesgo.
4. **Inclusiones y exclusiones:** Todo elemento excluido debe estar debidamente justificado y documentado, basado en los criterios de evaluación del riesgo y el convenio de servicio.
5. **Aprobación formal:** La alta dirección documenta y aprueba el alcance, asegurando compromiso y alineación estratégica.

6.2.2 Ejemplos de métodos de alcance.

El tamaño, la estructura o la estrategia de una organización pueden definir su alcance.

- El sistema toma como base la totalidad de la organización gubernamental desde sus inicios. Esto es recomendable en pymes.
- Distribuido enfoque: Se refiere a que cada una de las sedes geográficas o unidades de negocios define un alcance.
- El sistema se desarrolla por módulos y se implantan siguiendo un cierto orden de prioridades (módulos).

Cada aproximación debe elegirse de forma intencionada y documentada (Kruiskamp, 2025).

6.2.3 Indicadores de efectividad.

Evaluando la pertinencia del alcance definido y sus por qué.

- Porcentaje de procesos clave cubiertos.
- Justificaciones y exclusiones aprobadas.
- Evolución de las revisiones de alcance a partir de incidentes o cambios organizativos.

El SGSI debe contar con un alcance bien definido y acorde con los objetivos de seguridad (INCIBE, 2021).

6.3 Fase 3 — Creación de políticas y procedimientos.

6.3.1 Estructura documental del SGSI.

La documentación del SGSI define de forma formal, líneas de referencia, procesos y controles. De acuerdo con ISO/IEC 27001:2022, debe haber un control y trazabilidad de este (Parolin, 2022).

- Nivel 0: Manual y política general del SGSI
- Nivel 1: Políticas temáticas (acceso, criptografía, dispositivos móviles).
- Nivel 2: Procedimientos Operativos Estandarizados.
- Nivel 3: Descripciones de trabajos y guías detalladas”
- Nivel 4: Evidencias como logs, actas y auditorías.

Una estructura para mantener la documentación consistente y actualizada (NQA, 2023).

6.3.2 Ciclo de vida documental.

El manejo de los documentos necesita un ciclo formal que contemple.

- Redacción inicial.
- Revisión técnica y legal.
- Aprobación por responsables.
- Publicación y difusión controlada.
- Control de versiones.
- Archivo histórico.

Así se aseguran de que todos los documentos sean pertinentes, accesibles y actualizados (INCIBE, 2021).

6.3.3 Ejemplo de Directiva Política.

Por dar algunos ejemplos, una política de clasificación de la información puede incluir.

- **Clasificación:** Publico, Interno, Confidencial, Secreto
- **Requisitos:** Es la información que se clasifica y debe de encriptarse con AES-256 y TLS 1.3 para garantizar la confidencialidad y la integridad de los datos, validada por el equipo de seguridad.
- **Responsabilidades:** El equipo encargado de la seguridad de la información debe verificar el cumplimiento.

6.3.4 Medición de madurez documental.

Para evaluar el grado de formalización documental se recomienda medir.

- La proporción de documentos sin responsable asignado.
- El tiempo que se tarda en revisión y aprobación.
- La organización demuestra su compromiso y capacidad de respuesta a través de las métricas del Anexo A.

En resumen, estas estadísticas son muy importantes (Parolin, 2022).

6.4 Fase 4 — Implementación de controles.

6.4.1 Selección y priorización.

Los controles por seleccionar se determinarán en función del análisis de los riesgos y de los objetivos de mitigación. Es importante que se plasme la forma en que se manejan los riesgos y los controles que se aplican para evitarlos, reducirlos, transferirlos o aceptarlos.

Una estrategia de defensa en profundidad incluye.

- Controles preventivos: autenticación multifactorial, cifrado.
- Sistemas de identificación: Sistemas de detección de intrusos.
- Controles de respuesta: plan de respuesta a incidentes.

6.4.2 Implementación escalonada y validación.

Para evitar impactos de las técnicas, se implantará en fases

1. Pruebas piloto en entornos controlados.
2. Validación de funcionalidad.
3. Capacitación del personal.
4. Documentación detallada.
5. Despliegue completo.

El control debe ser evaluado en cada caso para verificar su eficiencia y su compatibilidad. (Grupo Atlas, 2023)

6.4.3 Tipos de controles.

Los controles pueden ser.

- Tecnológicos: Firewalls, cifrado, gestión de parches, RBAC (Control basado en roles).
- Físicos: Cerraduras electrónicas, CCTV, zonas restringidas.
- Administrativos: Políticas, cláusulas, formaciones.

Al juntar estos métodos, se refuerzan las capas de protección (*ISO 27001: Controles Y Cómo Implementarlos Correctamente*, n.d.).

6.4.4 Seguimiento de efectividad.

Se recomienda monitorizar indicadores como

- Fallas de controles y tasas de incidencia.
- Indicador de cumplimiento de políticas.
- Porcentaje de sistemas actualizados.

El monitoreo continuo permite ajustar las acciones según las necesidades de la entidad (Initialize, 2023).

6.5 Fase 5 — Gestión de incidencias de seguridad.

6.5.1 Flujo de respuesta estructurado.

La gestión de incidentes es una función que formaliza las acciones a seguir ante cualquier ataque que compromete la confidencialidad, integridad o disponibilidad de la información. El flujo de respuesta se debe basar en un ciclo de ISO/IEC 27035-1 (Parolin, 2022).

1. **Detección y reporte inicial:** Cualquiera puede dar aviso. Lo puede hacer cualquier persona o sistema.
2. **Clasificación:** La evaluación del incidente y el daño que causa.
3. **Contención inmediata:** Acciones que detienen la expansión rápidamente.
4. **Erradicación:** La eliminación de causas, como programa maligno “malware” o la intrusión de personas no autorizadas.
5. **Recuperación:** Restablecimiento de sistemas y servicios.
6. **Cierre y lecciones aprendidas:** Reevaluación posterior y actualización de controles.

Este enfoque sistemático permite reaccionar rápidamente y tener un registro de cada una de las etapas del proceso.

6.5.2 Clasificación del nivel de gravedad y tiempo de respuesta

Con el fin de poder decidir mejor, se sugiere clasificar los incidentes en cuatro niveles de gravedad.

- Crítico: Afecta información sensible o interrumpe servicios esenciales. Tiempo máximo de respuesta: 30 minutos, aproximado.
- Alto: Degrada servicios clave, pero no interrumpe totalmente. Tiempo máximo: 2 horas, aproximado.
- Medio: Impacto limitado o parcial. Tiempo máximo: 4 horas, aproximado.
- Bajo: Impacto menor o potencial. Tiempo máximo: 8 horas, aproximado.

Los niveles de servicio son acordados, formalmente, en los SLA, que luego deben ser medidos periódicamente (*ISO 27001: Controles Y Cómo Implementarlos Correctamente*, n.d.).

6.5.3 Registro estructurado de incidentes.

Cada incidente debe ser documentado en detalle.

- Fecha y hora en que se dio la detección
- Vía de reporte (usuario, SIEM, proveedor).
- Descripción del evento.
- Clasificación de severidad.
- Activos comprometidos.
- Acciones de evitar, eliminar y recuperar.
- Responsable de seguimiento.
- Costo estimado del impacto.
- Estado final.

Esta auditoría se basa en el feedback de los empleados (NQA, 2023).

6.5.4 Buenas prácticas post-incidentales.

La gestión eficaz no termina con la resolución técnica. Es necesario.

- Hacer revisión después de incidentes de seguridad.
- Encontrar el origen del problema y sus debilidades.
- Crear estrategias de acción preventiva y correctiva.
- Realizar ajustes tecnológicos y formativos.
- Transmita la información aprendida para prevenir rechazos.

Estas prácticas refuerzan en toda la organización una cultura de seguridad. (Drmunozcl, 2025).

6.5.5 Integración con mejora continua.

Cada incidente constituye una oportunidad de mejora. Su análisis debe retroalimentar.

- El ciclo PDCA del SGSI (fase Actuar) (Parolin, 2022)
- Las políticas y procedimientos se van actualizando.
- La revisión de los riesgos y los controles
- La sensibilización del personal.

El orden de las lecciones fortalece la resiliencia ante amenazas cada vez más complejas.

6.6 Fase 6 – Auditorías internas y mejora continua.

Planificación y ejecución de auditorías.

La auditoría interna revisa el funcionamiento del SGSI y su conformidad con los requisitos de la norma. El proceso comprende.

- **Planificación:** Anual y objetivos del programa, criterios, alcance, responsables y métodos.
- **Preparación:** Se debe revisar documentos, políticas, evidencias.
- **Ejecución:** Entrevistas, observación de operaciones y recolección de evidencias objetivas.
- Clasificación de hallazgos:
    - **No conformidades mayores:** Incumplimientos significativos.
    - **No conformidades menores:** Desviaciones puntuales.
    - **Observaciones:** Aspectos detectados sin incumplimiento.
    - **Oportunidades de mejora:** Recomendaciones proactivas.
- **Documentación de resultados:** cada hallazgo debe vincularse a acciones correctivas específicas.

Gracias a la auditoría se puede ver las desviaciones y fortalecer la gestión (Lucena, 2024).

6.6.1 Revisión por la dirección.

La dirección tiene que revisar el desempeño del SGSI durante el tiempo.

- Resultados de auditorías internas y externas
- Índice de logro de los objetivos de seguridad.
- Estado de acciones correctivas.
- Cambios en el entorno que impactan en el SGSI y sus componentes.

Se debe documentar las conclusiones y servir de base para la formulación de decisiones estratégicas, la reapertura de recursos y el ajuste del enfoque del sistema (Parolin, 2022); (Drmunozcl, 2025).

6.6.2 Mejora continua del SGSI.

La mejora continua es un principio importante que demanda.

- Colección organizada de datos indicadores, medidas, tendencias.
- Implementar medidas que eliminen las causas del problema en un proceso o producto.
- Realización de acciones preventivas, de forma tal que se mitiguen los riesgos futuros.
- Se utilizan modelos de madurez como COBIT, CMMI e ISOtools para determinar cuán formalizados y repetitivos son los procesos (ISOTools, 2017).

Estos elementos aseguran que el SGSI crezca de forma estratégica y flexible.

6.7 Cierre del ciclo PDCA.

El final de un ciclo PDCA no es una conclusión, es el inicio de un nuevo ciclo con un nivel de madurez superior. Una vez que se completa la revisión por la alta dirección se realizan las auditorias necesarias, el proceso se reinicia en la fase de planificación. En este nuevo ciclo deberá ser dinámico, incorporando las lecciones aprendidas en el camino por parte de las auditorias e incidentes, las sugerencias del personal y la adaptación a cambios regulatorios y tecnológicos.

Para que el SGSI se mantenga con una relevancia y una eficacia alta, se necesita su planificación y se debe de anticipar la evolución de las tácticas adversarias, en cual se debe prestar atención a:

Nuevas Amenazas Emergentes: Es de suma importancia considerar el impacto de amenazas impulsadas por la tecnología, uno de ellos es la ingeniería social la cual está empezando a ser impulsada por inteligencia artificial (IA), los cuales son capaces de crear un phishing altamente refinado y convincente a gran escala (CrowdStrike, 2025). Los atacantes ya

están utilizando y adaptando modelos de IA, especialmente los de Código abierto, esto para aumentar su eficiencia y el impacto de sus operaciones cibernéticas (NCSC, 2025); (Castillo del Rio, 2025a).

Integración de Paradigmas y Tecnologías Avanzadas: Para fortalecer la resiliencia, se integran conceptos estratégicos en la arquitectura de seguridad. La cual incluye la evolución de un modelo de Zero Trust (Confianza Cero), que elimina la confianza implícita y la cual verifica continuamente cada solicitud de acceso sin importar su origen (NIST, 2020). Al mismo tiempo, gestionar el volumen creciente de alertas, lo cual es clave para adoptar plataformas SOAR (Security Orchestration, Automation and Response). Estas herramientas permiten automatizar las tareas cíclicas y estandariza la respuesta a incidentes, lo cual reduce significativamente los tiempos de detección y recuperación (Palo Alto Networks, n.d.).

Por ultimo, la cultura organizacional de la seguridad de la información es uno de los factores el cual permite sostener el ciclo de mejora continua y la protección de la información en un entorno cambiante.

Capítulo 7: Conclusiones y Recomendaciones.

7.1 Cumplimiento de los objetivos.

En esta investigación se abordó el desarrollo de una guía metodológica para la implementación de la Norma ISO/IEC 27001:2022 en organizaciones de distintos tamaños, dando un enfoque particular en pequeñas y medianas empresas (PYMES). Esto se logró a través de un diseño metodológico aplicado, cualitativo y propositivo, fundamentado en el ciclo PDCA (Planificar-Hacer-Verificar-Actuar); se consolidó un marco práctico que simplifica una adopción de manera más efectiva de un Sistema de Gestión de la Seguridad de la Información (SGSI) en contextos con recursos limitados (Parolin, 2022).

7.2 Aportaciones centrales de la investigación

La principal contribución es una guía metodológica escalable que, por una parte, aporta la robustez de la norma ISO 27001 y, por otra parte, está escrita en un lenguaje accesible para organizaciones con recursos escasos (Parolin, 2022). Al reunir en un solo documento las buenas prácticas internacionales, como el marco del NIST CSF (National Institute of Standards and Technology, 2012), los controles CIS y el marco MITRE ATT&CK, se sigue una visión integradora orientada a la resiliencia operativa y no sólo a la certificación. El kit de implementación que se obtiene minimiza la dependencia de asesoría externa. Incluye un modelo de madurez en cinco niveles que permite programar la inversión en seguridad de manera progresiva y demuestra el retorno sobre la inversión (ISOTools, 2017).

7.3 Consecuencias prácticas para los involucrados

Ejecutivos de pymes reciben una hoja de ruta clara para cumplir con requerimientos regulatorios y contractuales sin coste inicial elevado (Drmunozcl, 2025). El CIO y el CISO cuentan con una lista priorizada de controles y métricas que son ideales para cuadros de mando

ejecutivos, por lo tanto, sirve para supervisar y rendir cuentas. Lo que el documento ofrece a la academia es un caso de uso didáctico que permite vincular la teoría de los SGSI a su aplicación práctica a fin de fortalecer la formación de los profesionales (Lucena, 2024). Finalmente, los reguladores halan evidencia de que ISO 27001 puede adaptarse con éxito en organizaciones de bajo recurso, hecho útil para diseñar programas de fomento y apoyo (Microsoft Security, 2023).

7.4 Limitaciones del estudio.

El trabajo se apoya en revisión documental y validación experta, por lo que falta contrastar la metodología en múltiples organizaciones y sectores a lo largo del tiempo para medir su efecto sobre incidentes reales. Asimismo, la mayoría de los textos revisados proviene de Europa y Norteamérica, lo que puede limitar la representatividad de algunos de los indicadores. De otra parte, el avance muy rápido de la tecnología, especialmente de la IA generativa, SASE y las arquitecturas Zero-Trust, requiere ser actualizada al menos una vez al año para que sea realmente pertinente (Assalian, 2025).

7.5 Recomendaciones derivadas del estudio.

Constituir un Comité permanente de SGSI, que asegure recursos y haga seguimiento a la hoja de ruta (NQA, 2023). Migrar, en el tiempo, a auditorías continuas con base en plataformas GRC/SIEM. Revisar el análisis de riesgo en forma semestral o ante incidentes críticos (ENISA, 2023). Comunicar el retorno de inversión en ciberseguridad, para reforzar la cultura interna y la confianza de clientes y socios (*ISO 27001: Controles Y Cómo Implementarlos Correctamente*, n.d.).

7.6 Líneas de investigación futura.

Para una validación del enfoque se puede llevar a cabo con un caso de estudio que se represente en un ambiente simulado, cuando se tenga la autorización de la alta dirección se puede

proseguir con su validación en un ambiente real para valorar su aplicabilidad, flexibilidad y beneficios. Resulta adecuado llevar a cabo la implementación de la guía en pyme de diversos sectores (finanzas, salud, manufactura), así como monitorizar sus indicadores durante un plazo mínimo de un año. También se espera la posibilidad de la automatización de tareas de clasificación documental y de generación dinámica de la SoA con modelos de lenguaje, la posibilidad de integrar el SGSI en reportes ESG, la evaluación de posibilidad de una certificación continua con evidencias digitales soportadas por tecnologías de registro inmutable como Blockchain.

7.7 Reflexión final.

La información no solo debe de ser cuidada por las empresas, también cualquier individuo que considere alguna información como importante. Usando un mapa que guía a los directivos y garantizando su involucramiento, se puede lograr el objetivo común por lograr. Resulta posible conseguir que nuestros índices de seguridad aumenten y se alineen a la ISO 27001:2022 y que nuestras herramientas sean asequibles, aun mas para las pymes, sin necesidad de un conocimiento técnico elevado. Un objetivo a la vista es incrementar la resiliencia y protección de la confianza digital que alimenta nuestra competitividad. Esta tarea, por lo tanto, no solo cumple con las exigencias académicas, sino que también proporciona un instrumento operativo, que puede ser utilizado y enriquecido inmediatamente por la comunidad profesional, que puede invitar a investigadores y organizaciones a hacerlo, ante la evolución de las amenazas, en la que hoy en día, todo ocurre al rito de la innovación técnica (Parolin, 2022).

Referencias Bibliográficas

Castillo del Rio, L. B. (2025b, septiembre). ¿Quiénes son los nuevos soldados de la guerra mundial silenciosa? Ciberguerra. Revista Digital, (2), 1-59.

Parolin, V. M. (2022). ISO 27001 2022 español. Scribd. https://es.scribd.com/document/616176936/ISO-27001-2022-espanol

Valencia Duque, & Orozco Alzate (2017). Metodología para la implementación de un sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas e Tecnologías de Información (RISTI), (24), 73–88. https://dialnet.unirioja.es/servlet/articulo?codigo=6672188

PMG-SSI. (2024). Pilares de la seguridad de la información: Qué son y cómo cumplir con ellos. https://www.pmg-ssi.com/2024/01/pilares-de-la-seguridad-de-la-informacion-que-son-y-como-cumplir-con-ellos/

Gartner. (2023). Gartner identifica las principales tendencias de ciberseguridad para 2023 [Comunicado de prensa]. https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023

Ohayon, H. (2024). The InfoSEC guide to the 10 types of information Security controls. Suridata. https://www.suridata.ai/blog/infosec-guide-to-information-security-controls

Auth0. (n.d.). Authentication and Authorization. Auth0 Docs. https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization

European Union Agency for Cybersecurity [ENISA]. (2023). Panorama de amenazas de ENISA 2023. Publications Office of the European Union.

https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

Open Web Application Security Project [OWASP]. (2021). OWASP Top 10:2021 – Los diez riesgos de seguridad de aplicaciones web más críticos. https://owasp.org/www-project-top-ten/

INCIBE. (2017, 16 de enero). ¡Fácil y sencillo! Análisis de riesgos en 6 pasos. https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

ISOTools. (2017). Mitigación en el tratamiento de riesgos ISO 27001: 4 opciones que puedes implementar. https://www.isotools.us/2017/08/20/4-opciones-mitigacion-tratamiento-riesgos-segun-iso-27001/

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

National Institute of Standards and Technology [NIST]. (2012). Guía para realizar evaluaciones de riesgos (NIST Special Publication 800-30, Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-30r1

López, A. SGSI (Sistema de Gestión de Seguridad de la Información). https://www.iso27000.es/sgsi.html

Ed, Z. (2013). Manual ISO 27001. 2013. Scribd. https://es.scribd.com/document/466720477/Manual-ISO-27001-2013

Microtek Learning. (2024, October 15). How ISO/IEC 27001 Certification Enhances an Organization's Cybersecurity: A Comprehensive Guide https://www.microteklearning.com/blog/iso-iec-27001-cybersecurity-guide

ISOTools. (2015). La familia de normas ISO 27000. https://www.isotools.us/2015/01/21/familia-normas-iso-27000/

NQA. (2023). *Guía de implantación de ISO 27001:2022*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

MDP Ajedrez. (2024). Implementa el ciclo Plan-Do-Check-Act para mejorar tu empresa. https://mdpajedrez.com/implementa-el-ciclo-plan-do-check-act-para-mejorar-tu-empresa

GlobalSuite Solutions. (2023). *Ciclo PDCA de gestión de la ISO 27001*. https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/

Castillo del Rio, L. B. (2025a, agosto). ¿Estamos preparados para sobrevivir a una ciberguerra a gran escala? Ciberguerra. Revista Digital, (1), 1-31.

IBM. (2024). Gestión de amenazas. IBM México. https://www.ibm.com/mx-es/topics/threat-management

World Economic Forum. (2023). Perspectiva global de ciberseguridad 2023. https://www.weforum.org/reports/global-cybersecurity-outlook-2023/

Cybersecurity Ventures. (2020). El ciberdelito costará al mundo 10,5 billones de dólares anuales para 2025. https://cybersecurityventures.com/cybercrime-damage-costs-to-hit-10-5-trillion-by-2025/

Andrea, P., & López, E. A. (2011). Fundamentos de ISO 27001 y su aplicación en empresas. Revista Visión de Futuro. https://www.redalyc.org/pdf/849/84921327061.pdf

Microsoft Digital Defense Report. (2023). Microsoft Digital Defense Report 2023. https://www.microsoft.com/es-mx/security/security-insider/microsoft-digital-defense-report-2023

Microsoft Security. (2023). Informe de defensa digital 2023. https://www.microsoft.com/en-us/security/business/security-intelligence-report

INCIBE (2021). Desarrollar cultura en seguridad. In PROTEGE TU EMPRESA (pp. 1–18) [Book]. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_desarrollar-cultura-en-seguridad.pdf

Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento [AGESIC]. (2021). Estudio comparado de metodologías de análisis de riesgos para TI y Seguridad de la Información (Versión 01). https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/book/6611/download

Pirani. (2022). Matriz de riesgos: qué es, ejemplos y cómo crearla fácil. https://www.piranirisk.com/es/blog/matriz-de-riesgos-que-es-ejemplos-y-como-crearla-facil

Pérez, P. (2025). Todos los controles del Anexo A de la norma ISO 27001 explicados. Software ISO. https://www.isotools.us/2025/01/06/todos-los-controles-del-anexo-a-de-la-norma-iso-27001-explicados/

Kruiskamp, K. (2025). Cómo redactar una declaración de alcance de la norma ISO 27001 (+3 ejemplos) - Compleye.Io. https://compleye.io/es/articulos/como-redactar-una-declaracion-de-alcance-de-la-norma-iso-27001-3-ejemplos/

ISO 27001: Controles y cómo implementarlos correctamente. (n.d.). https://www.piranirisk.com/es/academia/especiales/iso-27001-controles-y-como-implementarlos-correctamente

Initialize, N. (2023). Las 10 métricas y KPIs de ciberseguridad más importantes que los CISOs deben seguir. Secureframe. https://secureframe.com/es-es/blog/cybersecurity-metrics-and-kpis

Lucena, M. M. (2024). Evaluación de Riesgos de Seguridad de la Información según la ISO 27001. https://es.linkedin.com/pulse/evaluaci%C3%B3n-de-riesgos-seguridad-la-informaci%C3%B3n-seg%C3%BAn-mart%C3%ADn-lucena-yzuae

Drmunozcl. (2025). Cláusula 5: Liderazgo. InfoProtección. https://www.infoproteccion.com/iso-27001/clausula-5-liderazgo/

Niveles de madurez de la capacidad en la evaluación de riesgos - FasterCapital. (n.d.). FasterCapital. https://fastercapital.com/es/tema/niveles-de-madurez-de-la-capacidad-en-la-evaluaci%C3%B3n-de-riesgos.html/1

Vivas, J. D. (2025). Lo que debes saber sobre Indicadores Clave de Riesgo (KRI). Pirani. https://www.piranirisk.com/es/blog/que-es-un-indicador-clave-de-riesgo-kri

Grupo Atlas. (2023). 8 pasos para implementar un plan de ciberseguridad. https://www.atlas.com.co/8-pasos-para-implementar-un-plan-de-ciberseguridad/

Assalian, M. (2025, March 25). Zero Trust e IA: La dupla que redefinirá la ciberseguridad en 2025. Security Advisor. https://sadvisor.com/zero-trust-e-ia-la-dupla-que-redefinira-la-ciberseguridad-en-2025/

CrowdStrike. (2025). Most Common AI-Powered Cyberattacks. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

National Cyber Security Centre (NCSC). (2025). Impact of AI on the cyber threat from now to 2027. https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

NIST. (2020). Special Publication 800-207: Zero Trust Architecture. https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Palo Alto Networks. (n.d.). What Is SOAR? https://www.paloaltonetworks.com/cyberpedia/what-is-soar