



UNIVERSIDAD
NACIONAL
DE COLOMBIA

Estructuración de un Sistema Integrado de Gestión de tecnologías de la información basado en la familia de normas ISO/IEC 27000 e ISO/IEC 20000

Luisa Fernanda Jaramillo Ríos

Universidad Nacional de Colombia

Facultad de administración

Manizales, Colombia

2025

Estructuración de un Sistema Integrado de Gestión de tecnologías de la información basado en la familia de normas ISO/IEC 27000 e ISO/IEC 20000

Luisa Fernanda Jaramillo Ríos

Trabajo de investigación presentado como requisito parcial para optar al título de:
Magister en Administración

Director:

Ph.D. Francisco Javier Valencia Duque

Línea de Investigación:

Gestión integrada de tecnologías de la información

Universidad Nacional de Colombia

Facultad de administración

Manizales, Colombia

2025

Agradecimientos

Deseo expresar mi más sincero agradecimiento a todas las personas e instituciones que hicieron posible la realización de este trabajo. En primer lugar, a la Universidad Nacional de Colombia, sede Manizales, por brindar un entorno académico de excelencia y los recursos necesarios que permitieron desarrollar este trabajo.

Mi profundo reconocimiento al director de tesis, por su constante guía, apoyo y dedicación durante todo el proceso de investigación, brindando orientación valiosa y motivación en cada etapa del proyecto.

Extiendo mi gratitud a los expertos que participaron en la validación de los instrumentos, por su disposición, conocimiento y compromiso, los cuales fueron fundamentales para garantizar la rigurosidad y pertinencia del estudio.

Finalmente, agradezco a mi familia y a todas las personas que, de manera directa o indirecta, brindaron apoyo, comprensión y ánimo, permitiéndome completar esta etapa de mi formación profesional con éxito.

Resumen

A lo largo de este trabajo se plantea la estructuración de un sistema integrado de gestión con enfoque hacia la tecnología de la información (TI), basado en el conjunto de estándares enmarcado en la familia de normas ISO/IEC 27000 (Gestión de la Seguridad de la Información) e ISO/IEC 20000 (Gestión de Servicios de TI) aplicable a los distintos procesos de la organización. El documento se encuentra estructurado sobre tres objetivos base, que describen su contexto a partir de revisión narrativa de literatura, la formulación de una propuesta metodológica que mapee y armonice los requerimientos obligatorios de ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 e incorpore el ciclo PHVA, y la validación de la propuesta mediante el juicio de expertos en gestión tecnológica y normas ISO.

El valor central del estudio es ofrecer una guía metodológica práctica, orientada a organizaciones que buscan integrar la calidad en la prestación de servicios TI con prácticas sólidas de seguridad de la información. La propuesta enfatiza el uso de herramientas de gestión, la socialización interna en distintos niveles y la flexibilidad metodológica, de forma que, se mantenga la capacidad de adaptación y replicabilidad en diversos contextos organizacionales.

Palabras clave: Sistema Integrado de Gestión, Seguridad de la Información, gestión del servicio, confianza, calidad, gestión de riesgos

Structuring an Integrated Information Technology Management System based on the ISO/IEC 27000 and ISO/IEC 20000 family of standards

Abstract

Throughout this work, the structuring of an Integrated Management System with a focus on information technology is proposed, based on the set of standards framed within the ISO/IEC 27000 family (Information Security Management) and ISO/IEC 20000 (IT Service Management), applicable to different organizational processes. The document is structured around three main objectives: (i) conducting a narrative literature review to contextualize the study, (ii) formulating a methodological proposal that maps and harmonizes the mandatory requirements of ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018, incorporating the PDCA cycle as the axis of continuous improvement, and (iii) validating the proposal through expert judgment in technology management and ISO standards.

The central contribution of the study is to provide a practical methodological guide, aimed at organizations seeking to integrate quality in IT service delivery with robust information security practices. The proposal emphasizes the use of management tools, internal socialization at different levels, and methodological flexibility, ensuring the ability to adapt and replicate the model across diverse organizational contexts.

Keywords: Integrated Management System, Information Security, Service Management, Trust, Quality, Risk Management

Contenido

Contenido

1.	Antecedentes y estructura de la investigación.....	3
1.1	Antecedentes de investigación.....	3
1.2	Estructura de la investigación	4
1.2.1	Delimitación del problema de investigación	4
1.2.2	Definición de la pregunta de investigación	8
1.2.3	Objetivos.....	8
1.2.4	Justificación	9
1.2.5	Metodología de la investigación.....	11
2.	Revisión narrativa de literatura.....	13
2.1	Marco teórico	13
2.1.1.	Nacimiento y evolución de los sistemas de calidad.....	13
2.1.2.	Sistemas de Gestión basados en las normas ISO	19
2.1.2.1.	Sistema de Gestión de Seguridad de la información.....	20
2.1.2.2.	Sistema de Gestión de Servicios de Tecnologías de la Información	22
2.1.3.	Sistemas integrados de Gestión	23
2.2.	Marco conceptual.....	25
2.3.	Marco Normativo.....	29
2.3.1.	Serie ISO/IEC 27000	29
2.3.1.1.	Principales normas de implementación en la serie ISO/IEC 27000.....	32
2.3.1.2.	Transición de la norma ISO/IEC 27001:2013 a la norma ISO/IEC 27001:2022..	33
2.3.2.	Serie ISO/IEC 20000	35
2.3.3.	Norma ISO/IEC 27013:2021.	36
2.3.4.	Marcos de referencia complementarios	37
3.	Propuesta metodológica para la implementación de un Sistema Integrado de Gestión en Tecnologías de la Información.....	40
3.1.	Fase I: Integración de las normas ISO/IEC 27001 e ISO/IEC 20000-1.....	43
3.1.1.	Correspondencia entre las normas ISO/IEC 27001 e ISO/IEC 20000-1	43
3.1.2.	Requerimientos normativos: Mapeo ISO/IEC 27001 e ISO/IEC 20000-1	47
3.1.3.	Estructura de alto nivel y aplicación del ciclo PHVA en la integración de las normas ISO.	48
3.2.	Fase II: Propuesta metodológica. Sistema Integrado de Gestión de tecnologías de la información basado en las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	51
3.2.1.	Etapa I: Planear	52
3.2.2.	Etapa II: Hacer	72
3.2.3.	Etapa III: Verificar	84

3.2.4. Etapa IV: Actuar	90
4. Juicio de expertos sobre el Sistema Integrado de Gestión de Tecnologías de la Información. 95	
4.1. Metodología de validación	96
4.1.1. Selección y designación de expertos	97
4.1.2. Instrumentos empleados en la validación de los requisitos normativos de las normas NTC ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	100
4.2. Resultados presentados tras la validación de los expertos	101
4.3. Recomendaciones	103
5. Conclusiones	105

Lista de ilustraciones

Ilustración 1. Esquema Metodológico.	12
Ilustración 2. Perspectivas clásicas de la GCT.	19
Ilustración 3. Tríada de la seguridad de la información.	27
Ilustración 4. Principales normas de implementación de la serie ISO/IEC 27000.	33
Ilustración 5. Ciclo PHVA aplicado en la integración de las normas ISO.	50
Ilustración 6. Integración de las políticas de Seguridad de la Información y Gestión del servicio.	57
Ilustración 7. Proceso de gestión de riesgos.	62
Ilustración 8. Proceso de gestión de riesgos para la seguridad de la información.	63
Ilustración 9. Organigrama general.	143
Ilustración 10. Ejemplo grafico – red de valor.	147
Ilustración 11. Perspectiva del BSC para sistemas de información,	148
Ilustración 12. Guía matriz DOFA.	149
Ilustración 13. Presentación del formulario.	161
Ilustración 14. Ponderada pregunta (1) Formulario de evaluación.	162
Ilustración 15. Respuestas pregunta (1.1) Formulario de evaluación.	162
Ilustración 16. Respuestas pregunta (1.2) Formulario de evaluación.	162
Ilustración 17. Respuestas pregunta (2) Formulario de evaluación.	163
Ilustración 18. Respuestas pregunta (3) Formulario de evaluación.	163
Ilustración 19. Respuestas pregunta (4) Formulario de evaluación.	164
Ilustración 20. Respuestas pregunta (5) Formulario de evaluación.	164
Ilustración 21. Ponderada pregunta (6) Formulario de evaluación.	165
Ilustración 22. Respuestas pregunta (6.1) Formulario de evaluación.	165
Ilustración 23. Respuestas pregunta (6.2) Formulario de evaluación.	165

Lista de tablas

Tabla 1. Aportes a la evolución del concepto de calidad.	15
Tabla 2. Serie ISO/IEC 27000.	32
Tabla 3. Cambios introducidos por la ISO/IEC 27001:2022.	35
Tabla 4. Serie ISO/IEC 20000.	36
Tabla 5. Fases, etapas y actividades de implementación para el Sistema Integrado de Gestión de Tecnologías de la Información.	42
Tabla 6. Análisis de correspondencia.	44
Tabla 7. KPIs beneficios de la integración.	46
Tabla 8. Elementos para definir criterios de riesgo.	65
Tabla 9. Gestión de información documentada.	76
Tabla 10. Ficha técnica de expertos. Escalona, Z.	98
Tabla 11. Ficha técnica de expertos. Silva, A.	98
Tabla 12. Ficha técnica de expertos. Hernández, L.	99
Tabla 13. Ficha técnica de expertos. Valencia, F.	100
Tabla 14. Tabla de correspondencia.	109
Tabla 15. Controles de Seguridad de la Información.	114
Tabla 16. Capítulo 4. Contexto de la organización.	115
Tabla 17. Capítulo 5. Liderazgo.	117
Tabla 18. Capítulo 6. Planificación.	120
Tabla 19. Capítulo 7. Apoyo del sistema de gestión.	123
Tabla 20. Capítulo 8. Operación.	137
Tabla 21. Capítulo 9. Evaluación de desempeño.	139
Tabla 22. Capítulo 10. Mejora.	139
Tabla 23. Formato Manual de funciones.	144
Tabla 24. Ejemplo gestión por procesos.	146
Tabla 25. Contexto externo, partes interesadas.	150
Tabla 26. Contexto interno, partes interesadas.	151
Tabla 27. Checklist de aspectos claves para la formulación del alcance del SIG.	152
Tabla 28. Guía metodológica para la definición de objetivos.	155
Tabla 29. Plantilla Declaración de aplicabilidad.	159
Tabla 30. Plantilla Matriz Diagnostico.	167

Introducción

El crecimiento sostenido de la digitalización y la provisión de servicios basados en tecnologías de la información (TI) ha transformado radicalmente el contexto operacional y la relación entre organizaciones y usuarios. Este fenómeno no solo amplía las oportunidades de negocio, sino que incrementa de manera proporcional la necesidad de garantizar calidad en la prestación y seguridad en el manejo de la información, exigencias que hoy constituyen un requisito estratégico para la competitividad y la confianza del cliente. En este marco, las normas internacionales ISO/IEC han consolidado herramientas técnicas y administrativas que permiten estandarizar buenas prácticas; sin embargo, su adopción y la forma de integrarlas aún presentan desafíos operativos y de gobernanza.

A partir de la revisión de estadísticas y literatura reciente, se observa una evolución heterogénea en la adopción de estas normas: mientras la gestión de la seguridad (ISO/IEC 27001) ha mostrado una difusión importante, la certificación en gestión de servicios (ISO/IEC 20000-1) presenta menor penetración en ciertos contextos nacionales, lo que revela una oportunidad de consolidación y articulación entre ambas disciplinas. Esta heterogeneidad y la creciente complejidad del riesgo tecnológico motivaron la pregunta central de esta investigación: ¿cómo integrar la gestión de la seguridad de la información y la calidad en los servicios TI mediante un sistema híbrido que armonice requisitos normativos y prácticas organizacionales?

El propósito de la tesis es diseñar una propuesta metodológica práctica y replicable que permita a las organizaciones estructurar un Sistema Integrado de Gestión de TI partiendo de la correspondencia entre ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018. Para este fin, el trabajo se apoya en tres líneas de acción: una revisión narrativa del marco teórico y normativo que sustenta las normas involucradas; la elaboración de un repositorio y mapeo de requisitos que facilite la convergencia operativa; y la validación técnica del

modelo mediante juicios de expertos con trayectoria en implementación y auditoría de estos estándares. Estas acciones están organizadas en una ruta metodológica estructurada en cuatro fases, que incorpora el ciclo Planear–Hacer–Verificar–Actuar (PHVA) como columna vertebral del despliegue y la mejora continua.

Desde el punto de vista metodológico, la investigación combina una revisión crítica de la bibliografía normativa con un ejercicio aplicado de correspondencia entre numerales normativos, la propuesta de artefactos documentales y la recolección de juicio experto para validar pertinencia y viabilidad. La validación permite contrastar la solidez conceptual del modelo con criterios prácticos y operativos, identificando barreras típicas y priorizando mejoras.

El aporte esperado de este trabajo es dual: académico, por contribuir al corpus sobre integración de normas ISO en el ámbito tecnológico; y práctico, por ofrecer un marco operativo que reduzca duplicidades, facilite auditorías y promueva una gobernanza más coherente de los servicios TI y la seguridad.

1. Antecedentes y estructura de la investigación

Tras llevar a cabo un análisis exhaustivo de diversas fuentes bibliográficas, se determinó que la línea de investigación que permitiría abordar los diferentes objetivos de la propuesta de trabajo es la referente a los Sistemas Integrados de Gestión (SIG), cuyo enfoque destaca por su capacidad de implementar buenas prácticas en los procesos organizacionales, con énfasis en aquellos que se encuentran fundamentados en TI, siendo una de las tendencias globales con mayor crecimiento en los últimos años.

1.1 Antecedentes de investigación

Los Sistemas Integrados de Gestión representan una estructura única que permite gestionar múltiples aspectos de las operaciones ejecutadas en una organización, tomando como base, diferentes estándares normativos que conllevan al desarrollo de buenas prácticas en las actividades operativas, tácticas y estratégicas que enmarcan el funcionamiento de las empresas.

La adecuada integración de los sistemas es una problemática que ha sido abordada por diversos autores, quienes destacan la importancia de fusionar los sistemas y procesos existentes en la organización a partir de la aplicación de prácticas específicas cuyo enfoque se encuentre sustentado en modelos de integración eficientes.

Autores como Carmona y Rivas en [1] plantearon un modelo de integración que respondía a la premisa “la gestión integrada es más eficaz y eficiente cuando esta se aborda mediante un enfoque de gestión basado en procesos”, este modelo promete mejores resultados siempre y cuando las actividades y los recursos relacionados sean formulados en función de una múltiple orientación que considere los efectos para el producto, el entorno y quienes lo producen

Para el caso específico de los Sistemas Integrados de Gestión que se encuentran estructurados bajo el conjunto de estándares planteados en las normas ISO (International Standards Organization), se utiliza como modelo de referencia el anexo SL, el cual proporciona una estructura de alto nivel para los sistemas de gestión ISO, facilitando su uso y proporcionando herramientas necesarias en la racionalización de los sistemas, encontrando una mayor compatibilidad y permitiendo una integración eficaz. [2]

En concordancia con lo expuesto anteriormente, el presente trabajo procura en cada una de las fases de su construcción, contribuir en la generación de respuestas ante uno de los principales desafíos que enfrentan diferentes organizaciones, en particular, aquellas cuya naturaleza plantea la implementación de buenas prácticas desde sus procesos y buscan la integración de sus actividades en sistemas más estructurados y eficientes. Si bien, el desarrollo de un sistema integrado de gestión basado en TI no proporciona una solución total a la creciente necesidad que se presencia a escala global en materia de estándares de calidad; si busca generar un aporte desde la estructuración de un sistema donde se integren prácticas y requerimientos de dos normas, cuya demanda frente a su implementación ha aumentado a raíz de la percepción de crecimiento tecnológico a escala mundial.

1.2 Estructura de la investigación

1.2.1 Delimitación del problema de investigación

En la actualidad, el panorama mundial en términos de desarrollo empresarial apunta hacia el crecimiento en materia de tecnología y el uso de herramientas informáticas que facilitan la creación de productos, tareas, profesiones y actividades económicas nuevas en el conjunto de la economía, siendo crucial que las empresas dispongan de las capacidades necesarias, incluyendo no solo las competencias científicas o técnicas, sino también las políticas, los reglamentos y las infraestructuras que se requieren con tal fin.[3]

Siguiendo este orden de ideas, el crecimiento que han alcanzado los servicios tecnológicos en la sociedad moderna pone en relieve las necesidades de seguridad en el manejo de datos, y a su vez, la calidad en la prestación de servicios informáticos. Los

clientes de las organizaciones dedicadas a la producción de servicios de TI exigen una asistencia más segura, eficaz y eficiente. [4] Dando respuestas a esta demanda por parte del mercado, surge como necesidad la integración de buenas prácticas que respalden la seguridad de los datos y la calidad del servicio, incorporando controles orientados hacia la protección de la información generada a partir del uso de las tecnologías.

Ampliando la visión del estudio desde los datos globales, la tendencia mundial hacia la implementación de procesos estandarizados guiados por prácticas internacionales que respalden la producción de servicios ha tenido un auge con respecto a los años anteriores; las organizaciones cada vez son más conscientes de la necesidad latente frente al despliegue de procesos de calidad; pues entienden que los usuarios buscan garantías sobre el uso de su información y el manejo de sus datos, por lo que cualquier empresa que haga uso de las tecnologías en sus procesos productivos, debe empezar a implementar prácticas orientadas hacia la satisfacción de esta necesidad.

En el informe más reciente presentado por ISO en 2024, titulado *“The ISO Survey 2023”*, se evidencian cambios relevantes en la evolución de las certificaciones a escala mundial. En 2022, la norma ISO/IEC 27001:2013, orientada a la gestión de la seguridad de la información, alcanzó un total de 71.549 organizaciones certificadas, lo que representó un crecimiento del 21,92% respecto a 2021 y la consolidó como la cuarta norma más implementada en el ámbito global. [5] Sin embargo, para 2023, el número de certificaciones cayó abruptamente a 48.671, reflejando una disminución del 31,97%. Esta variación significativa se explica, en gran parte, por la ausencia del organismo de acreditación de China en el levantamiento de datos del último año; no obstante, el descenso sigue siendo considerable frente a la tendencia de crecimiento sostenido de años anteriores. [6]

Por su parte, la norma ISO/IEC 20000-1:2018, centrada en la gestión de calidad de los servicios de TI, tuvo un comportamiento contrastante. En 2022, experimentó el mayor crecimiento porcentual entre todas las normas evaluadas, con un aumento del 129,49% frente a 2021, alcanzando un total de 27.009 organizaciones certificadas en el mundo. [5] No obstante, en 2023, esta norma también presentó una caída drástica en sus cifras, reportando únicamente 3.670 certificaciones globales, lo que representa una reducción del 86,41% respecto al año anterior. [6]

Llevando el análisis hacia el panorama nacional, en 2023 un total de 395 organizaciones obtuvieron la certificación en seguridad de la información, superando las 338 certificaciones registradas en 2022. Este crecimiento posicionó al país en el segundo lugar del ranking latinoamericano, reflejando un compromiso creciente con la protección de los activos de información. En contraste, la adopción de la norma ISO/IEC 20000-1:2018, enfocada en la gestión de calidad de los servicios tecnológicos, continúa siendo limitada en Colombia. En 2022, se registraron 22 organizaciones certificadas, cifra que apenas aumentó a 26 en 2023. [6] A pesar del leve crecimiento, estas cifras evidencian una baja penetración de esta norma en el país. Esta situación pone de relieve la necesidad urgente de fomentar no solo la cultura de la seguridad de la información, sino también el fortalecimiento de la gestión de servicios de TI como un pilar estratégico para la eficiencia operativa, la mejora continua y la competitividad del sector productivo colombiano.

La adecuación de sistemas de gestión se ha convertido en un sinónimo de avance progresivo, donde la implementación de metodologías explícitas dentro de la normativa internacional, como lo son las normas ISO, les permite a las organizaciones alcanzar un correcto desempeño y ampliar la proyección de beneficios, tanto internos como externos; de tal forma, que con su implementación se logre legitimar las capacidades de las organizaciones para satisfacer los requerimientos de comercialización, bajo el cumplimiento del marco legal y reglamentario. [7]

Mencionado lo anterior, la búsqueda de crecimiento por parte de las empresas, quienes sustentan su ejercicio bajo procesos innovadores que les permiten adquirir cierta competitividad ante el mercado, encuentra su mayor aliado para el cumplimiento de este objetivo en los procesos de calidad, donde el reconocimiento brindado por una certificación, ofrece garantías al consumidor frente a la calificación de los procesos ejecutados para el desarrollo de ese producto, lo que se traduce en confianza del cliente con su proveedor y finaliza en la generación de valor agregado para el usuario. [8]

Este tipo de procesos permite que las organizaciones perciban una mejor recepción del mercado ante sus productos, dado que se genera una diferenciación significativa frente a los demás bienes o servicios que responden a la misma naturaleza, generando confianza en los consumidores dada la alta calificación asociada a sus procesos productivos, lo que

aumenta los índices de credibilidad y ayuda al posicionamiento de la organización en el mercado.

El aumento de amenazas que vulneran la seguridad de los datos dispuestos por los usuarios es una realidad innegable que las organizaciones no pueden tomar a la ligera. El número de incidentes relacionados con ataques intencionales y violaciones a la seguridad continúa en ascenso, poniendo en riesgo constante la integridad de la información. Los informes de ciberamenazas publicados por el CCN-CERT en sus ediciones 35/23 [9] y 04/24 [10] evidencian una evolución clara en los métodos de ataque empleados durante 2022 y 2023, destacando el uso de técnicas más sofisticadas y la participación de actores estatales, grupos hacktivistas y cibercriminales.

En el marco global, el World Economic Forum advierte que los riesgos más críticos para la resiliencia digital se concentran en la gestión de terceros, la falta de procesos para evaluar la seguridad de herramientas de inteligencia artificial y la creciente amenaza hacia infraestructuras de investigación y bioseguridad, lo que refleja una brecha sustancial entre la evolución de los riesgos y la capacidad de respuesta de las organizaciones. [11] En este contexto, se hace urgente el despliegue de prácticas robustas de seguridad en TI, especialmente frente a un panorama donde los sectores estratégicos, las infraestructuras críticas y las organizaciones públicas y privadas son blanco de amenazas constantes, muchas de ellas facilitadas por vulnerabilidades conocidas o mal gestionadas.

Siguiendo esta línea de pensamiento, el problema que se ha identificado frente al despliegue de estándares de calidad en la prestación de servicios basados en tecnología, es la falta de integración de prácticas que respalden el uso de la información y le permitan a las organizaciones prestar un servicio mucho más transparente, donde los usuarios perciban mayor satisfacción desde los procesos; siendo una necesidad clave fomentar el despliegue de un sistema integrado de gestión de TI donde se integren prácticas de calidad sobre sus actividades, junto con la implementación de controles que mitiguen los riesgos informáticos, logrando así, una mayor percepción de satisfacción desde los servicios prestados al cliente.

1.2.2 Definición de la pregunta de investigación

¿Cómo integrar la gestión de la Seguridad de la Información y la calidad de los sistemas de TI a partir de un sistema híbrido que designe múltiples aspectos de la operación de acuerdo con diferentes normas internacionales?

1.2.3 Objetivos

Objetivo general

Estructurar un sistema integrado de gestión de tecnologías de la información basado en la familia de normas ISO/IEC 27000 e ISO/IEC 20000

Objetivos específicos

1. Analizar, mediante una revisión narrativa de literatura, la evolución y los aportes de los estándares internacionales ISO/IEC 27000 e ISO/IEC 20000, contextualizando sus alcances desde el marco teórico, conceptual y normativo como base para el diseño de un sistema integrado de gestión en tecnologías de la información.
2. Formular una propuesta metodológica para el diseño de un sistema integrado de gestión que articule los requisitos mandatorios de la norma ISO/IEC 27001 con los de la norma ISO/IEC 20000-1, estableciendo lineamientos para la elaboración de instructivos, procedimientos y formatos que orienten su desarrollo y posterior implementación.
3. Validar los resultados del sistema integrado de gestión de tecnologías de la información a partir de una evaluación de expertos en gestión tecnológica con experiencia en el despliegue de la familia de normas ISO/IEC 27000 e ISO/IEC 20000 en el contexto organizacional.

1.2.4 Justificación

La implementación de sistemas de gestión basados en actividades que respalden la calidad de los productos o servicios ofrecidos al cliente es una necesidad creciente para todas las organizaciones, dado que desde la perspectiva del consumidor, la percepción de calidad ha sido un factor determinante en la toma de decisiones ante la adquisición de bienes o servicios; razón por la cual, los diferentes sectores industriales le apuestan al mejoramiento continuo desde sus prácticas y actividades productivas, generando un respaldo a partir de estándares internacionales, que posibiliten la generación de confianza ante la visión del consumidor final.

Desde una perspectiva global, la integración de estándares de calidad en la estructuración de sistemas de gestión orientados a optimizar los esfuerzos y recursos organizacionales se ha consolidado como una práctica ampliamente adoptada por diversas administraciones públicas, privadas y corporativas. Esta integración permite comparar, refinar y unificar los procesos derivados de diferentes normas, y, a partir de elementos comunes, dar respuesta a las necesidades específicas de cada sistema.

En el ámbito académico, diversos autores le han apostado a la integración de normas y modelos que respondan a las necesidades de implementación desde distintos ámbitos, como es el caso de Herrera en [12] quien propone un despliegue de sistemas integrados de gestión de calidad, ambiente y seguridad en el entorno empresarial o en el caso de Pinto y Sampaio en [13] quienes presentan un análisis de impacto sobre la integración de estos tres sistemas en la industria 4.0.

Tras identificar los avances en la investigación sobre sistemas de gestión reflejados en la literatura, se evidencia una limitada profundización en normas o estándares orientados a la gestión tecnológica en el contexto internacional. Del total de setenta y cuatro estudios citados, aproximadamente el 74 % se centra en la integración de estándares relacionados con la gestión de la calidad, el medio ambiente y la seguridad, mientras que solo una fracción minoritaria aborda de manera específica la gestión tecnológica y sus modelos asociados, como las familias de normas ISO/IEC 27000 e ISO/IEC 20000. Esta brecha resulta significativa, dado que en el contexto actual la gestión tecnológica constituye una de las prácticas con mayor incidencia en los distintos sectores económicos. La tendencia hacia la automatización y el crecimiento tecnológico de las

organizaciones obliga a las empresas a fortalecer sus capacidades en materia de seguridad informática y calidad en la prestación de servicios tecnológicos, ya sea mediante operaciones directas o procesos de tercerización.

En Colombia, las prácticas de calidad han incrementado considerablemente en los últimos años, logrando cifras alentadoras con relación a sistemas de calidad, ambiente y seguridad; pero, considerando el auge tecnológico que han tenido las organizaciones, los niveles de certificación de Colombia frente a prácticas en seguridad informática, protección de datos y prestación de servicios tecnológicos reflejan cifras muy bajas en comparación con los índices globales. Con el fin de reducir las brechas en materia de certificación y facilitar la expansión de las empresas nacionales hacia mercados globales, el gobierno colombiano ha desarrollado un programa que promueve la transformación productiva de las empresas, a partir de la implementación de estándares de calidad y generación de valor agregado, ofreciendo acompañamiento en los procesos de despliegue de sistemas de gestión para los diferentes sectores económicos; Colombia productiva, como se llama la entidad encargada de su despliegue, ha generado un programa orientado hacia el fortalecimiento de la cultura de calidad en las empresas, a partir del acompañamiento y cofinanciación de empresas que realicen proyectos de mejora de calidad y productividad con el fin de obtener certificaciones internacionales. [14]

En el contexto empresarial, la estructuración de un sistema integrado de gestión de TI basado en la familia de normas ISO/IEC 27000 e ISO/IEC 20000, representa una ventaja competitiva y genera impactos significativos desde el ámbito socioeconómico, dado que brinda un modelo guía donde se integran prácticas de ambos estándares y a su vez, se genera una optimización de esfuerzos y recursos, que desde un punto de vista estratégico, representa una gran oportunidad de crecimiento para las organizaciones.

Desde una visión más académica, y con el objetivo de impactar en la formación profesional de jóvenes y adultos que muestran interés en el despliegue de sistemas de gestión de calidad en los diferentes sectores económicos, esta propuesta impacta a la Universidad Nacional de Colombia, quien en aras de su función misional frente a la formación de profesionales e investigadores que actúen responsablemente frente a los requerimientos y tendencias del mundo contemporáneo, generen aportes sociales y

económicos a partir de una visión empresarial y organizacional, donde la apuesta se encuentre dirigida hacia la optimización de procesos, esfuerzos, tiempos y recursos, generando un valor agregado en la oferta profesional sobre entidades de la misma naturaleza. [15]

La integración de prácticas y la consolidación de un sistema integrado para la gestión tecnológica impacta la formación de tres perfiles profesionales ofertados por la universidad en la sede Manizales; desde la formación estratégica y ampliando la visión empresarial, este tipo de prácticas genera una mayor preparación desde los programas de administración de empresas e ingeniería industrial, conectando la integración y armonización de estándares en la gestión de la calidad y productividad, preparando a los jóvenes desde un pensamiento gerencial orientado a la optimización de tiempos y recursos; por otro lado, el programa con mayor impacto es el pregrado en Administración de sistemas informáticos, el cual, desde su objeto de estudio, busca la formación de profesionales con gran capacidad de discernimiento y síntesis, conocedores del desarrollo administrativo y con capacidad de aplicar una gestión adecuada en el campo de los sistemas informáticos de las organizaciones. [16]

Basándonos en lo expuesto anteriormente, se justifica la necesidad de estructurar un sistema integrado de gestión de TI, donde se unifiquen las prácticas de ambos estándares, dando cumplimiento a los puntos de control de la familia de normas ISO/IEC 27000 e ISO/IEC 20000, a partir de un modelo que permita la optimización de recursos para las organizaciones que tomen de referencia el sistema, potenciando sus capacidades de respuesta y ampliando su visión desde la gestión tecnológica.

1.2.5 Metodología de la investigación

La necesidad de estructurar un modelo sólido y coherente para el desarrollo de un Sistema Integrado de Gestión de TI exige una planificación metodológica que permita abordar cada etapa con claridad, orden y propósito. En respuesta a esta necesidad, se plantea una secuencia metodológica compuesta por cuatro (4) fases principales, concebidas para guiar la construcción del sistema bajo una perspectiva técnica, normativa y estratégica.

Este enfoque metodológico se fundamenta en la integración progresiva de diferentes elementos que permitan una alineación efectiva entre los requisitos de las normas ISO/IEC 27001 e ISO/IEC 20000-1. Más allá de una simple secuencia de pasos, cada fase representa un análisis que contribuye al entendimiento del entorno, a la estructuración de procedimientos y a la validación del modelo propuesto. Así, se garantiza que el diseño del sistema responda tanto a los requisitos mandatorios como a las necesidades reales de implementación y sostenibilidad.

En la ilustración No. 1 se presenta la visualización del modelo metodológico utilizado, en el cual se delinearán las cuatro fases que orientan la organización del contenido y la ruta de trabajo seguida. Cada una de estas etapas será desarrollada en detalle a lo largo del documento, con el fin de evidenciar cómo contribuyen de forma articulada a la consecución de los resultados esperados.

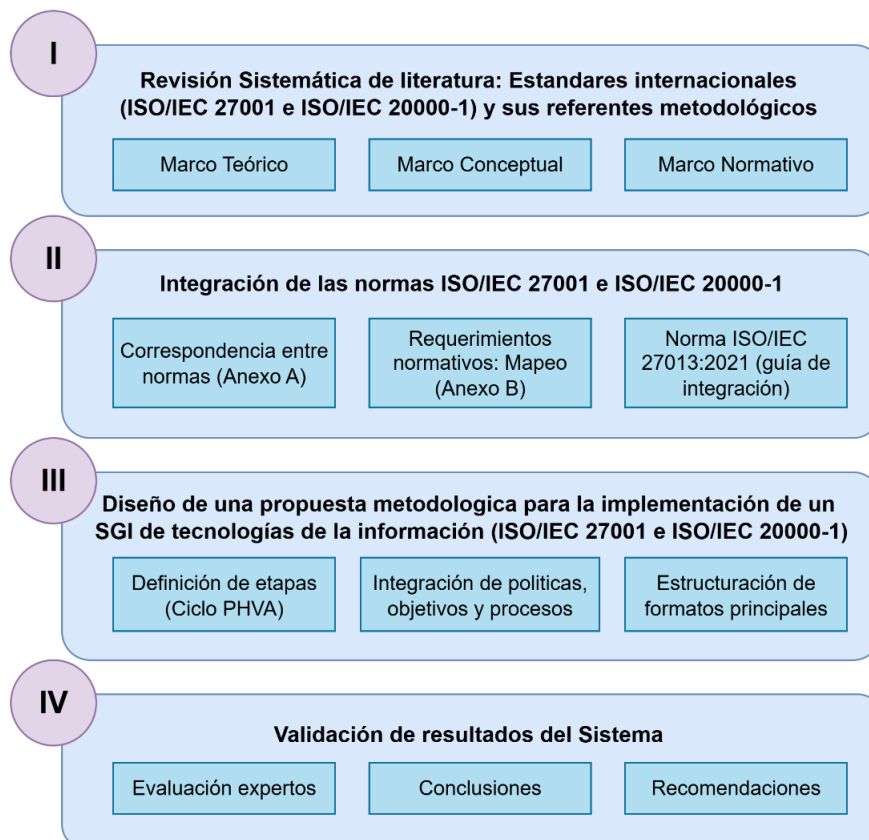


Ilustración 1. Esquema Metodológico. (Elaboración propia)

2. Revisión narrativa de literatura

Dando respuesta al primer objetivo específico planteado en la propuesta de trabajo, se propone la implementación de una revisión narrativa de literatura la cual permitirá estructurar teóricamente un Sistema Integrado de Gestión con enfoque en TI, tomando como base el marco teórico, conceptual y normativo que enmarcan las familias de normas ISO/IEC 27000 e ISO/IEC 20000.

2.1 Marco teórico

2.1.1. Nacimiento y evolución de los sistemas de calidad

El concepto de calidad siempre ha estado arraigado a la historia de la humanidad, dadas las actividades de observación y mejora que el hombre ejecutaba sobre las características de las herramientas que utilizaban; desde tiempos inmemorables se implementaba el concepto de calidad que muchos años después sería definido y estructurado formalmente por diversos teóricos.

Las prácticas de verificación ejecutadas sobre los productos y servicios prestados por comerciantes, artesanos y obreros, se remonta a épocas anteriores al nacimiento de Cristo; el concepto de calidad sobre los productos ofrecidos a la comunidad se regía desde la normativa aplicada por cada civilización, múltiples casos de implementación de estándares y normas aplicables sobre los procesos de construcción se datan en la literatura, un claro ejemplo es la ley 229 del código de Hammurabi, 1760 a.C., la cual establecía que “si un albañil construye una casa para un hombre, y su trabajo no es sólido y la casa se derrumba matando a su dueño, el albañil será condenado a muerte”; por otro lado, procesos como la construcción de la tumba de Rekh-Mi-Re datada en 1450 a.C., consideran procesos rigurosos de inspección sobre las características de los materiales, entre muchos otros ejemplos. [17]

A lo largo de los años las practicas encaminadas a la inspección y garantía de la calidad en los productos y procesos ejecutados en la producción fueron evolucionando y refinándose con cada oficio, el desarrollo de actividades productivas condujeron al nacimiento de aprendices y gremios, lo que a su vez genero una jerarquización en los niveles de mando, donde los instructores desempeñaban a la par el papel de inspectores, cerciorándose de la correcta utilización del material y que el producto estuviera dotado de ciertas características que garantizaran perdurabilidad y reconocimiento.

Con el paso de la producción artesanal a la producción en serie, y el auge del concepto de optimización de procesos empleados en la fabricación de productos a gran escala que arraigo la revolución industrial, el control en términos de calidad tuvo un gran crecimiento; con los grandes lotes que se generaban a diario en las cadenas de producción, era muy común que aparecieran productos defectuosos o con bajos estándares frente a lo que se esperaba del modelo, es aquí, cuando los industriales de la época comienzan a examinar las características de cada lote garantizando la calidad de los productos y separando aquellos que tuvieran defectos, lo que años más adelante evolucionaria hacia una inspección mediante métodos estadísticos a partir de muestras representativas del producto, determinando si el proceso se estaría desarrollando adecuadamente. [17]

La creación de un método de administración encaminado hacia la eficacia y la eficiencia en relación con los tiempos y costos de los procesos productivos, la cual fue ideada por Frederick W. Taylor en 1903, impulso en gran medida las bases de la producción en masa y la creación de la línea de montaje que sería utilizada años más adelante por la compañía Ford, quienes hacían de la calidad uno de los puntos fundamentales en la organización del trabajo. Otro claro ejemplo de la segregación de funciones encaminadas al aseguramiento de la calidad fue la gestión realizada por el departamento de inspección independiente que se instauró en la compañía Western Electric, quienes tenían como objetivo resolver numerosos fallos presentados en la central telefónica. [17]

Finalmente, se habla de la evolución del concepto y se describe desde los modelos de producción japonesa, los cuales, posterior a una renovación y reestructuración en sus criterios de producción, llegaron a representar alta calidad y fiabilidad en los mercados mundiales, logrando el desarrollo de diferentes modelos que serían fuertes impulsores de lo que conocemos actualmente como "Gestión de la calidad". La Tabla No. 1, presentada

a continuación, muestra una detallada recopilación de los aportes teóricos y prácticos que han jugado un papel fundamental en el desarrollo de técnicas y modelos actualmente empleados en diversos sectores productivos.

Autor / Año	Aporte
Walter A. Shewhart en 1924	Aplicación del control estadístico por primera vez con propósitos industriales, buscando mejorar en términos de costo-beneficio las líneas de producción, aumentando la productividad y disminuyendo los errores.
Kaoru Ishikawa en 1943	Considerado el padre del análisis científico de las causas de problemas en procesos industriales, dando nombre al diagrama Ishikawa, cuyos gráficos agrupan por categorías todas las causas de los problemas.
Armand V. Feigenbaum en 1945	"La calidad como gestión" donde describe el resultado del proceso de calidad de General Electric y la primera aplicación del TQC (control de la calidad total)
1946	En Estados Unidos se funda la American Society for Quality Control – ASQC y ese mismo año, los japoneses quienes absorbieron las ideas de control de calidad fundan la JUSE - Unión de Científicos e Ingenieros Japoneses (Organizaciones encaminadas al resguardo de los procesos de calidad en la industria)
1947	Se publica la primer norma ISO, la cual fue ISO/R 1:1951 Standard reference temperature for industrial length measurements
W. Edward Deming en 1950	Aporte en la evolución de la industria japonesa a partir de las charlas impartidas sobre control estadístico de procesos. Creador del ciclo PHVA (Planear – Hacer – Verificar – Actuar)
Kaoru Ishikawa en 1957	"Control de la calidad en toda la compañía" definió la filosofía administrativa que se encuentra detrás de la calidad, los elementos de los sistemas de calidad y lo que él denomina, las "siete herramientas básicas de la gestión de la calidad", donde se le considera una fuerte inclinación hacia las técnicas estadísticas
Phiñip B. Crosby en 1961	Lanza el concepto "cero defectos" exponiendo los primeros fracasos en el terreno espacial los cuales ponen de manifiesto que los fallos provienen casi exclusivamente de errores humanos, lo que buscaba suscitar en los operarios la toma de conciencia sobre el proceso
1980	Aplicación del concepto "Gestión de la calidad total – TQC", promoviendo un enfoque organizacional completo hacia la calidad.
Bill Smith en 1986	Creación de la metodología Six Sigma para la mejora de procesos, la cual se origina a partir de la modelación estadística de los procesos de fabricación, buscando reducir o eliminar los defectos o fallas en la entrega de un producto o servicio al cliente
1987	Publicación de la primera serie de normas ISO 9000, las cuales establecían estándares internacionales para los sistemas de gestión de calidad.

Tabla 1. Aportes a la evolución del concepto de calidad. Elaboración propia, basado en [17]

2.1.1.1. Evolución de las teorías de calidad

Las teorías aplicables sobre el concepto global de gestión de la calidad han tenido una importante evolución a lo largo de los años, diversas corrientes teóricas han sido bases fundamentales de los modelos que se manejan en la actualidad, pero dentro de la literatura se destacan tres postulados cuya aplicación en los procesos ha generado gran impacto sobre la gestión realizada por las organizaciones.

A continuación, se enumeran las teorías que marcaron un hito histórico en el desarrollo conceptual y práctico de lo que hoy conocemos como gestión de la calidad.

A. Control de la calidad

En la literatura se habla del “control de la calidad” desde diferentes conceptos que enmarcan su aplicación sobre los procesos industriales; entre las definiciones más conocidas es mencionado como el proceso de regulación a través del cual es posible medir la calidad real, compararla con las normas y actuar sobre la diferencia. [18]

Por otro lado, la definición de este concepto se enmarca desde tres enfoques adicionales, donde su enunciación varía según la contextualización que se quiera brindar, acogiendo significados como:

1. El control de la calidad es una parte del proceso de regulación e inspección del producto acabado, que más adelante sería ejercido sobre el proceso de fabricación, determinando la correcta elaboración de cada unidad.
2. “Control de calidad” como la denominación de un departamento de la empresa, el cual se encuentra dedicado tiempo completo en función de la calidad, ejerciendo actividades de inspección y pruebas continuas para verificar que los productos cumplan con las especificaciones establecidas.
3. Considerado como el conjunto de herramientas, conocimientos prácticos o técnicas a partir de las cuales son desarrolladas las funciones enmarcadas dentro del concepto de “Calidad”

Este término nace en los años veinte, siendo utilizado como sinónimo de “prevención de defectos”, lo que años más adelante evolucionaría y su principal enfoque estaría encaminado hacia el desarrollo de métodos estadísticos, donde los promotores de este movimiento bautizarían la técnica como “Control estadístico de la calidad (CEC)”, siendo

ampliamente aceptada por diversos directores, quienes tomarían como impresión que el control de la calidad consistía únicamente en el uso de métodos estadísticos en la industria, debilitando el enfoque del término hacia el proceso de regulación. [18]

Este postulado tenía un enfoque totalmente dirigido hacia las tareas o actividades del proceso productivo, sin considerar las necesidades sociales o personales que se vieran involucradas en el proceso, puesto que el objetivo de la industria para ese entonces era netamente la eficiencia productiva de la capacidad instalada.

B. Aseguramiento de la calidad

Con el auge industrial que se vivió hacia los años cuarenta, y los cambios sobre el patrón tradicional de administración que surgen posterior a la segunda guerra mundial, nacen estudios enfocados hacia el comportamiento de las personas dentro de las organizaciones, donde se introducen conceptos como las necesidades básicas de las personas por autores como A. Maslow quien menciona el aumento de la productividad a través del esfuerzo concentrado en grupo, donde la gerencia es responsable de garantizar entornos efectivos y productivos para que los individuos bajo su mando puedan aprovechar la totalidad de su potencial de la mejor manera.

Hacia finales de los años cincuenta, teniendo en cuenta la limitación del enfoque CEC, surge un contra movimiento que buscaba restaurar el concepto sobre la necesidad de aplicación de un amplio conjunto de instrumentos y actividades planificadas que dieran conformidad a los requerimientos establecidos sobre un producto o servicio, naciendo así, el término “Quality Assurance” traducible como Garantía o Aseguramiento de la Calidad. [17]

Este postulado tenía un enfoque hacia el alcance de acciones planificadas y sistemáticas sobre los sistemas de producción, buscando la prevención de defectos antes de su ocurrencia, logrando alcanzar la excelencia funcional que generara confianza sobre el proceso y garantizara que el producto o servicio cumpliera con los estándares asociados a la satisfacción del cliente. [19]

C. Gestión de la calidad total (TQM)

En paralelo, hacia los años cincuenta las industrias japonesas enfocaron sus esfuerzos sobre una reestructuración económica e industrial, para la cual consideraban que la calidad debía ser un factor imperativo dentro de sus procesos, comprendiendo que la respuesta frente a la fabricación de productos no defectuosos dependía del correcto desarrollo del proceso desde el principio.

Para 1950 Deming, uno de los pioneros de la teoría y considerado como el padre de la calidad japonesa, introduce a los procesos industriales el modelo administrativo para el manejo de la calidad, explicando la responsabilidad del personal directivo en el logro de dicho objetivo, enmarcando la importancia de la prevención sobre el control de los factores en el proceso, disminuyendo la aparición de productos defectuosos. El control de cada una de las fases del proceso fue ilustrado por Deming a partir del ciclo PHVA (Planear, Hacer, Verificar y Actuar), partiendo de la necesidad de control desde la concepción del producto o servicio, hasta la mejora continua aplicable sobre los modelos de desarrollo. [20]

Persiguiendo la mejora continua en las organizaciones, la Gestión de la Calidad Total (TQM) concibe la importancia de concientizar a todas las partes involucradas en el proceso frente a la calidad en cada uno de los sectores que conforman la organización, creando constancia frente al propósito de mejora, partiendo de una gestión eficiente por parte de la dirección, cuyo enfoque está dirigido al logro de objetivos a largo plazo, siendo medido desde la satisfacción de todas las partes involucradas en el proceso.

Con la finalidad de ilustrar de forma comparativa el sentido de la Gestión de la Calidad Total, a partir de los postulados presentados por los padres de la teoría, quienes difundieron como método de gerencia este concepto, se toma del artículo presentado por Perdomo y Gonzales [21], una tabla descriptiva que presenta una visión simplificada de los preceptos, principios y pasos recomendados desde las obras de W. Deming, J.M. Juran y P. B. Crosby quienes buscaban el despliegue de la función de calidad en las empresas.

Perspectivas clásicas de la GCT

Deming (principios)	Juran (trilogía)	Crosby (pasos)
1. Crear constancia en el propósito de mejorar.	<i>Planificación de la calidad:</i> 1. Establecer metas de calidad.	1. Compromiso de la dirección.
2. Adoptar la nueva filosofía de la calidad.	2. Identificar clientes y sus necesidades.	2. Equipos para el mejoramiento de la calidad.
3. Dejar de depender de la inspección en masa.	3. Desarrollar productos y procesos.	3. Medición de la calidad.
4. Finalizar la práctica de basar los negocios en el factor precio.		4. Costo de la evaluación de la calidad.
5. Mejorar constantemente la producción y el servicio.	<i>Control de la calidad:</i> 4. Elegir elementos de control y unidades de medida.	5. Conciencia sobre la calidad.
6. Instituir la formación en el trabajo.	5. Establecer metas.	6. Acciones correctivas.
7. Instituir el liderazgo.	6. Medir el desempeño.	7. Compromiso con el cero defectos.
8. Desechar el miedo a la responsabilidad.	7. Comparar metas y desempeño.	8. Entrenamiento.
9. Derribar barreras entre departamentos.	<i>Mejora de la calidad:</i> 8. Identificar proyectos y organizar equipos.	9. Día del cero defectos.
10. Eliminar eslóganes	9. Proveer recursos y entrenamiento.	10. Fijación y ajuste de metas.
11. Eliminar metas numéricas y gestión por objetivos.	10. Manejar la resistencia al cambio y establecer controles.	11. Remover causas de errores.
12. Fomentar el orgullo en el trabajo.		12. Reconocimiento.
13. Instituir programas de educación y autodesarrollo.		13. Consejos de calidad.
14. Actuar basándose en un plan.		14. Hágalo nuevamente.

Ilustración 2. Perspectivas clásicas de la GCT. Fuente: Adaptado de [21]

2.1.2. Sistemas de Gestión basados en las normas ISO

A raíz de la necesidad latente en la industria frente a la formalización de los procesos y la aplicación de prácticas de normalización que facilitaran las transacciones de carácter internacional y garantizaran la satisfacción de todas las partes involucradas en los procesos relacionados con actividades productivas y económicas, la ISO buscando estandarizar los procesos en materia de calidad para todos los usuarios, emite para mediados de los años ochenta la primera guía normativa en términos de calidad para procesos organizacionales, conocida como la norma ISO 9001:1987, la cual describía un modelo estandarizado de prácticas que garantizaran la gestión de la calidad para los diferentes sectores a partir de elementos y actividades coordinadas que interactúan, y

que a su vez, proporcionan herramientas para el establecimiento de políticas y objetivos que facilitan la dirección de las organizaciones.

El nacimiento de un modelo de normas cuyo propósito es garantizar la calidad en la gestión de los procesos, brinda a las organizaciones un referente de buenas prácticas aplicables sobre las actividades realizadas por la empresa. El nivel de complejidad de cada sistema dependerá de diferentes factores asociados a la operación, tamaño y estructura de las organizaciones; pues este tipo de modelos tienen como objetivo mejorar el desempeño de los procesos a partir de la inserción de culturas organizacionales que implementen conscientemente ciclos continuos de autoevaluación y corrección a partir del involucramiento de cada una de las fuerzas de la empresa.

Los sistemas de gestión basados en las normas ISO pueden organizarse bajo cuatro tipos diferentes de esquemas documentales, dependiendo de la necesidad de aplicación que cada norma posea. Estos esquemas son:

- A. Normas de sistemas de gestión generales.** Establecen requisitos y orientan a las organizaciones a gestionar sus políticas y procesos en el cumplimiento de objetivos. Son aplicables a todos los sectores económicos, independiente de las condiciones y factores a los que se encuentren sujetos las organizaciones.
- B. Normas de sistemas de gestión específicos de un sector.** Proveen requerimientos o guías adicionales para la aplicación de un sistema de gestión general sobre un sector específico.
- C. Normas relacionadas con el sistema de gestión y las directrices de aplicación.** Son estándares que proporcionan mayor orientación sobre requerimientos y pasos a seguir sobre aspectos específicos de un sistema de gestión organizacional.
- D. Normas de gestión.** Apoyan la implementación de aspectos específicos del sistema de gestión de una organización. [22]

2.1.2.1. Sistema de Gestión de Seguridad de la información enfocado en las normas ISO

El concepto de gestión de seguridad de la información nace formalmente en la década de los noventa, cuando el gobierno británico, a través del Department of Trade and Industry

(DTI), impulsó el desarrollo de una guía de buenas prácticas para proteger la información en las organizaciones. Esta iniciativa derivó en la publicación, en 1995, de la norma BS 7799-1 por parte del British Standards Institution (BSI), la cual recogía recomendaciones para gestionar la seguridad de la información en ambientes corporativos. Posteriormente, en 1998, se publicó la BS 7799-2, que introdujo por primera vez los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), consolidando así un enfoque sistemático y verificable para administrar la seguridad de la información.[23]

Con el tiempo, estos desarrollos británicos fueron adoptados por las normas ISO y la Comisión Electrotécnica Internacional (IEC). En el año 2000, se internacionalizó la BS 7799-1 bajo el nombre ISO/IEC 17799, como código de buenas prácticas. Sin embargo, el paso decisivo ocurrió en octubre de 2005, cuando se publicó oficialmente la norma ISO/IEC 27001:2005, basada en la BS 7799-2. Esta versión se convirtió en la primera norma internacional certificable en gestión de la seguridad de la información, incorporando principios como la identificación y el tratamiento de riesgos, la implementación de controles, la definición de políticas y la mejora continua. [23] Esta norma no solo estandarizó el enfoque de protección de información en el mundo corporativo, sino que también otorgó una base para las auditorías internas y externas en organizaciones de todos los sectores.

La evolución normativa continuó con la publicación de la versión del 2013, que introdujo la Estructura de Alto Nivel (High Level Structure – HLS), alineando su arquitectura con otras normas ISO facilitando la integración de sistemas y simplificó la gestión conjunta. Asimismo, se reorganizó el Anexo A, que agrupa los controles de seguridad en 14 dominios estratégicos. En octubre de 2022, se publicó una nueva versión, ISO/IEC 27001:2022, que ajusta los controles a 93 y los clasifica en cuatro grandes categorías: organizacionales, personas, físicos y tecnológicos, con base en la nueva ISO/IEC 27002:2022. Este cambio representa una respuesta al avance tecnológico y a los nuevos desafíos, como la ciberseguridad, el trabajo remoto y la protección de datos personales.

En paralelo a esta evolución normativa, diversos estudios han documentado la implementación del SGSI en entornos reales. Por ejemplo, el diseño de un SGSI basado en ISO/IEC 27001:2013 para una empresa financiera en Cali, abordando desde el

análisis de riesgos hasta la definición de políticas y controles, lo cual demuestra la aplicabilidad práctica de la norma en el contexto colombiano. [24] Asimismo, el desarrollo de un SGSI para instituciones educativas, aplicando metodologías como MAGERIT para la gestión de riesgos y fortaleciendo la seguridad en entornos no corporativos, lo que evidencia la versatilidad del estándar.[25]

Estas experiencias refuerzan la comprensión de que la norma ISO/IEC 27001 no es simplemente una herramienta técnica, sino un marco estratégico de gestión organizacional. Su historia, desde los orígenes en el Reino Unido hasta su consolidación global, muestra cómo las necesidades de proteger la información han evolucionado hacia un modelo estructurado, certificable y adaptable, que hoy en día se integra fácilmente en sistemas de gestión más amplios, permitiendo a las organizaciones responder de manera efectiva a las exigencias regulatorias, tecnológicas y sociales del entorno digital actual.

2.1.2.2. Sistema de Gestión de Servicios de Tecnologías de la Información enfocado en las normas ISO

Frente a la necesidad de asegurar un Sistema de Gestión del Servicios alineado con buenas prácticas internacionales, surgió el interés por estandarizar y formalizar las actividades asociadas a la gestión eficiente de los servicios de TI. El origen de esta norma se remonta al British Standards Institution (BSI), que en 1995 publicó la guía DISC PD0005:1995, considerada el primer referente formal en la materia. Este documento sería el antecedente directo de la norma BS 15000:2000, reconocida como la primera especificación técnica orientada a la gestión de servicios de TI, fundamentada en un enfoque por procesos y orientada a la mejora continua mediante la aplicación del ciclo de Deming.[26] Posteriormente, en 2002, se publicaron las versiones BS 15000-1:2002, que establecía los requisitos del sistema de gestión del servicio, y BS 15000-2:2003, que proporcionaba directrices para su implementación. Estas versiones consolidaron un marco integral de gestión basado en las mejores prácticas del modelo ITIL (Information Technology Infrastructure Library), fortaleciendo así la estructura metodológica del estándar y su aplicabilidad en distintos contextos organizacionales.

Reconociendo su potencial como estándar internacional, en 2005 la ISO y la IEC adoptaron la BS 15000 mediante un proceso de aprobación acelerada (fast track),

publicando la primera versión de la norma como ISO/IEC 20000-1:2005 e ISO/IEC 20000-2:2005. En el primer tramo se establecieron los requisitos formales para implementar un sistema de gestión de servicios de TI, mientras que en el segundo tramo se proporcionó una guía práctica para su implementación. [27] Con esta adopción, se consolidó el primer estándar internacional certificable en gestión de servicios TI, aplicable a organizaciones proveedoras internas o externas de servicios tecnológicos.

En 2011, se publicó una revisión sustancial bajo el título ISO/IEC 20000-1:2011, orientada a mejorar la claridad, alinear los conceptos con otras normas como ISO/IEC 27001 y reflejar prácticas más modernas de entrega de servicios. A ello le siguió la publicación de la segunda parte revisada en 2012, con orientación actualizada para implementación efectiva. Sin embargo, fue en 2018 cuando se realizó el cambio estructural más profundo: la ISO/IEC 20000-1:2018 adoptó la Estructura de Alto Nivel (High Level Structure – HLS), común a normas como ISO 9001, ISO/IEC 22301 e ISO/IEC 27001, con el objetivo de facilitar la integración de sistemas de gestión. [28] Esta versión también incorporó elementos clave como el enfoque basado en riesgos, el contexto de la organización, el conocimiento organizacional, y procesos renovados para gestión de la demanda, relaciones, proveedores, y continuidad del servicio.

En síntesis, desde su adopción en 2005 como estándar certificable, la norma ISO/IEC 20000 ha evolucionado hacia un modelo robusto y estratégico para la gestión de servicios de TI, integrable con otros sistemas ISO, orientado a resultados, flexible y adecuado a entornos dinámicos de prestación tecnológica.

2.1.3. Sistemas integrados de Gestión

En vista de la creciente necesidad de asegurar un sistema de gestión alineado con buenas prácticas internacionales, surgió la búsqueda de integrar múltiples prácticas dentro de una sola estructura organizacional, lo que dio origen a los Sistemas Integrados de Gestión. Estos sistemas permiten a las organizaciones coordinar de manera eficaz distintas funciones, procesos y estructuras bajo un modelo único y coherente, con el propósito de evitar duplicidades, optimizar recursos y fomentar una cultura organizacional centrada en la mejora continua. La integración, entendida como la alineación de sistemas de gestión mediante la eliminación de solapamientos conceptuales y la unificación del

lenguaje organizacional, potencia la eficacia operativa y estratégica. Esto se traduce en beneficios tangibles como la reducción de la burocracia, la mejora en la calidad de bienes y servicios, el fortalecimiento de la comunicación interna, una mayor agilidad en la toma de decisiones, y una disminución de los costos administrativos. Además, se incrementa la satisfacción de las partes interesadas, al facilitar un enfoque sistémico más eficiente y alineado con los objetivos organizacionales [29]

En sus orígenes, los Sistemas Integrados de Gestión fueron desarrollados de forma empírica por empresas que, al implementar varias normas de forma simultánea, enfrentaban dificultades en la compatibilidad de sus estructuras, lo que generaba sobrecarga documental, duplicación de procesos y auditorías aisladas. Esta situación motivó a la ISO a buscar una estrategia de estandarización a partir de una estructura de alto nivel que garantizara la coherencia y compatibilidad entre los diferentes estándares, lo que dio paso a la creación del Anexo SL.

El Anexo SL fue oficialmente publicado en el año 2012, siendo una estructura de alto nivel de que establece una arquitectura común para todas las normas sobre sistemas de gestión. Este marco proporciona un conjunto uniforme de 10 cláusulas principales, junto con términos y definiciones armonizados, que permiten alinear múltiples sistemas bajo un esquema coherente y racionalizado. Las cláusulas abarcan desde el contexto de la organización, liderazgo y planificación, hasta el soporte, operación, evaluación del desempeño y mejora continua, lo cual asegura una lógica común en todas las normas. [30] El Anexo SL fue diseñado para simplificar la integración y fomentar la estandarización entre áreas organizacionales, mejorando así la eficiencia en la implementación, auditoría y mejora de los sistemas existentes.

Esta evolución estructural supuso un hito en la historia de los Sistemas Integrados de Gestión, ya que por primera vez se permitió una integración verdaderamente coherente entre diferentes marcos normativos. Esta convergencia facilita la implementación de políticas unificadas, auditorías integradas y una visión sistémica del desempeño organizacional, siendo especialmente beneficiosa para organizaciones que operan en sectores regulados o que requieren certificaciones múltiples.

Además, estudios recientes como el de Frontiers han demostrado que el Anexo SL no solo fomenta la integración técnica, sino que promueve una gobernanza organizacional

más sólida, al obligar a las empresas a analizar su contexto, considerar las partes interesadas y tomar decisiones basadas en evidencias. Esto refuerza el carácter estratégico de los Sistemas Integrados de Gestión en contextos empresariales modernos y sostenibles. [31]

2.2. Marco conceptual

International Organization for Standardization (ISO): Organización internacional independiente y no gubernamental, conformada por 173 países y respaldada por una red de 828 comités técnicos responsables del desarrollo de normas. Fue fundada en 1946 en Londres, con el objetivo de reunir a expertos de todo el mundo para establecer métodos más eficientes, seguros y sostenibles para la realización de actividades en diversos sectores. Desde su creación, ISO ha emitido más de 25.900 normas internacionales y documentos complementarios, que abarcan aspectos clave de la tecnología, la gestión, la producción y la seguridad. [32]

El propósito de las normas ISO es estandarizar los procesos críticos, especialmente en áreas como la gestión de la calidad, la seguridad de la información y la prestación de servicios, promoviendo prácticas globalmente aceptadas. Su misión se centra en fomentar el desarrollo de la estandarización y actividades conexas, con el fin de facilitar el intercambio internacional de bienes y servicios, impulsar la eficiencia organizacional y mejorar la competitividad global.

Sistema Integrado de Gestión (SIG): modelo organizacional que combina dos o más sistemas de gestión que comparten elementos comunes, con el objetivo de facilitar su planificación, implementación, control y mejora dentro de una estructura única y coherente. [33]

Desde una perspectiva técnica, un Sistema Integrado de Gestión busca reducir duplicidades, optimizar recursos, mejorar la coherencia operativa y fortalecer la cultura de mejora continua. Su diseño responde a principios de eficiencia sistémica, y se apoya en marcos comunes como el Anexo SL, que proporciona una estructura armonizada de alto nivel para las normas ISO de gestión. [29]

Sistema de Gestión de Seguridad de la Información (SGSI): proceso sistemático, estructurado y protocolizado, adoptado por toda la organización, que tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información. Este sistema establece políticas, procedimientos, controles y responsabilidades claras para gestionar los riesgos asociados al uso, almacenamiento y transmisión de la información. [34]

El SGSI no solo se basa en herramientas tecnológicas, sino en la participación de todos los miembros de la empresa, quienes desempeñan un papel fundamental en la protección de los activos de información. Su implementación permite proteger los procesos de negocio frente a amenazas internas y externas, asegurar la continuidad operativa y generar confianza entre clientes, socios y partes interesadas.

Información como activo: Un activo de información se refiere a cualquier elemento humano, físico o electrónico que almacena, procesa, transmite o utiliza información relevante para los procesos de negocio de una entidad. Este activo puede incluir desde bases de datos, documentos, sistemas tecnológicos y redes, hasta el conocimiento de los empleados. [35]

Dado su carácter crítico, la información contenida o manipulada por estos activos debe ser resguardada frente a riesgos, vulnerabilidades y amenazas. Por lo tanto, proteger los activos de información es un objetivo central de cualquier sistema de gestión de seguridad de la información, ya que de ellos depende el funcionamiento, la reputación y la continuidad del negocio.

Seguridad de la información: Disciplina integral orientada a proteger la información mediante la implementación de procesos, políticas, controles y tecnologías adecuados. Esta disciplina integra tanto aspectos relacionados con la seguridad informática como con la ciberseguridad, asegurando la protección de los artefactos tecnológicos que generan, procesan, almacenan, difunden y transmiten datos e información.

La seguridad de la información tiene como propósito preservar las propiedades esenciales del dato: confidencialidad, integridad y disponibilidad, así como otras propiedades complementarias como autenticidad, no repudio y fiabilidad. Se fundamenta en la identificación y gestión sistemática de riesgos, amenazas y vulnerabilidades

asociadas a los activos de información, bajo un enfoque estructurado y continuamente mejorable. [36]

En su enfoque, Valencia [36] resalta que la implementación de la seguridad de la información no debería verse como un proyecto puntual, sino como un proceso permanente de la organización, alineado con los objetivos del negocio. El autor plantea que este proceso debe estar respaldado por metodologías estructuradas, garantizando adecuación regulatoria, mejora continua y consolidación de una cultura organizativa enfocada en la protección de su información crítica.

A continuación, en la ilustración No. 3 puede evidenciarse la triada de seguridad de la información planteada por el autor:

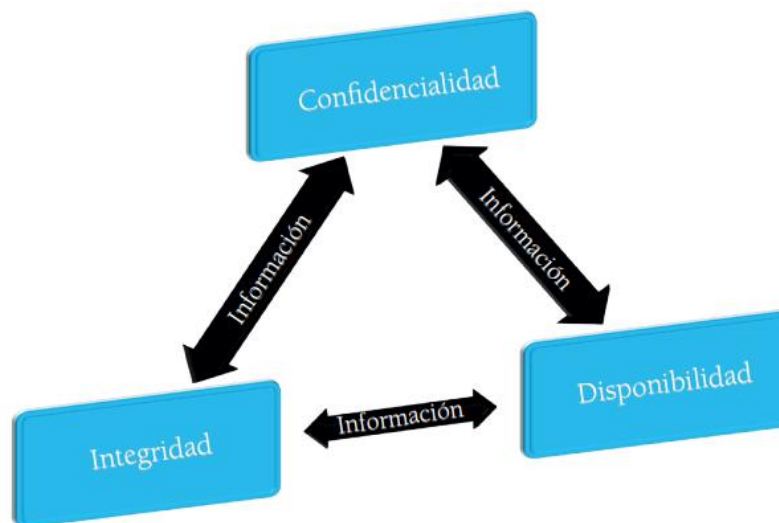


Ilustración 3. Tríada de la seguridad de la información. Fuente: Adaptado de [36]

Pilares de la seguridad de la información

- **Confidencialidad de la información:** Protección de la información contra el acceso no autorizado, asegurando que los datos sensibles solo estén disponibles para quienes cuentan con los permisos adecuados. La confidencialidad implica establecer niveles de acceso diferenciados, aplicar métodos de autenticación y definir roles y privilegios para cada usuario o grupo dentro del sistema.

Una adecuada clasificación de la información es esencial para determinar qué datos deben protegerse y en qué condiciones. Por ejemplo, en entornos donde los datos se manejan bajo distintos niveles de sensibilidad (como "Confidencial" o "Reservado"), solo los usuarios con el nivel correspondiente de autorización pueden acceder a cada categoría. De esta forma, se evita que personas sin los permisos requeridos visualicen, copien o modifiquen información crítica, reduciendo el riesgo de filtraciones, espionaje o mal uso de los datos. [37]

- **Disponibilidad de la información:** Capacidad de garantizar que la información y los recursos tecnológicos estén accesibles y utilizables en todo momento por los usuarios autorizados, en el formato correcto y desde ubicaciones pertinentes, siempre que se requieran.

La disponibilidad se ve afectada cuando los sistemas presentan fallos, interrupciones, accesos ineficientes o tiempos de respuesta elevados, comprometiendo la operatividad y afectando significativamente a los usuarios y a los procesos de negocio. Para garantizarla, las organizaciones deben implementar mecanismos de redundancia, recuperación ante desastres, almacenamiento seguro y planes de continuidad que aseguren el acceso oportuno a los datos, incluso ante fallos del sistema. [37]

- **Integridad de la información:** Principio de la seguridad de la información que garantiza que los datos se mantengan exactos, completos y sin alteraciones no autorizadas a lo largo de todo su ciclo de vida. Este principio asegura que la información permanezca intacta desde su creación o captura hasta su almacenamiento, procesamiento, transferencia y uso, protegiéndola tanto de modificaciones accidentales como maliciosas.

La integridad implica que los datos conservan su consistencia y fiabilidad, lo que se logra mediante controles como validaciones de formato y tipo, sumas de verificación, firmas digitales y controles de acceso adecuados. Estos mecanismos permiten detectar cualquier alteración y asegurar que la información no ha sido modificada sin autorización. [37]

Sistema de Gestión de Servicio (SGS): Conjunto formal de políticas, procesos y procedimientos que permiten planificar, implementar, operar, supervisar y mejorar la entrega de servicios de TI, alineados con los objetivos estratégicos de la organización y los compromisos adquiridos. [38] Su propósito es asegurar que dichos servicios cumplan con los requisitos establecidos y generen valor para sus partes interesadas.

La norma ISO/IEC 20000 formaliza este enfoque como un Service Management System, proporcionando un modelo orientado a procesos para gestionar de forma eficiente el ciclo de vida de los servicios. En su análisis, los autores destacan que la norma define un sistema de gestión de servicios que permite a las organizaciones entregar servicios con un nivel consistente de calidad, ajustados a los compromisos con el cliente y en línea con los objetivos estratégicos del negocio. [39] El SGS, al estructurar los servicios bajo principios de estandarización, permite a las organizaciones resolver eficazmente problemas relacionados con la continuidad, la disponibilidad y el desempeño de los servicios de TI.

Mejora continua: Actividad recurrente para mejorar el desempeño, mediante la identificación e implementación de oportunidades que aumenten la eficacia, eficiencia y adecuación de los procesos. [38] En el contexto de la seguridad de la información, permite adaptar el SGSI frente a un entorno cambiante, caracterizado por riesgos, amenazas y tecnologías en constante evolución, asegurando así la protección continua de la confidencialidad, integridad y disponibilidad de la información.

De igual forma, en la gestión del servicio (ISO/IEC 20000-1), la mejora continua garantiza que los servicios de TI respondan de forma efectiva a las necesidades del negocio, optimizando su calidad y sostenibilidad.

2.3. Marco Normativo

2.3.1. Serie ISO/IEC 27000

La serie ISO/IEC 27000 es un compendio de estándares técnicos desarrollados por ISO e IEC, que brindan un marco de gestión en seguridad de la información que puede ser aplicado en cualquier tipo de organización.

La serie de normas ISO 27000 está compuesta por diversos estándares que, en conjunto, proporcionan un marco integral para la gestión de la seguridad de la información. En particular, la norma ISO/IEC 27001 establece los requisitos para implementar un SGSI, mientras que la ISO/IEC 27002 actúa como un código de buenas prácticas y controles que complementa dichos requisitos. [40] Estas normas, junto con otras pertenecientes a la misma serie, conforman una guía estructurada que se ilustra en la tabla No. 2:

Norma	Definición
27000:2018	"Tecnología de información – técnicas de seguridad – sistemas de gestión de seguridad de la información – marco general y vocabulario" Describe los fundamentos de un SGSI a partir de un marco general de la familia de estándares; brinda una introducción a la gestión de seguridad de la información, así como los términos y definiciones usados por los diferentes estándares.
27001: 2022	"Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos" Contiene los requisitos del sistema de gestión de seguridad de la información
27002:2022	"Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información" Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información
27003:2017	"Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Orientación" Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases
27004:2016	"Tecnología de la información – Técnicas de seguridad – Gestión de la seguridad de la información – Monitoreo, medición, análisis y evaluación". Guía utilizada para el desarrollo y uso de métricas y técnicas aplicables con el fin de determinar la eficacia y efectividad de un SGSI
27005:2022	"Seguridad de la información, ciberseguridad y protección de la privacidad - Guía para la gestión de riesgos de seguridad de la información" Proporciona las directrices para la gestión del riesgo en la seguridad de la información
27006-1:2024	"Seguridad de la información, ciberseguridad y protección de la privacidad: requisitos para organismos que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información" Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información
27007:2020	"Seguridad de la información, ciberseguridad y protección de la privacidad: Directrices para la auditoría de sistemas de gestión de la seguridad de la información" Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.
TS27008:2019	"Tecnología de la información – Técnicas de seguridad – Directrices para la evaluación de los controles de seguridad de la información" Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI

Norma	Definición
27009:2020	"Tecnología de la información - Técnicas de seguridad - Aplicación sectorial de ISO/IEC 27001 - Requisitos" Es una guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte
27010:2015	"Tecnología de la información -- Técnicas de seguridad -- Gestión de seguridad de la información para comunicaciones intersectoriales e interorganizacionales"
27011:2024	"Tecnología de la información -- Técnicas de seguridad -- Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para organizaciones de telecomunicaciones" Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones
27013:2021	"Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1"
27014:2020	"Tecnología de la información - Técnicas de seguridad - Gobernanza de la seguridad de la información" Guía de gobierno corporativo de la seguridad de la información.
TR27015:2012	"Tecnología de la información -- Técnicas de seguridad -- Directrices de gestión de seguridad de la información para servicios financieros" Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002
27016:2014	"Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Economía organizacional" Guía de valoración de los aspectos financieros de la seguridad de la información.
27017:2015	"Tecnología de la información — Técnicas de seguridad — Código de prácticas para controles de seguridad de la información basado en ISO/IEC 27002 para servicios en la nube" Guía de seguridad para Cloud Computing
27018:2019	Código de prácticas para la protección de información de identificación personal (PII) en la nube pública que actúan como procesadores de PII
27019:2017	"Tecnología de la información — Técnicas de seguridad — Controles de seguridad de la información para la industria de servicios públicos de energía" Guía para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía
27021:2021	"Tecnología de la información - Técnicas de seguridad - Requisitos de competencia para profesionales de sistemas de gestión de seguridad de la información"
27023:2015	"Correspondencia entre las versiones de ISO/IEC 27001 e ISO/IEC 27002"
27030:2014	"Tecnología de la información -- Técnicas de seguridad -- Seguridad de la información en redes de sensores inalámbricas"
27031:2011	"Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de las tecnologías de la información y la comunicación para la continuidad del negocio"
27032:2012	"Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad" Proporciona orientación para la mejora del estado de seguridad cibernética.
27033:2009	"Tecnología de la información - Técnicas de seguridad - Seguridad de red" Norma dedicada a la seguridad en redes, consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante

Norma	Definición
	gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.
27034:2011	"Tecnologías de la información - Técnicas de seguridad - Seguridad de aplicaciones" Norma dedicada la seguridad en aplicaciones informáticas, consistente en 6 partes: conceptos generales, marco normativo de la organización, proceso de gestión de seguridad en aplicaciones, validación de la seguridad en aplicaciones, estructura de datos y protocolos y controles de seguridad de aplicaciones, guía de seguridad para aplicaciones de uso específico
27035:2016	Guía sobre la gestión de incidentes de seguridad en la información
27036:2011	"Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con proveedores" guía sobre la seguridad en las relaciones con proveedores, consiste en cuatro partes: visión general y conceptos, requisitos comunes, seguridad en la cadena de suministro TIC, seguridad en entornos de servicios Cloud.
27037:2018	"Tecnología de la información — Técnicas de seguridad — Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital" Guía para la Identificación, recolección, adquisición y preservación de evidencia
27038:2014	"Tecnología de la información – Técnicas de seguridad – Especificación para la redacción digital"
27039:2015	"Tecnología de la información - Técnicas de seguridad - Selección, despliegue y operación de sistemas de detección y prevención de intrusiones (IDPS)"
27040:2015	"Tecnología de la información - Técnicas de seguridad - Seguridad del almacenamiento"
27041:2015	"Tecnología de la información - Técnicas de seguridad - Orientación para garantizar la idoneidad y adecuación del método de investigación de incidentes"
27042:2015	"Tecnología de la información - Técnicas de seguridad - Directrices para el análisis e interpretación de evidencia digital".
27043:2015	"Tecnología de la información – Técnicas de seguridad – Principios y procesos de investigación de incidentes"
27044:2016	"Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Medición"
27799:2016	Es un estándar de gestión de seguridad que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes

Tabla 2. Serie ISO/IEC 27000. Elaboración propia, basado en [40]

2.3.1.1. Principales normas de implementación en la serie ISO/IEC 27000

Uno de los aspectos fundamentales para implementar de forma eficaz un sistema con enfoque hacia la Seguridad de la Información conforme con los estándares internacionales, es la comprensión integral del marco normativo que lo sustenta. En particular, la serie ISO/IEC 27000 proporciona una arquitectura estructurada que define el vocabulario, los requisitos, los controles, las guías y las aplicaciones específicas del

SGSI. Conocer su estructura y las relaciones entre sus distintas partes resulta esencial para planear una implementación eficaz y conforme con las mejores prácticas. [41]

A continuación, en la ilustración No. 4 se presenta una representación gráfica de las principales normas que soportan la implementación de un SGSI dentro de la familia ISO/IEC 27000, evidenciando su relación jerárquica y funcional en torno a la norma central ISO/IEC 27001:2022.



Ilustración 4. Principales normas de implementación de la serie ISO/IEC 27000. Fuente: Adaptado de [41]

Estas normas están interrelacionadas y conforman una base normativa que no solo apoya la gestión técnica del sistema, sino que permite articular las actividades estratégicas, operativas y de mejora continua dentro de una organización. La comprensión clara de esta relación favorece la construcción de esquemas de implementación integrados y efectivos, adaptados a las particularidades de cada entorno organizacional.

2.3.1.2. Transición de la norma ISO/IEC 27001:2013 a la norma ISO/IEC 27001:2022

La actualización de la norma ISO/IEC 27001:2022 representa una evolución técnica que refuerza la capacidad de las organizaciones para adaptarse a los nuevos desafíos de la gestión de la seguridad de la información, sin modificar la estructura central basada en el

ciclo Deming. Aunque se mantiene la lógica del sistema de gestión, se introducen cambios relevantes en varios numerales de la norma, con énfasis en una mayor claridad en la planificación, control y mejora continua del SGSI. Esta revisión también permite una integración más sencilla con otros sistemas de gestión basados en normas ISO, gracias a su completa alineación con la Estructura de Alto Nivel (Anexo SL). [42]

El cambio más representativo se encuentra en el Anexo A, cuya reorganización busca simplificar la aplicación de los controles, responder a nuevas amenazas del entorno digital y facilitar su contextualización en los entornos tecnológicos actuales. Esta transformación refleja un enfoque más estratégico, flexible y orientado al riesgo, manteniendo la coherencia con los objetivos del sistema y su entorno operativo. En la tabla No. 3 se resumen los principales ajustes normativos incorporados en la transición:

N°	Cambios clave por numeral	Descripción
4.2	Comprender las necesidades y expectativas de las partes interesadas	Se agregó explícitamente la indicación de determinar cuáles de esas necesidades y expectativas se convierten en requisitos para el SGSI, lo que implica mayor claridad en la identificación de requisitos de cumplimiento y exigencias contractuales, regulatorias o sociales relevantes.
4.4	Sistema de gestión de la seguridad de la información	Se actualiza el texto para alinearse completamente con la estructura del Anexo SL, por lo que se fortalece la redacción sobre la necesidad de establecer, implementar, mantener y mejorar continuamente el SGSI de manera integral.
6.2	Objetivos de seguridad de la información y planificación para alcanzarlos	Mayor detalle en cómo se deben planificar los objetivos: quién es responsable, qué recursos se requieren, plazos, resultados esperados y método de evaluación.
6.3	Planificación de los cambios	Este numeral no existía explícitamente en la versión 2013, se requiere que las organizaciones planifiquen formalmente cualquier cambio dentro del SGSI, considerando su propósito, posibles consecuencias, recursos y riesgos asociados.
8.1	Planificación y control operativos	Se refuerza el vínculo con los controles del Anexo A y se especifica que se deben implementar procesos documentados para cumplir con los requisitos del SGSI.
9.1	Seguimiento, medición, análisis y evaluación	Se clarifica que el seguimiento y la medición deben hacerse con frecuencia planificada, y que deben evaluarse los resultados y la eficacia del SGSI, buscando que el análisis no sea solo cumplimiento, sino que contribuya a la mejora del sistema.
9.3.2	Aportaciones para la revisión de la gestión	Se amplía la lista de elementos que deben incluirse en la revisión de la dirección (por ejemplo, cambios en el entorno interno/externo, información sobre el desempeño de los proveedores). Fortalece el enfoque estratégico de la alta dirección y su involucramiento con decisiones basadas en datos.
10	Mejora	Se mantiene el enfoque en la no conformidad y acción correctiva, pero se actualiza el lenguaje para reforzar que se deben tomar medidas que eliminen las causas raíz.
AA	Anexo A (controles)	Los controles han sido reorganizados pasando de 14 dominios a cuatro categorías principales: Organizativos, de personas, físicos y tecnológicos. El número total de controles del anexo A asciende a 93, frente a los 114 de la edición anterior.

N°	Cambios clave por numeral	Descripción
AC	Atributos de control	Introducción de cinco atributos de control que permiten clasificar los controles desde múltiples perspectivas. (Tipo de control (preventivo, detectivo, correctivo, etc.), Propiedades de seguridad de la información (confidencialidad, integridad, disponibilidad), Conceptos de ciberseguridad, Capacidades operativas, Dominios de seguridad)

Tabla 3. Cambios introducidos por la ISO/IEC 27001:2022. Elaboración propia

Este proceso de transición no solo requiere adecuaciones documentales, sino una revisión profunda del SGSI bajo una mirada más analítica y proactiva. Se convierte así en una oportunidad para fortalecer la gobernanza de la seguridad de la información, adaptarse a las dinámicas actuales y mejorar el desempeño organizacional.

2.3.2. Serie ISO/IEC 20000

La serie ISO/IEC 20000 es un compendio de estándares técnicos desarrollados por La ISO e IEC, donde se establece una implementación efectiva y un planteamiento estructurado para desarrollar servicios de TI fiables. [43]

La certificación en la norma ISO/IEC 20000 permite a las organizaciones demostrar, de manera independiente, que sus servicios de tecnologías de la información cumplen con estándares internacionales y buenas prácticas en la gestión del servicio. Esta norma se basa en un enfoque estructurado que contempla un conjunto de trece procesos definidos, complementados por un proceso de planificación e implementación orientado a garantizar la prestación eficaz de los servicios. Además, establece requisitos específicos para el sistema de gestión del servicio y se fundamenta en el ciclo de mejora continua (PHVA/PDCA), promoviendo así la eficiencia operativa, la satisfacción del cliente y la alineación con los objetivos del negocio. [43] Como se muestra en la Tabla No. 4, estos elementos conforman el marco esencial para la gestión integral y la mejora continua de los servicios de TI.

Norma	Definición
20000-1:2018	"Tecnología de la información - Gestión de servicios - Parte 1: Requisitos del sistema de gestión de servicios"
20000-2:2019	"Tecnología de la información - Gestión de servicios - Parte 2: Guía para la aplicación de sistemas de gestión de servicios" Código de práctica para la implementación de un SGS

Norma	Definición
20000-3:2024	"Tecnología de la información - Gestión de servicios - Parte 3: Guía para la definición del alcance y aplicabilidad de la norma ISO/IEC 20000-1"
20000-4:2010	"Tecnología de la información - Gestión del servicio - Parte 4: Modelo de referencia para procesos de gestión de servicios". Modelo para realizar una evaluación de procesos de provisión de servicios TI, contiene escala de medición para evaluar la capacidad del proceso
20000-5:2013	"Tecnología de la información - Gestión de servicios - Parte 5: Ejemplo de plan de implantación de la Norma ISO/IEC 20000-12". Ejemplo de implementación gradual de la norma que establece los requisitos para un sistema de gestión de servicios a partir de tres fases.
20000-6:2017	"Tecnología de la información - Gestión de servicios - Parte 6: Requisitos para los organismos que proporcionan la auditoría y certificación de los SGS"
20000-9:2015	"Tecnología de la información — Gestión de servicios — Parte 9: Guía sobre la aplicación de ISO/IEC 20000-1 a los servicios en la nube" Guía de implementación para proveedores que ofrecen servicios en la nube
20000-10:2018	"Tecnología de la información — Gestión de servicios — Parte 10: Conceptos y vocabulario" Contiene conceptos básicos de la norma y las relaciones con otras normas internacionales e informes técnicos, junto con una explicación de la terminología utilizada para su correcta interpretación
20000-11:2015	Se trata de un informe técnico sobre la relación entre ISO / IEC 20000-1 y los modelos de gestión de servicios: ITIL, incluyendo recomendaciones para su integración enfocándose en la relación de causas, procesos y términos incluidos en ambas normas
20000-12:2016	Se trata de un informe técnico sobre la relación entre ISO / IEC 20000-1 y los modelos de gestión de servicios: CMMI-SVC (conexión entre ambos marcos)

Tabla 4. Serie ISO/IEC 20000. Elaboración propia

En definitiva, la norma ISO/IEC 20000 proporciona un marco estructurado para gestionar eficientemente los servicios de TI, tanto internos como orientados al cliente. Su enfoque basado en procesos y buenas prácticas internacionales permite no solo mejorar la calidad del servicio, sino también optimizar costos, aumentar la rentabilidad y fortalecer la reputación organizacional.

2.3.3. Norma ISO/IEC 27013:2021. Guía para la implantación integrada de ISO/IEC 27001 e ISO/IEC 20000-1

La norma ISO/IEC 27013:2021, titulada "Seguridad de la información, ciberseguridad y protección de la privacidad: Guía para la implementación integrada de las normas ISO/IEC 27001 e ISO/IEC 20000-1"; surge como una guía práctica para apoyar a las organizaciones en la implementación coordinada de ambos sistemas de gestión. Su propósito es ofrecer orientación sobre cómo aprovechar las similitudes y objetivos

comunes de las dos normas internacionales, reduciendo duplicidades y optimizando recursos. [44]

La norma destaca que una implementación coordinada permite:

- Mayor credibilidad organizacional, al ofrecer garantía de servicios eficaces.
- Reducción de costos y tiempos de implementación, al desarrollar de manera integral procesos comunes y evitar la duplicación de controles.
- Mejora de la comunicación y colaboración interna, favoreciendo el entendimiento entre los equipos de gestión de servicios y de seguridad de la información.
- Mayor capacidad de cumplimiento normativo, facilitando auditorías y evaluaciones al disponer de controles alineados y documentados bajo una lógica común
- Estandarización de procesos y prácticas, fortaleciendo la coherencia en la operación y la toma de decisiones.
- Fortalecimiento de la cultura organizacional, al promover una visión integral donde la seguridad y la calidad del servicio no se gestionan por separado, sino como componentes de un mismo modelo estratégico. [45]

En este sentido, la ISO/IEC 27013:2021 no reemplaza ni modifica los requisitos de las normas principales, sino que actúa como un documento de apoyo que orienta a las organizaciones en la planificación, integración y mantenimiento de un sistema de gestión que combine los controles de seguridad de la información con los procesos de gestión de servicios.

2.3.4. Marcos de referencia complementarios

ISO/IEC 31000:2018. Estándar internacional que proporciona principios y directrices para la gestión de riesgos en organizaciones de cualquier tamaño o sector. Su propósito es integrar la gestión del riesgo en todos los niveles de la organización, fortaleciendo la toma de decisiones, la planificación estratégica y la resiliencia operativa. Esta norma promueve un enfoque estructurado y proactivo que permite identificar oportunidades,

anticipar amenazas y aumentar la confianza de las partes interesadas frente a un entorno incierto y cambiante. [46]

ITIL (Information Technology Infrastructure Library): Conjunto de buenas prácticas diseñado para optimizar la gestión de servicios de TI. Surgió a finales de los años ochenta a través de la Agencia Central de Computación y Telecomunicaciones (CCTA), en respuesta a la creciente dependencia de las organizaciones respecto a la infraestructura tecnológica y la necesidad de garantizar su uso eficiente y alineado con los objetivos del negocio. Su versión más reciente, ITIL 4 adopta un enfoque moderno y flexible, centrado en la generación de valor mediante la integración de marcos como Agile, DevOps y Cloud Computing. Introduce el Sistema de Valor del Servicio (SVS) y un modelo de cuatro dimensiones para facilitar una visión holística de la gestión, permitiendo que cada organización defina sus propios procesos de acuerdo con sus necesidades, promoviendo así agilidad y eficiencia operativa. [47]

NIST Cybersecurity Framework (CSF): El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF) es una guía estructurada que permite a las organizaciones gestionar y reducir los riesgos asociados a la ciberseguridad de manera sistemática. Este marco está compuesto por tres elementos fundamentales:

- **Núcleo (Core):** Conjunto de funciones esenciales que representan el ciclo completo de la gestión de ciberseguridad dentro de una organización. Estas funciones (identificar, proteger, detectar, responder y recuperar) orientan las acciones necesarias para establecer, operar y mejorar un programa de ciberseguridad, desde el análisis de riesgos hasta la capacidad de respuesta ante incidentes.
- **Niveles de Aplicación:** Sistema que permite valorar el nivel de madurez en la gestión del riesgo cibernético a partir de escalas numéricas. Las organizaciones pueden asignarse una puntuación según el grado de formalización y efectividad de sus prácticas de seguridad, lo que facilita una autoevaluación.
- **Perfiles:** Herramientas que permiten a las organizaciones comparar su estado actual de seguridad con un estado objetivo deseado. Esta comparación les ayuda a priorizar acciones, optimizar el uso de recursos y planificar mejoras alineadas con sus necesidades específicas y su tolerancia al riesgo.[48]

CMMI (Capability Maturity Model Integration): Conjunto estructurado de buenas prácticas que ayudan a las organizaciones a elevar su capacidad en distintas áreas claves de gestión, permitiendo evaluar el nivel de madurez de los procesos y orientar mejoras graduales, desde prácticas informales hasta procesos definidos, gestionados y optimizados.

- **CMMI-DEV** define cinco niveles de madurez que permiten a las organizaciones evaluar y optimizar sus capacidades en ingeniería de sistemas y software, desde la planificación hasta la entrega, promoviendo la calidad, la eficiencia y la reducción de riesgos. [49]
- **CMMI-SVC** se enfoca en mejorar la prestación y gestión de servicios mediante áreas de práctica orientadas al desempeño. Proporciona orientación a las organizaciones proveedoras de servicios para configurar, gestionar y entregar servicios de forma eficiente y consistente. [50]

COBIT (Control Objectives for Information and Related Technology): Marco de referencia para el gobierno y la gestión de TI en el contexto empresarial. COBIT 5.0 establece principios y prácticas que integran requerimientos de control, riesgos y aspectos técnicos, asegurando que la Seguridad de la Información apoye los objetivos corporativos. Incluye tres procesos claves como la administración de la seguridad, la continuidad y los servicios de seguridad, los cuales proporcionan guías para su adecuada gestión. Además, describe procesos genéricos con objetivos de control, actividades clave y métricas, integrando un modelo de madurez para evaluar y mejorar su desempeño. [41]

3. Propuesta metodológica para la implementación de un Sistema Integrado de Gestión en Tecnologías de la Información.

El despliegue de un sistema orientado a la gestión de TI constituye un componente estratégico para la sostenibilidad y la competitividad de las organizaciones. En este escenario, la estructuración de procesos de manera ordenada y fundamentada en estándares internacionales se convierte en un factor decisivo para garantizar tanto la protección de los activos de información como la calidad en la prestación de los servicios. Las buenas prácticas promovidas por modelos normativos como la ISO/IEC 27001 y la ISO/IEC 20000-1 ofrecen lineamientos que, al integrarse de forma coherente, permiten a las organizaciones alcanzar mayores niveles de eficiencia, control y confianza institucional.

La articulación de estas normas no solo responde a la necesidad de las organizaciones de cumplir con los requisitos mandatorios de cada sistema, sino que también aporta a la consolidación de un modelo de gestión coherente, en el cual la seguridad de la información y la gestión de servicios se entienden como dimensiones complementarias dentro de un mismo sistema. Esta integración permite reducir duplicidades, fortalecer la capacidad de respuesta frente a incidentes y generar valor agregado para las organizaciones, al ofrecer un marco unificado de control y mejora continua. En este sentido, la estructuración del modelo a través de fases metodológicas constituye una estrategia efectiva para garantizar su adaptabilidad, organización y pragmatismo, al tiempo que favorece una dinámica de mejora permanente. Tal enfoque ha sido resaltado en investigaciones recientes, como la de Guerrero y Niño en [51], quienes evidencian que la integración normativa mediante fases de diagnóstico, diseño y validación facilita la construcción de sistemas de gestión aplicables y replicables en diversos contextos empresariales.

En coherencia con lo anterior, este trabajo plantea el diseño de una propuesta metodológica orientada a la implementación de un sistema integrado de gestión de TI. Dicho esquema se desarrolla en tres fases principales. La primera corresponde a la integración de normas y se centra en analizar los puntos de convergencia entre la ISO/IEC 27001 y la ISO/IEC 20000-1, considerando guías como la ISO/IEC 27013 y estructurando el modelo bajo el enfoque de mejora continua del ciclo Deming. Con base en este diagnóstico normativo, la segunda fase se orienta al diseño del sistema, en la que se definen los elementos esenciales y se construyen los documentos (instructivos, procedimientos y formatos) que soportan la operación del modelo, permitiendo que los requisitos de ambas normas se traduzcan en prácticas concretas y coherentes. Finalmente, la tercera fase se centra en la validación de la propuesta mediante la evaluación de expertos, lo que garantiza que el sistema no solo cumpla con la formalidad documental, sino que resulte aplicable, pertinente y adaptable a distintos contextos organizacionales.

Cada una de estas fases se desglosa en etapas y actividades específicas que una organización debería ejecutar para desplegar un sistema integrado de gestión de TI. Dichas etapas permiten traducir los requisitos normativos en acciones concretas, de manera que el sistema no se limite a un marco documental, sino que se configure como un instrumento operativo de mejora continua y alineación estratégica. En la tabla No. 5 se presentan de forma detallada las fases, etapas y actividades definidas para este proyecto, en correspondencia con los numerales de las normas ISO/IEC 27001 e ISO/IEC 20000-1.

Fases		Etapas	Actividades
I	Integración de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	Correspondencia entre las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	<ul style="list-style-type: none"> - Analizar la estructura de alto nivel de los estándares evaluados - Reconocer puntos comunes en la planificación del sistema
		Requerimientos normativos: Mapeo de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	<ul style="list-style-type: none"> - Desglosar los numerales comunes de cada norma - Determinar procesos duplicados y áreas que pueden ser integradas
		Aplicación del ciclo PHVA en la integración de las normas ISO/IEC 27001 e ISO/IEC 20000-1	Definir aplicación del ciclo Deming en la estructura integrada
II	Propuesta metodológica. Sistema Integrado de Gestión de tecnologías de la información basado en las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	Despliegue del ciclo PHVA. Etapa I: Planear.	<ul style="list-style-type: none"> - Analizar y comprender la organización - Definir el alcance del sistema integrado de gestión - Explicar el liderazgo y compromiso de la alta dirección - Definir la política integrada - Definir los objetivos del sistema - Analizar la disponibilidad de recursos, así como los riesgos y oportunidades del sistema
		Despliegue del ciclo PHVA. Etapa II: Hacer.	<ul style="list-style-type: none"> - Gestionar los recursos y competencias del sistema integrado de gestión - Crear conciencia y cultura organizacional a partir de la comunicación de las actividades desplegadas en el cumplimiento del Sistema Integrado - Gestionar la información documentada - Ejercer control sobre la operación y la prestación del servicio - Desplegar actividades de gestión sobre el ciclo de vida del servicio - Gestionar incidentes y problemas - Gestionar la continuidad y disponibilidad del servicio - Gestionar riesgos y controles - Desplegar políticas y requisitos específicos de la operación
		Despliegue del ciclo PHVA. Etapa III: Verifica.	<ul style="list-style-type: none"> - Realizar seguimiento, medición, análisis y evaluación del sistema - Planear el esquema de la auditoría interna y su ejecución - Plantear revisiones periódicas por parte de la alta dirección - Generar informes de desempeño y comunicación de los resultados.
		Despliegue del ciclo PHVA. Etapa IV: Actuar	<ul style="list-style-type: none"> - Gestionar las no conformidades y acciones correctivas - Implementar acciones de mejora sobre el sistema integrado de gestión

Tabla 5. Fases, etapas y actividades de implementación para el Sistema Integrado de Gestión de TI. Elaboración propia

3.1. Fase I: Integración de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018

El punto de partida de la propuesta se encuentra en la integración de las normas ISO/IEC 27001 e ISO/IEC 20000-1, concebida como un proceso estratégico para consolidar un marco de gestión unificado que, además de dar cumplimiento a los requisitos mandatorios de cada estándar, aproveche sus sinergias. Esta fase constituye el fundamento metodológico del proyecto, pues busca articular ambos marcos de manera que la seguridad de la información y la gestión de servicios se comprendan como dimensiones interdependientes dentro de un mismo sistema, garantizando coherencia, eficiencia y complementariedad en su aplicación organizacional.

3.1.1. Correspondencia entre las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018

Para lograr realizar una adecuada implantación integrada de la familia de normas ISO/IEC 27000 e ISO/IEC 20000, es necesario partir de un análisis de correspondencia que permita contrastar la estructura de los sistemas de gestión propuestos por cada estándar. Este proceso se fundamenta en los lineamientos de la **ISO/IEC 27001:2022**, Seguridad de la información, ciberseguridad y protección de la privacidad – Requisitos del Sistema de Gestión de Seguridad de la Información, junto con los de la **ISO/IEC 20000-1:2018**, Tecnologías de la Información – Gestión del servicio – Requisitos del Sistema de Gestión del Servicio. A partir de esta comparación estructural, es posible identificar los puntos de convergencia que facilitan la integración, así como aquellos requisitos que requieren un tratamiento independiente, asegurando de este modo el cumplimiento integral y efectivo de ambos marcos normativos.

El instrumento central empleado para establecer la correspondencia entre ambas normas fue diseñado a partir de las directrices incluidas en el Anexo A de la ISO/IEC 27013, documento que orienta la integración entre los dos modelos. Este recurso permitió realizar un comparativo entre las categorías contempladas en los diez capítulos de cada estándar, asegurando la identificación de coincidencias y diferencias. Asimismo, se tomó como referencia el modelo metodológico desplegado por la consultora Sánchez-Toledo & Asociados, aplicado inicialmente en la integración de sistemas de gestión de calidad, ambiente y seguridad y salud en el trabajo (SST). [52] De este enfoque se rescataron aspectos clave para la unificación de marcos normativos, los cuales fueron adaptados a las particularidades de la integración entre la ISO/IEC 27001:2022 y la ISO/IEC 20000-1:2018, garantizando un proceso estructurado y aplicable al contexto del proyecto.

Desde la perspectiva metodológica, el análisis de correspondencia tuvo como objetivo determinar el grado de integración alcanzable entre ambos estándares. Para ello se realizó una revisión numeral por numeral, clasificando los requisitos en tres categorías: (i) requisitos plenamente integrables, (ii) requisitos parcialmente integrables y (iii) requisitos exclusivos de cada norma. Con base en esta clasificación, se aplicó una fórmula sencilla que permitió establecer el porcentaje de integración alcanzado en cada capítulo, expresado como la relación entre los requisitos integrables (plenos y parciales) y el total de requisitos analizados.

$$\% \text{ Integración} = \frac{N^{\circ} \text{Requisitos Integrables}}{N^{\circ} \text{Total Requisitos del Capitulo}} \times 100$$

En la tabla No. 6 se presentan los resultados consolidados del análisis por capítulo:

Cap	Total actividades	Plenamente integrables	Parcialmente integrables	Excluidos de cada norma	% Integración global
Sim.	X	Y (Y%)	W (W%)	Z (Z%)	(Y + W / X) * 100
4	4	2 (50%)	1 (25%)	1 (25%)	75%
5	4	2 (50%)	2 (50%)	0 (00%)	100%
6	6	1 (16%)	4 (68%)	1 (16%)	84%
7	10	3 (30%)	7 (70%)	0 (00%)	100%
8	33	3 (09%)	3 (09%)	27 (82%)	18%
9	7	3 (43%)	3 (43%)	1 (14%)	86%
10	2	2 (100%)	0 (00%)	0 (00%)	100%

Tabla 6. Análisis de correspondencia (Elaboración propia)

Posteriormente, se ponderaron los resultados generales, asignando un porcentaje de integración con base en el número de requisitos comunes frente al total analizado.

$$\% \textit{ Integración Total} = \frac{\sum Y + \sum W}{\sum X}$$

De este ejercicio se obtuvo que, en promedio, cerca del 55% de los requisitos analizados presentan algún grado de integración (plena o parcial). Este resultado confirma que la mayor parte de las exigencias normativas pueden gestionarse de manera conjunta, al estar alineadas en propósito, alcance y resultados esperados. El porcentaje restante corresponde a requisitos que deben ser tratados de forma independiente: en la ISO/IEC 20000-1:2018, aquellos vinculados con la operación detallada del ciclo de vida del servicio (gestión de incidentes, problemas, cambios y continuidad); y en la ISO/IEC 27001:2022, los controles específicos asociados a la confidencialidad, integridad y disponibilidad de la información.

Este nivel de integración permite no solo reducir duplicidades y optimizar recursos internos, sino también generar beneficios tangibles en términos de certificación y auditoría. Aunque cada norma se certifica de manera independiente, muchas entidades certificadoras (NYCE, BSI, SGS, Bureau Veritas, ICONTEC) ofrecen esquemas de auditoría combinada o certificación en paralelo, en los cuales los requisitos comunes se evalúan en una sola jornada. Este modelo ha demostrado reducir los costos totales de certificación entre un 25% y un 30%, dependiendo del número de normas integradas. Por ejemplo, si el costo promedio de certificar de forma aislada dos normas es de USD 20.000 (USD 10.000 cada una), una certificación combinada puede situarse en torno a USD 13.000 – 15.000, lo que representa un ahorro significativo para la organización.

En cuanto al tiempo de certificación, el impacto es igualmente relevante. Una empresa que decide certificar dos normas por separado puede enfrentar hasta 6 auditorías anuales (entre auditorías de certificación y de seguimiento), lo que implica una alta carga administrativa. En cambio, bajo un sistema integrado, estas auditorías se consolidan en procesos transversales, reduciendo en promedio un 50% los tiempos de evaluación. En términos operativos, si cada auditoría independiente demanda 5 días de trabajo de auditores externos y equipos internos (10 días en total para tres normas), al integrarlas

se requieren solo 5 días, liberando hasta una semana laboral completa para el personal clave de la organización.

En síntesis, la integración de normas bajo la Estructura de Alto Nivel no solo aporta coherencia metodológica, sino que garantiza eficiencia operativa, reducción de costos y optimización de tiempos de auditoría. Para un director que evalúa la adopción de este enfoque, los datos muestran que la inversión en un sistema integrado de gestión puede traducirse en:

- Una reducción de entre el 50% y el 60% en duplicidad de tareas, al unificar políticas, procedimientos, auditorías internas y revisiones por la dirección.
- Una optimización en el uso de recursos humanos, que permite operar con un equipo integrado, reduciendo aproximadamente un 30% la carga administrativa frente a la gestión separada de ambos sistemas.
- Una disminución en tiempos y costos asociados a auditorías externas y procesos de certificación, dado que un mismo ciclo de preparación y revisión documental responde a la mayoría de los requisitos normativos.
- Una mejora en la aplicabilidad de actividades parcialmente integrables, que, al apoyarse en metodologías compartidas, generan resultados más consistentes y fortalecen la experiencia organizacional en seguridad de la información y gestión de servicios.

Para que estos beneficios no se queden en el plano teórico, se propone expresarlos en KPIs o fórmulas de cálculo, de manera que cada organización pueda evaluarlos en su propia realidad. Algunos ejemplos pueden observarse en la tabla No. 7

Ítem	Formula
Reducción de costos de auditoría	$Ahoros = \frac{\text{Costo individual} - \text{Costo integrado}}{\text{Costo individual}} \times 100$
Optimización de carga administrativa	$Optimización = \frac{\text{Horas iniciales} - \text{Horas integradas}}{\text{Horas iniciales}} \times 100$
Avance en madurez del sistema integrado	$Avance = \frac{\text{N. de madurez actual} - \text{N. de madurez base}}{\text{Nivel de madurez máximo}} \times 100$
Reducción en tiempos de certificación	$Reducción = \frac{\text{Tiempos C. individual} - \text{Tiempos C. integrada}}{\text{Tiempos C. individual}} \times 100$

Tabla 7. KPIs beneficios de la integración

En conclusión, los resultados del análisis de correspondencia demuestran que la integración entre la ISO/IEC 27001:2022 y la ISO/IEC 20000-1:2018 es no solo viable, sino altamente recomendable, al permitir reducir duplicidades, fortalecer la coherencia de procesos y optimizar recursos financieros y humanos. Asimismo, se resalta que en este análisis se incorporaron los controles actualizados de la ISO/IEC 27001:2022 (basados en la ISO/IEC 27002), garantizando que la propuesta responda a los cambios introducidos en la versión vigente. La correspondencia completa entre ambas normas, junto con los controles documentados, se encuentra detallada en el Anexo A y B, que constituye la base de referencia para futuras implementaciones organizacionales.

3.1.2. Requerimientos normativos: Mapeo de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018

El análisis normativo realizado parte de un mapeo detallado de los requisitos establecidos en los capítulos cuatro (4) al diez (10) de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018, con el objetivo de identificar de manera comparativa los puntos de coincidencia y las diferencias específicas entre ambos marcos. Este ejercicio no se limita a establecer correspondencias textuales, sino que permite reconocer con claridad qué requisitos pueden ser atendidos mediante un mismo conjunto de prácticas y cuáles exigen un tratamiento particular para garantizar el cumplimiento integral de cada estándar.

El instrumento de análisis, consignado en el Anexo B: Matriz comparativa de requerimientos normativos ISO/IEC 27001:2022 – ISO/IEC 20000-1:2018, se presenta en formato tabular y organiza los numerales de ambas normas de manera estructurada. Dicho mapeo especifica:

- **Requisitos normativos plenamente integrables:** aquellos numerales de ambas normas que comparten propósito y alcance, lo que permite su cumplimiento conjunto mediante un único control o procedimiento integrado.
- **Requisitos normativos parcialmente integrables:** numerales que, aunque no coinciden completamente en su redacción, sí permiten armonizar procesos y

controles bajo un mismo esquema metodológico, con ajustes menores para responder a las particularidades de cada estándar.

- **Requisitos exclusivos de integración:** aspectos propios de ISO/IEC 27001 o ISO/IEC 20000-1 que no tienen un equivalente en la otra y que, por lo tanto, exigen mecanismos, controles o procedimientos específicos para su cumplimiento. El mapeo identifica claramente estos casos para que la organización diseñe acciones diferenciadas sin perder la visión integrada del sistema.

De este modo, el mapeo proporciona a las organizaciones una visión práctica y comparativa de los requerimientos normativos, funcionando como una guía metodológica para planificar la implementación de un sistema integrado. Su valor reside en que permite evitar duplicidades en procesos comunes, aprovechar las sinergias entre seguridad de la información y gestión del servicio, y reconocer los requisitos diferenciadores que deben ser atendidos con especial cuidado para garantizar la efectividad del sistema.

3.1.3. Estructura de alto nivel y aplicación del ciclo PHVA en la integración de las normas ISO.

La etapa final de la primera fase se enfoca en la aplicación del ciclo de mejora continua PHVA (ciclo Deming), concebido como la **herramienta metodológica transversal a toda norma ISO** y, en este caso en particular, a los estándares ISO/IEC 27001 e ISO/IEC 20000-1. Este ciclo constituye la estructura central sobre la cual se organizan los sistemas de gestión, al proporcionar un proceso iterativo y secuencial que facilita la integración de múltiples marcos normativos.

De manera complementaria, las normas ISO modernas comparten la denominada Estructura de Alto Nivel (HLS, High Level Structure), definida en el Anexo SL. Esta estructura establece un marco común de capítulos, cláusulas y terminología que garantiza que todas las normas de gestión hablen un mismo “idioma organizacional”. Gracias a esta homogeneidad, las organizaciones pueden iniciar la integración de nuevos estándares afines a su propósito con una ventaja aproximada del 50% sobre lo ya desplegado. En particular, los requisitos relacionados con el contexto de la organización,

liderazgo, planificación, soporte, evaluación del desempeño y mejora alcanzan una integración global superior al 75%, lo que facilita su implementación conjunta dentro de un sistema integrado de gestión. El mayor desafío se encuentra en la operación, núcleo de cada norma, que debe ajustarse de manera estratégica a las necesidades y objetivos específicos de cada organización.

Este nivel de integración reduce duplicidades, aprovecha sinergias y posibilita una gestión más eficiente y coherente. A su vez, el ciclo no solo establece una secuencia lógica de implementación, sino que también asegura que los sistemas evolucionen mediante la retroalimentación continua derivada de actividades de monitoreo, revisión, medición, métricas y auditorías. [53] En este sentido, se trata de estándares que, al apoyarse en el ciclo de Deming y la HLS, consolidan la mejora del diseño y la implementación de los sistemas de gestión. Así, aplicado de manera conjunta, se convierte en el pilar que fortalece la integración entre la gestión de la seguridad de la información y la gestión de servicios de TI garantizando coherencia, sostenibilidad y orientación a la mejora permanente.

En este sentido, la combinación entre la HLS y el ciclo PHVA constituye la columna vertebral de los sistemas de gestión ISO: la primera aporta una estructura común y transversal que permite integrar cualquier norma afín con los objetivos de la organización, mientras que el segundo proporciona la metodología de mejora continua que asegura que dichas normas evolucionen de manera coherente, sostenible y orientada a resultados medibles.

A continuación, en la ilustración No. 5 se presenta en síntesis las fases del ciclo y su aplicación en el marco del sistema integrado:

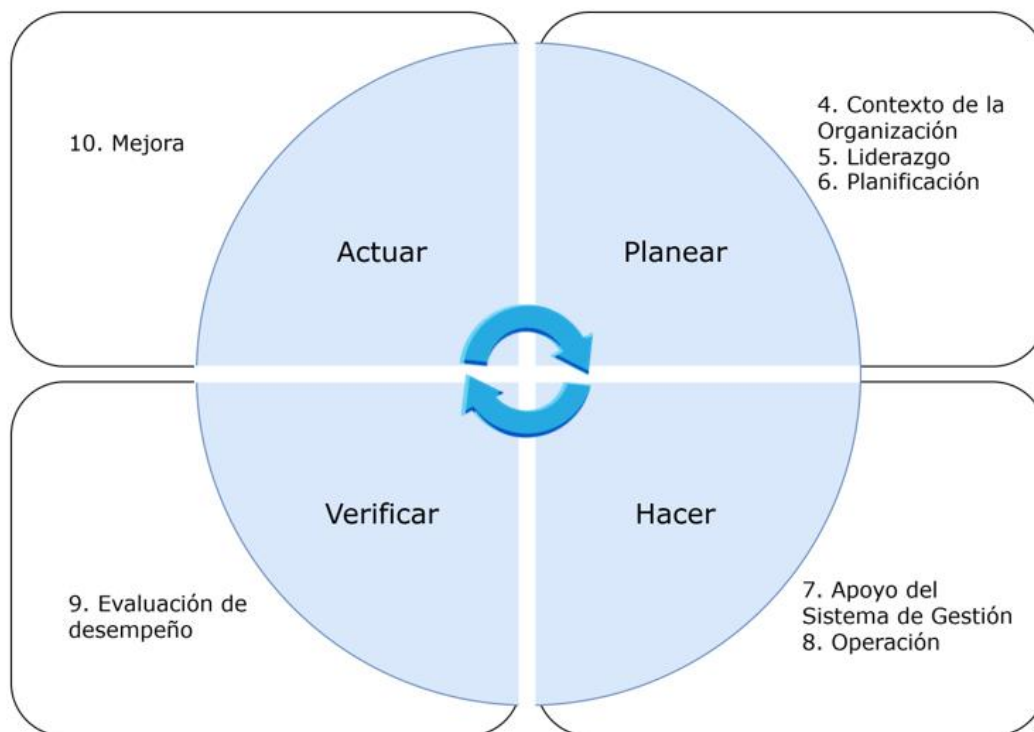


Ilustración 5. Ciclo PHVA aplicado en la integración de las normas ISO.

Cada fase del PHVA cumple una función estratégica:

- **Planear**, donde se definen el contexto, los objetivos, procesos y procedimientos necesarios para alinear la gestión integrada de TI con las necesidades estratégicas de la organización.
- **Hacer**, en el que se ejecutan las acciones y procesos planificados; desplegando controles, procesos de entrega de servicios, actividades de gestión operativa, así como programas de capacitación y concienciación. Aquí se materializa la puesta en marcha de los requisitos documentados en ambos sistemas.
- **Verificar**, orientado a la medición, monitoreo y evaluación del desempeño frente a los requisitos; se emplean indicadores de desempeño, revisiones de cumplimiento, informes de auditoría interna y revisiones por la dirección para determinar el grado de efectividad.
- **Actuar**, que impulsa las acciones correctivas y de mejora continua.

3.2. Fase II: Propuesta metodológica. Sistema Integrado de Gestión de tecnologías de la información basado en las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018

La segunda fase de este trabajo se encuentra orientada a dar respuesta al objetivo general mediante la construcción de una propuesta metodológica para el diseño de un sistema integrado de gestión. Esta fase se fundamenta en el ciclo de mejora continua PHVA, reconocido como una herramienta eficaz para estructurar, implementar y optimizar sistemas de gestión en el marco de estándares internacionales.

En esta sección se presentan de manera detallada las cuatro etapas del ciclo PHVA, adaptadas al contexto de integración entre las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018. Cada etapa no solo define actividades y lineamientos metodológicos, sino que también plantea los puntos clave que deben ser considerados en el despliegue del sistema integrado, resaltando los elementos críticos para asegurar la coherencia entre la gestión de la seguridad de la información y la gestión de los servicios de TI.

Adicionalmente, se incorporan ejemplos teóricos y prácticos que ilustran cómo pueden aplicarse estas pautas en escenarios organizacionales, brindando así una guía clara para orientar a las empresas en el desarrollo posterior de sus instructivos, procedimientos y formatos. Los numerales normativos aplicables se encuentran distribuidos en cada una de las fases del ciclo PHVA, lo cual permite visualizar de manera estructurada los requisitos mandatorios que deben cumplirse y su correspondencia con las actividades metodológicas propuestas.

3.2.1. Etapa I: Planear

La etapa **planear** representa el punto de partida estratégico para el despliegue de un Sistema Integrado de Gestión que está diseñado para articular los requisitos normativos de los estándares de seguridad de la información y gestión de los servicios de TI. En esta etapa, la organización define y articula de forma clara las actividades de planificación bajo una perspectiva de mejora continua y gestión basada en riesgos, alineada con las bases del ciclo Deming, donde el "Plan" implica "analizar y evaluar la situación existente, identificar oportunidades de mejora y establecer objetivos que guían los cambios propuestos" [54]

El éxito de la implementación del Sistema Integrado de Gestión depende directamente de la claridad y profundidad con que se estructuren los componentes de esta etapa. De ella emergen las políticas institucionales, el alcance del sistema, las directrices estratégicas y los objetivos tácticos, que orientarán el comportamiento organizacional y el despliegue de procesos robustos. Para facilitar su desarrollo, esta etapa se organiza en las siguientes actividades clave:

3.2.1.1. Comprensión de la Organización y su contexto.

La comprensión del contexto organizacional constituye el fundamento analítico del sistema integrado de gestión y se orienta a determinar, qué factores internos y externos condicionan la capacidad de la entidad para alcanzar resultados coherentes con su estrategia y con los requisitos de seguridad de la información y gestión de servicios de TI. En ambos estándares, esta exigencia implica identificar cuestiones pertinentes (tanto favorables como desfavorables) que puedan influir en el logro de objetivos, en la efectividad de los procesos y en la continuidad de los servicios, de modo que la planeación posterior no sea una declaración abstracta, sino un plan situado en la realidad del negocio y sus riesgos. La lectura del contexto, por tanto, se convierte en una explicación razonada de dónde está hoy la organización, hacia dónde pretende llegar y en qué condiciones debe operar para cumplir sus propósitos.

Para sostener esta comprensión, se elabora un documento formal para el levantamiento del Contexto Organizacional y elementos de Gestión del Sistema Integrado que contempla unas actividades bases para el cumplimiento normativo de ambos estándares.

La primera es la plataforma estratégica, donde se describe de forma clara la identidad organizacional: una presentación introductoria que explique el ámbito de operación, la misión y la visión como referentes de dirección, los valores que orientan la conducta corporativa, el propósito general y la estructura organizacional que da soporte a la toma de decisiones y a la prestación de servicios TI. Esta plataforma no se limita a proclamas; debe mostrar coherencia entre el modelo de negocio, la proposición de valor para clientes internos y externos, y las expectativas normativas y regulatorias que le aplican. Dentro de esta se contempla una explicación de la relevancia de la confidencialidad, integridad y disponibilidad de la información para la propuesta de valor; así como la conexión con la calidad y confiabilidad de los servicios, la experiencia del usuario y los compromisos de niveles de servicio.

La segunda capa profundiza en el análisis del entorno y su impacto en el sistema. Aquí se integran, en una narrativa unificada, los factores externos (regulatorios, tendencias del mercado, evolución tecnológica, ciberamenazas relevantes, dependencia de terceros, entre otros) y los factores internos (madurez de procesos, cultura y competencias, capacidad y continuidad, gobernanza y experiencia previa en seguridad y gestión de servicios). Este análisis no es meramente descriptivo: debe explicar causalmente cómo cada factor condiciona los resultados del Sistema Integrado de Gestión.

La tercera capa consolida la justificación de la implementación del Sistema Integrado de Gestión y la alineación estratégica aprobada por la alta dirección. En este punto, el documento debe articular por qué la organización decide integrar los estándares y qué beneficios y necesidades atiende: reducción de eventos de seguridad y de indisponibilidades, cumplimiento regulatorio, mejora en tiempos de respuesta y en niveles de servicio, Reducción de costos de operación, confianza del cliente y habilitación de oportunidades de negocio. Asimismo, se expone cómo las partes interesadas influyen en el diseño del sistema, señalando sus requisitos explícitos e implícitos y la forma en que estos se traducen en criterios de desempeño y controles. Esta justificación debe presentar una línea de trazabilidad entre las expectativas de las partes interesadas, la realidad del contexto y las decisiones de diseño del Sistema Integrado de Gestión.

3.2.1.2. Definición del alcance del sistema integrado.

La definición del alcance constituye un elemento esencial en la estructuración del Sistema Integrado de Gestión, en tanto delimita con claridad los procesos, servicios, activos y áreas de la organización que estarán cobijados bajo el sistema, garantizando así que los objetivos estratégicos, los compromisos de seguridad de la información y las obligaciones de gestión de servicios se apliquen dentro de un marco verificable y controlado. La ausencia de una definición precisa podría generar ambigüedades que afecten el cumplimiento de los requisitos normativos o generen vacíos de responsabilidad frente a las partes interesadas.

Ambos marcos normativos establecen que el alcance debe determinarse considerando simultáneamente los procesos organizacionales y de TI que soportan la propuesta de valor, los servicios que se prestan, los activos de información que requieren protección, las obligaciones regulatorias y contractuales que condicionan la operación y, de manera fundamental, las necesidades y expectativas de las partes interesadas. En consecuencia, definir el alcance no puede entenderse como un trámite administrativo, sino como el resultado de integrar el diagnóstico contextual de la organización con las decisiones estratégicas de la alta dirección, materializando en un documento formal los límites del sistema y las responsabilidades asociadas a su implementación.

Para establecer estos límites resulta indispensable fijar criterios objetivos que permitan determinar qué procesos, servicios y activos se encuentran incluidos o excluidos. Dichos criterios abarcan aspectos como:

- La cobertura organizacional, donde se debe especificar si el sistema aplica a toda la entidad, a determinadas unidades de negocio o a sedes específicas;
- La cobertura de servicios, donde se identifican los que forman parte del Sistema Integrado de Gestión y aquellos que se excluyen con justificación verificable;
- La cobertura de activos de información, que detalla los sistemas, plataformas, infraestructuras y aplicaciones críticas; y

- La relación con proveedores y terceros, aclarando si los servicios contratados están bajo el alcance y en qué condiciones se gestionan los riesgos derivados.

Esta delimitación del alcance no puede desligarse del análisis de contexto ni de la identificación de las necesidades y expectativas de las partes interesadas. Los requisitos deben traducirse en criterios de inclusión que orienten la definición del sistema. En este sentido, el alcance funciona como el puente entre lo que las partes interesadas demandan y lo que la organización se compromete a garantizar bajo estándares internacionales.

La evidencia documental del alcance debe plasmarse en un documento oficial aprobado por la alta dirección. Este debe contener una declaración formal donde se describan procesos, servicios, activos, ubicaciones y funciones incluidas, así como las exclusiones justificadas que expliquen por qué determinados elementos no forman parte del sistema y cómo ello no compromete el logro de los objetivos. Además, debe incorporar un mapa de trazabilidad que vincule a las partes interesadas, los requisitos relevantes y los procesos o servicios que los atienden, asegurando así la coherencia entre lo que se declara y lo que se gestiona. La aprobación ejecutiva de este documento representa la validación final de que el alcance definido refleja tanto la estrategia como la realidad operativa de la organización.

Finalmente, el ANEXO C: instructivo para el levantamiento del contexto organizacional y elementos de gestión del sistema integrado, en su quinto apartado, constituye una guía práctica para el proceso de definición del alcance, al permitir estructurar de manera clara diferentes factores para su definición. Dicho documento se convierte en la evidencia operativa que complementa la declaración formal del alcance y facilita la auditoría de la consistencia entre lo planificado y lo ejecutado.

3.2.1.3. Liderazgo y compromiso de la alta dirección.

La consolidación del Sistema Integrado de Gestión depende en gran medida, del liderazgo ejercido por la alta dirección, por medio de sus decisiones y apoyo estratégico se asegura la eficacia del sistema. El compromiso de los niveles directivos no se limita a una declaración formal de intenciones, sino que se materializa en la capacidad de alinear

la política y los objetivos del sistema con la dirección estratégica de la organización, garantizando que el Sistema Integrado de Gestión no opere como un ente aislado, sino como un engranaje integrado en la dinámica organizacional.

El liderazgo se expresa a partir de la incorporación de los requisitos del sistema de gestión en los procesos de la organización. Este paso supone un ejercicio de transversalidad, en el cual las prácticas del Sistema Integrado de Gestión se convierten en parte de la operación cotidiana, evitando que se perciban como cargas adicionales. En este sentido, se garantiza la disponibilidad de recursos financieros, tecnológicos y humanos necesarios para mantener la operatividad y mejorar continuamente el desempeño del sistema.

La alta dirección debe también comunicar la importancia de una gestión eficaz, transmitiendo a todos los niveles de la organización la relevancia de cumplir con los requisitos, entregar valor y asegurar resultados consistentes. Esta comunicación no es un acto simbólico, sino un proceso de retroalimentación constante que refuerza la cultura organizacional orientada a la calidad, la seguridad y la sostenibilidad.

El compromiso directivo se refleja en la capacidad de asegurar el logro de los resultados previstos, lo cual implica establecer mecanismos de monitoreo, medición y control que permitan verificar la eficacia del sistema. Adicionalmente, la alta dirección tiene la responsabilidad de dirigir y apoyar a las personas, fomentando su participación, fortaleciendo sus competencias y motivándolas a contribuir al mejoramiento continuo.

Dentro de este liderazgo, resulta imprescindible la promoción de la mejora continua como principio rector. La alta dirección no debe limitarse a mantener el sistema en funcionamiento, sino impulsar constantemente su perfeccionamiento, identificando oportunidades, gestionando riesgos y adaptándose a las transformaciones del entorno.

Asimismo, la demostración de compromiso incluye apoyar otras funciones de gestión, generando sinergias con las diferentes áreas organizacionales y asegurando que el Sistema Integrado de Gestión tenga un alcance integral. Este rol articulador refuerza la visión de un sistema que trasciende la sumatoria de procesos, para convertirse en una plataforma estratégica que soporta la creación de valor.

3.2.1.4. Política del Sistema Integrado de Gestión.

La política integrada de gestión constituye la declaración formal de la alta dirección en la que se expresa la orientación estratégica de la organización frente a la calidad, la gestión del servicio y la seguridad de la información. Esta política no es un documento aislado, sino que se configura como el marco rector sobre el cual se fundamenta el Sistema Integrado de Gestión, siendo coherente con el propósito, la misión y la visión institucional.

Una política de gestión debe ser apropiada para el propósito de la organización, lo que implica que debe reflejar las particularidades del sector en el que esta ópera, los productos o servicios que ofrece y el valor agregado que entrega a sus clientes y demás grupos de interés. Asimismo, debe evidenciar la inclusión del compromiso de satisfacer los requisitos aplicables. Esto abarca no solo el cumplimiento de la normatividad legal vigente, sino también de las obligaciones contractuales, regulatorias y de las disposiciones establecidas en los estándares internacionales que sustentan el Sistema Integrado de Gestión. De igual forma, la política debe expresar de manera explícita el compromiso de mejora continua, entendido como la disposición permanente de la organización a identificar oportunidades de optimización en sus procesos, incorporar prácticas innovadoras y adaptarse a los cambios del entorno, asegurando así su sostenibilidad y competitividad en el largo plazo.

En la ilustración No. 6 se plantean las necesidades que deben ser resueltas en ambos sistemas para definir de forma global una política integrada.

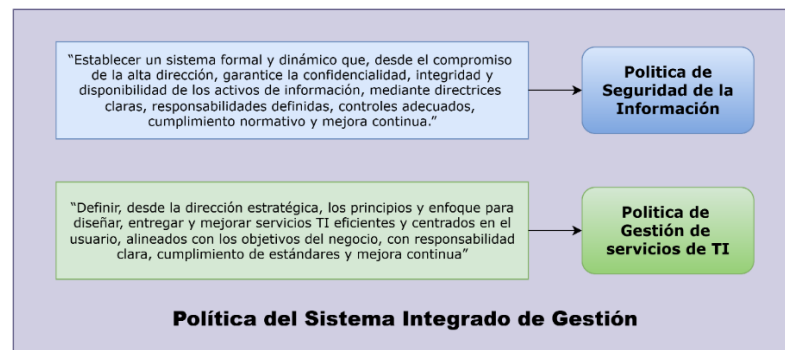


Ilustración 6. Integración de las políticas de Seguridad de la Información y Gestión del servicio. Fuente: Elaboración propia

En lo que respecta a su comunicación, la política debe estar disponible como información documentada dentro del sistema, de manera que se mantenga accesible, actualizada y debidamente controlada. Además, es responsabilidad de la organización asegurar que esta política sea comunicada en todos los niveles, promoviendo que los colaboradores la comprendan, la apliquen y la asuman como parte integral de su trabajo. Finalmente, debe ponerse a disposición de las partes interesadas externas, según corresponda, garantizando transparencia y consolidando la confianza en la capacidad de la organización para gestionar de manera eficaz la calidad, el servicio y la seguridad de la información.

3.2.1.5. Objetivos compatibles con la dirección estratégica.

Los objetivos definidos en la etapa de planeación del Sistema Integrado de Gestión constituyen la base para garantizar la coherencia entre los compromisos normativos, las expectativas de las partes interesadas y los lineamientos estratégicos de la organización. Su propósito es asegurar tanto la protección de la información como la excelencia en la prestación de los servicios, consolidando la confianza de clientes, usuarios y aliados.

En concordancia con los principios de planificación, los objetivos deben ser coherentes con la política de gestión, ser medibles siempre que sea posible, considerar los requisitos aplicables y los resultados de la evaluación y tratamiento de riesgos, además de ser monitoreados, comunicados y actualizados según se requiera. La organización debe conservar esta información documentada, garantizando su disponibilidad para los niveles y funciones pertinentes.

Para lograr estos objetivos, la planificación establece de manera clara qué se hará, qué recursos serán necesarios, quién será el responsable de cada acción, en qué plazos se completarán las actividades y cómo se evaluarán los resultados. Este enfoque asegura que la gestión sea transparente, verificable y orientada a la mejora continua.

Asimismo, cuando la organización determine la necesidad de realizar cambios en el sistema, éstos deberán planificarse adecuadamente para garantizar que la seguridad de la información y la continuidad de los servicios no se vean comprometidas. Dichos cambios se alinean con la política de gestión de servicios y con los objetivos estratégicos definidos, manteniendo un control efectivo sobre su implementación.

De manera complementaria, la gestión de servicios requiere un plan específico que considere una lista de servicios, las limitaciones conocidas, las obligaciones legales y contractuales, las responsabilidades asociadas, los recursos necesarios, la tecnología de soporte y el enfoque de trabajo con otras partes interesadas. Adicionalmente, se debe establecer cómo se medirá, auditará e informará la eficacia del sistema, asegurando que los resultados se traduzcan en valor para los usuarios y en sostenibilidad para la organización.

En conjunto, estos objetivos y planes garantizan que la seguridad de la información y la gestión de servicios evolucionen de manera integrada, contribuyendo a fortalecer la eficiencia operativa, gestionar adecuadamente los riesgos y consolidar la confianza de las partes interesadas.

3.2.1.6. Disponibilidad de recursos y orientación a la mejora continua.

La disponibilidad de recursos y la orientación a la mejora continua representan un eje fundamental dentro del Sistema Integrado de Gestión, ya que garantizan que la organización cuente con las capacidades necesarias para implementar, operar y mantener los procesos de seguridad de la información y gestión de servicios de TI de manera efectiva. La alta dirección, en cumplimiento de los requisitos normativos, debe asegurar que los recursos humanos, tecnológicos, financieros y de conocimiento estén disponibles en la medida adecuada, de modo que se cubran tanto las necesidades actuales como las proyecciones de evolución del sistema. Esta disponibilidad no se limita a la provisión de personal o infraestructura, sino que implica también la asignación de competencias específicas, la creación de programas de formación y concienciación, y la implementación de herramientas que fortalezcan el desempeño y la seguridad de los servicios.

El compromiso con la mejora continua debe integrarse como un principio rector en esta gestión, de manera que los recursos no solo sirvan para sostener la operación cotidiana, sino que habiliten la innovación, la prevención de incidentes y la capacidad de respuesta ante los cambios del entorno. Para ello, resulta indispensable que la organización establezca mecanismos de evaluación periódica de la suficiencia y eficacia de los recursos, promueva la retroalimentación en todos los niveles, documente lecciones

aprendidas y mantenga un ciclo de revisión que permita identificar oportunidades de optimización.

3.2.1.7. Riesgos y oportunidades.

En la planificación de un sistema integrado de gestión, la identificación de riesgos y oportunidades se convierte en un ejercicio estratégico que permite anticipar los factores que pueden facilitar o limitar el logro de los resultados previstos. Este análisis no solo contribuye a prevenir efectos no deseados, sino que también garantiza la orientación hacia la mejora continua, lo cual es esencial para la sostenibilidad del sistema en el tiempo. En este marco, resulta necesario reconocer que la gestión de riesgos no se limita a una acción correctiva posterior, sino que constituye un proceso preventivo y dinámico que orienta la toma de decisiones.

Un primer conjunto de riesgos está vinculado directamente con la organización y su capacidad de adaptación al cambio. En la práctica, la resistencia de los colaboradores y de la alta dirección frente a nuevas políticas, controles o procedimientos suele ser un obstáculo recurrente, pues genera barreras culturales que dificultan la implementación del sistema. Este fenómeno se intensifica cuando los cambios no son comunicados de manera clara o cuando no se logra demostrar a los miembros de la organización el valor agregado de las nuevas prácticas. Asimismo, la existencia de fricciones en la comunicación interdepartamental representa un riesgo latente, ya que la falta de coordinación puede derivar en duplicidad de esfuerzos, retrasos en la ejecución de actividades e incluso en contradicciones dentro de los procesos. Del mismo modo, la asignación insuficiente de recursos —sean financieros, tecnológicos o humanos— limita la capacidad de respuesta de la organización, afectando la efectividad y la continuidad del sistema de gestión.

Otro grupo de riesgos está asociado con el cumplimiento de los requisitos del servicio. La ausencia de una formación adecuada en normas y procedimientos puede conducir a errores que comprometan la organización en el marco de exigencias regulatorias. En contextos donde no existen metodologías estandarizadas, el riesgo se materializa en retrasos, reprocesos y posibles incumplimientos, generando una percepción negativa por parte de los clientes. A esto se suma la dependencia de proveedores externos, la cual, si

no se gestiona mediante mecanismos de control, puede poner en riesgo la calidad y la seguridad de los servicios. Este escenario muestra que los riesgos relacionados con el servicio no solo afectan la operación, sino también la confianza que los clientes depositan en la organización.

Los riesgos también surgen de la relación con las partes interesadas. La baja participación de usuarios en procesos de retroalimentación reduce la capacidad de la organización para ajustar sus servicios a las necesidades reales del entorno. Asimismo, cuando existe desalineación entre las expectativas de los clientes y el alcance de los servicios, se incrementa la posibilidad de insatisfacción, lo que impacta la reputación institucional y el valor percibido. En consecuencia, gestionar estos riesgos implica diseñar mecanismos de comunicación efectivos, orientados a garantizar que las expectativas sean comprendidas y gestionadas desde el inicio del ciclo de vida del servicio.

Ahora bien, el análisis de riesgos no se limita a señalar amenazas, sino que también permite identificar oportunidades que fortalecen la gestión organizacional. Entre ellas, se encuentra la posibilidad de aumentar la confianza de clientes, aliados y entes reguladores mediante la certificación en normas internacionales, lo que refuerza la credibilidad y la competitividad en el mercado. De igual manera, la estructuración de procesos alineados con estándares reconocidos abre el camino hacia el fortalecimiento de una cultura organizacional enfocada en la seguridad de la información y en la gestión eficiente de los servicios. Esta cultura, a su vez, fomenta la innovación, impulsa la integración de las áreas y favorece la optimización de recursos. Así, la organización no solo cumple con los requisitos normativos, sino que también genera ventajas competitivas sostenibles que mejoran su posición en el sector.

En conclusión, la identificación de riesgos y oportunidades constituye un elemento clave para la planificación del sistema de gestión. Este ejercicio, además de anticipar escenarios adversos, permite trazar un horizonte de mejora que, al integrarse en los procesos organizacionales, asegura que las acciones emprendidas no sean reactivas, sino preventivas y estratégicas. De este modo, la organización logra consolidar un sistema que no solo responde a las exigencias normativas, sino que también se proyecta como un mecanismo de aprendizaje y fortalecimiento institucional.

3.2.1.8. Gestión de riesgos y aplicación de controles.

La gestión de riesgos y la aplicación de controles constituye un componente esencial en la planificación y operación de un Sistema Integrado de Gestión, dado que permite identificar, analizar y tratar aquellos factores que pueden comprometer el logro de los resultados previstos. En coherencia con los lineamientos de la ISO 31000:2018, la organización debe abordar los riesgos de manera integral, considerando tanto su contexto interno como externo, el análisis de partes interesadas y los requisitos normativos, contractuales y regulatorios que resultan aplicables. Este enfoque asegura que la gestión de riesgos se convierta en un proceso sistemático y permanente, que no solo prevenga la ocurrencia de incidentes, sino que también oriente la toma de decisiones estratégicas.

En este marco, la ISO 31000:2018 propone un proceso estructurado para la gestión de riesgos que permite abordar de manera sistemática todas las fases necesarias para su control y tratamiento. A continuación, en la ilustración No. 7 y No. 8 se presenta gráficamente este modelo, donde se observa cómo cada fase interactúa de forma dinámica con el entorno organizacional, generando registros que respaldan la toma de decisiones y la mejora continua:

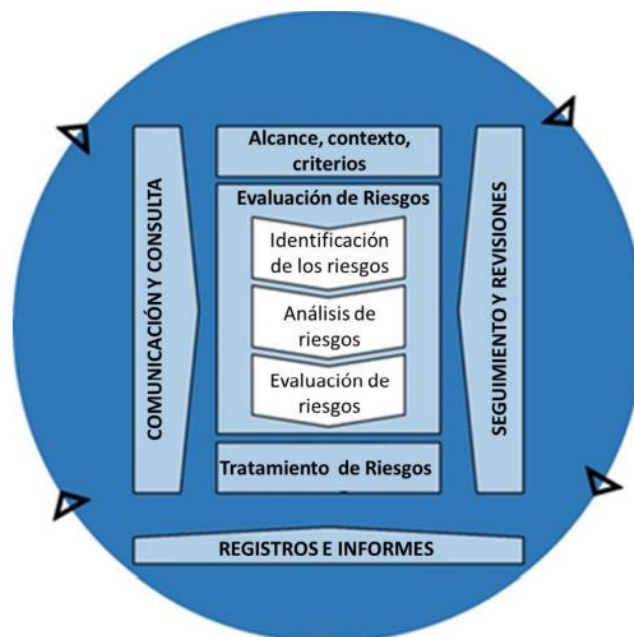


Ilustración 7. Proceso de gestión de riesgos. Fuente: Adaptado de [46]

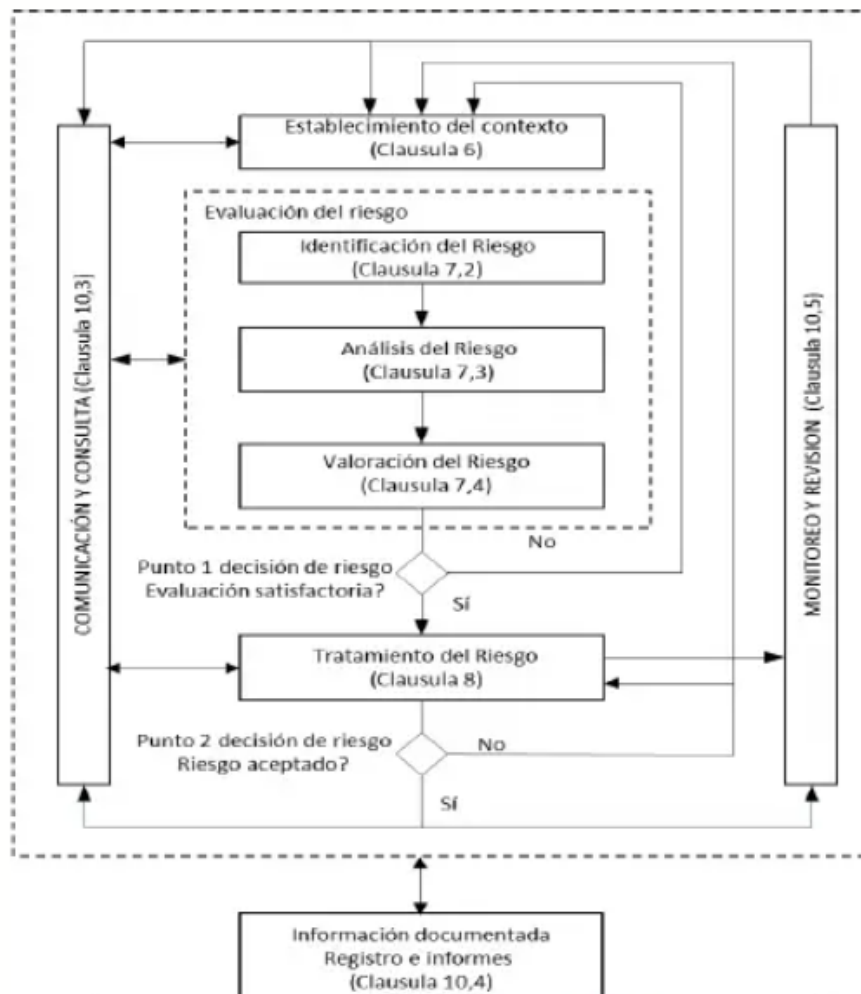


Ilustración 8. Proceso de gestión de riesgos para la seguridad de la información. Fuente: Adaptado de [55]

La ISO 31000:2018 establece un marco genérico y flexible que se adapta a cualquier tipo de organización, proponiendo un proceso estructurado que abarca la identificación, el análisis, la evaluación, el tratamiento, el monitoreo y la comunicación de los riesgos. Cada una de estas fases se integra con la gestión global de la organización, aportando evidencia documentada y fomentando la trazabilidad de las decisiones. Sin embargo, cuando se abordan riesgos específicos de seguridad de la información, resulta necesario complementar este marco con la orientación de la ISO/IEC 27005:2022, norma que desarrolla metodologías detalladas para la gestión de riesgos en el contexto de un SGSI. [55]

La ISO/IEC 27005 aporta un enfoque especializado que facilita la identificación de activos de información, la evaluación de amenazas y vulnerabilidades, y la estimación del impacto potencial de incidentes que comprometan la confidencialidad, la integridad o la disponibilidad de la información. Esta aproximación no se limita únicamente a la seguridad de la información, sino que puede aplicarse de manera transversal en la identificación y análisis de riesgos en la gestión de servicios, dado que muchas amenazas tecnológicas y organizacionales tienen implicaciones directas en la continuidad y calidad del servicio. Así, riesgos como accesos no autorizados, pérdida de datos críticos o interrupciones en la infraestructura tecnológica deben ser valorados y tratados mediante controles proporcionales, en concordancia con los lineamientos de la ISO/IEC 27001 y en estrecha relación con las buenas prácticas de la gestión de servicios.

3.2.1.8.1. Planificación de acciones para abordar riesgos

El punto de partida radica en la planificación de las acciones necesarias para abordar dichos riesgos. Esto supone no solo definir las medidas que mitiguen amenazas, sino también aquellas que permitan capitalizar escenarios positivos, integrando estas acciones de manera efectiva dentro de los procesos del sistema de gestión. La eficacia de dichas medidas debe ser objeto de evaluación continua, asegurando que no queden como ejercicios documentales, sino que generen resultados verificables en la práctica. En este contexto, la ISO 31000 y la ISO/IEC 27005 coinciden en que las organizaciones pueden optar por diferentes estrategias como evitar riesgos, asumirlos con fundamento en decisiones informadas, transferirlos a terceros, reducirlos mediante controles o incluso incrementar su exposición cuando se traduzca en nuevas oportunidades de negocio o innovación.

La primera actividad de esta planificación corresponde al establecimiento del contexto, el alcance y los criterios de riesgos. Aquí la organización debe comprender cuáles son sus objetivos estratégicos y cómo la gestión del riesgo contribuye a alcanzarlos. Se requiere delimitar el alcance de la evaluación, definiendo los procesos, activos de información, servicios y partes interesadas que deben ser considerados, ya que la seguridad y la calidad de los servicios se ven afectadas tanto por factores internos como externos. A partir de esta definición se construyen los criterios de valoración, que permiten medir la

probabilidad y el impacto de los eventos, así como los umbrales de tolerancia y aceptación del riesgo. Estos criterios se convierten en una guía para evaluar, priorizar y decidir sobre las acciones de tratamiento.

Definición de criterios para la identificación de riesgos

De acuerdo con la norma, las organizaciones deben establecer de forma clara los riesgos que están dispuestas a aceptar y los criterios con los que evaluarán su relevancia. Dichos criterios han de alinearse con el marco de gestión de riesgos y reflejar tanto los valores y objetivos institucionales como las obligaciones regulatorias y las expectativas de las partes interesadas. A continuación, en la tabla No. 8 se presentan los aspectos clave sugeridos por el estándar para su definición:

Elementos para definir criterios de riesgo	Descripción
Naturaleza y tipos de incertidumbre	Analizar qué factores tangibles e intangibles pueden afectar los resultados.
Definición y medición de consecuencias y probabilidad	Determinar cómo se mide el impacto (positivo o negativo) y su probabilidad de ocurrencia.
Factores relacionados con el tiempo	Considerar horizontes temporales en los que el riesgo puede manifestarse o cambiar.
Coherencia en las mediciones	Establecer un método uniforme de valoración para evitar interpretaciones dispares.
Determinación del nivel de riesgo	Definir criterios que permitan clasificar y priorizar el nivel de los riesgos identificados.
Combinaciones y secuencias de riesgos	Analizar efectos acumulados o encadenados de múltiples riesgos.
Capacidad de la organización	Reconocer los recursos, límites y fortalezas institucionales para gestionar los riesgos.

Tabla 8. Elementos para definir criterios de riesgo. Elaboración, basada en [46]

Definición de parámetros de calificación

Una vez definido el marco de referencia, la organización procede a establecer con precisión los criterios de consecuencia y de probabilidad, cuyo propósito es orientar a los propietarios del riesgo en la decisión sobre su retención o tratamiento, así como en la asignación de prioridades para su gestión [55]. En este sentido, la **probabilidad** se concibe como la posibilidad de que un evento adverso se materialice en un periodo y contexto determinados, mientras que la **consecuencia** o impacto describe los efectos que dicho evento tendría sobre los objetivos de seguridad de la información y de los

servicios. Ambos criterios forman un binomio inseparable: la probabilidad aporta la medida de ocurrencia, y el impacto define la magnitud de las repercusiones, de modo que su combinación orienta la valoración integral del riesgo. [37] Para asegurar consistencia, ambos conceptos deben parametrizarse mediante escalas explícitas y deben ser aplicables tanto de forma cualitativa como cuantitativa.

Operativamente, el nivel de riesgo se modela habitualmente como el producto:

$$R = P * I$$

Donde **P** es la probabilidad estimada e **I** representa el impacto acumulado sobre dimensiones clave del Sistema Integrado de Gestión, como confidencialidad, integridad, disponibilidad, cumplimiento normativo o cumplimiento del nivel de servicio (SLA).

La probabilidad puede expresarse en diferentes formas, desde escalas cualitativas (muy baja – muy alta), hasta enfoques semicuantitativos (1–5) o plenamente cuantitativos con tasas de ocurrencia; mientras que el impacto, por su parte, puede medirse en términos monetarios (pérdida esperada), horas de indisponibilidad, severidad regulatoria, deterioro en indicadores de servicio o niveles de afectación sobre la triada en seguridad de la información.

Sobre esta base, la identificación de escenarios de riesgo deja de ser una lista de amenazas genéricas y se convierte en narrativas verificables que describen la cadena: “activo o servicio, vulnerabilidad, amenaza o evento desencadenante y consecuencia identificable”. Cada escenario debe identificar:

- (i) el activo o servicio afectado,
- (ii) la condición de vulnerabilidad,
- (iii) la amenaza que puede explotar dicha vulnerabilidad y
- (iv) las consecuencias sobre seguridad y servicio.

En este punto cobra relevancia el concepto de vulnerabilidad como medida relativa de exposición. Pudiéndose expresar matemáticamente así:

$$V = \frac{P * I}{I_{m\acute{a}x}}$$

donde $I_{m\acute{a}x}$ es el máximo impacto definido por la organización como su umbral crítico o límite superior de daño aceptable. De esta manera, la vulnerabilidad se sitúa en un rango entre 0 y 1, lo que permite establecer criterios de priorización: mientras más cercano a 1 se ubique un escenario, mayor será su criticidad y más urgente el tratamiento. Además, al integrarse con los criterios de aceptación del riesgo, facilita decisiones basadas en métricas claras y comparables, evitando la subjetividad.

Es útil diferenciar entre vulnerabilidad inherente (antes de controles) y residual (después de controles), una distinción clave en la literatura sobre ISO/IEC 27005 y en desarrollos académicos como los del autor Valencia [41], quien insiste en contextualizar escenarios con control tecnológico y organizacional.

Con todos los escenarios caracterizados, se definen los criterios de aceptación del riesgo que discernirán si se acepta, mitiga, transfiere o evita un riesgo. Estos criterios deben alinearse según los estándares de aceptación y los niveles de tolerancia establecidos por la alta dirección, respetando límites innegociables (como normativa o contratos).

3.2.1.8.2. Evaluación de riesgos

Una vez que la organización ha definido los parámetros y criterios que guían la gestión del riesgo, el siguiente paso lógico es la evaluación misma. Esta fase no se limita únicamente a identificar amenazas y vulnerabilidades, sino que busca estimar y calificar el riesgo en función de lo previamente establecido. En este sentido, la evaluación de riesgos actúa como un puente entre la teoría y la práctica: se ponen a prueba los criterios definidos, se mide la probabilidad y el impacto de los eventos, y se determinan los niveles de riesgo que orientarán las decisiones futuras. De esta manera, se garantiza que la gestión no se base en percepciones subjetivas, sino en un proceso estructurado y replicable, cumpliendo con los requisitos normativos de coherencia, validez y comparabilidad.

La estimación del riesgo comienza con la identificación de escenarios que puedan afectar la confidencialidad, integridad y disponibilidad de la información. Una vez identificados, se evalúan sus consecuencias potenciales y la probabilidad de materialización. Esta combinación permite determinar el nivel de riesgo, lo cual aporta una visión clara de qué

tan expuesta se encuentra la organización frente a cada amenaza. Aquí es donde cobra relevancia el concepto de riesgo inherente, entendido como el nivel de exposición antes de aplicar cualquier medida de control. [37] El riesgo inherente refleja la vulnerabilidad real del sistema ante la amenaza, y sirve como línea base para dimensionar el esfuerzo requerido en el tratamiento posterior.

Definición de controles

Una vez establecido el riesgo inherente como la exposición inicial que enfrenta la organización antes de aplicar medidas de protección, el paso siguiente consiste en determinar y seleccionar los controles más adecuados para disminuir esa vulnerabilidad. Los controles son medidas técnicas, organizativas o procedimentales que actúan como barreras para reducir la probabilidad de que un riesgo se materialice o, en su defecto, mitigar su impacto sobre los procesos y activos críticos. [37] La correcta definición de controles constituye un elemento esencial del Sistema Integrado de Gestión, ya que su efectividad impacta directamente en el nivel de riesgo residual.

En materia de seguridad de la información, la norma ISO/IEC 27002 proporciona un catálogo de 93 controles, organizados en cuatro grandes categorías: controles organizacionales, controles relacionados con las personas, controles físicos y controles tecnológicos. Estos controles, que se detallan en el Anexo A de la norma, abarcan aspectos como la definición de políticas de seguridad, la gestión de accesos, el uso de criptografía, la seguridad física de instalaciones, la continuidad de la información y la protección en entornos tecnológicos, entre otros. Constituyen una guía práctica para que las organizaciones estructuren su estrategia de protección, seleccionando aquellos controles más pertinentes según los riesgos identificados y el contexto particular de su operación.

Por su parte, en el ámbito de la gestión de servicios, marcos como ISO/IEC 20000 o ITIL orientan la definición de controles relacionados con la calidad de la prestación, la continuidad de los servicios, la gestión de incidentes y problemas, o el cumplimiento de los acuerdos de nivel de servicio (ANS). De esta manera, el diseño de controles se adapta a las particularidades de cada dimensión del sistema, garantizando una cobertura integral de los riesgos identificados.

La selección de los controles no puede hacerse de manera aislada ni genérica. Para que sean pertinentes, es necesario determinar con claridad qué variable del riesgo mitigan: si la probabilidad de ocurrencia del evento, o el impacto de sus consecuencias en caso de materialización. Esta distinción permite articular los controles de manera estratégica, priorizando aquellos que inciden directamente sobre los escenarios de mayor criticidad.

Una vez definidos, los controles deben ser evaluados en cuanto a su efectividad, entendida como la capacidad real de disminuir la exposición al riesgo. Este análisis se basa en dos dimensiones complementarias:

- **Eficiencia:** mide el grado en que el control aprovecha los recursos (tiempo, costos, personal, tecnología) de manera óptima para alcanzar sus objetivos.
- **Eficacia:** evalúa el grado en que el control logra realmente reducir la probabilidad o el impacto del riesgo identificado. [56]

Matemáticamente, la efectividad del control (EC) puede representarse como:

$$EC = (Eficiencia * (asignación \%)) + (Eficacia * (asignación \%))$$

De esta forma, la valoración final del control dependerá no solo de su calificación en eficiencia y eficacia, sino también de los pesos que se les otorguen en la metodología de la organización, garantizando un enfoque ajustado a sus prioridades estratégicas.

Una vez calculada esta efectividad, se procede a integrar el resultado en la reevaluación del riesgo. El principio consiste en que la calificación obtenida define cuánto logra disminuir la probabilidad de ocurrencia o el impacto asociado, dependiendo de la naturaleza del control. Así, si el riesgo inherente refleja el nivel de exposición inicial, el riesgo residual se obtiene aplicando el efecto de los controles sobre esa valoración, siempre en función de las escalas previamente establecidas. Representándose matemáticamente como:

$$RR = (P - \Delta P) * (I) \text{ o } RR = (I - \Delta I) * (P)$$

donde ΔP o ΔI representan la reducción alcanzada en probabilidad o impacto, definida en función de la calificación obtenida en eficiencia y eficacia, y conforme a la escala establecida por la organización.

El resultado de este cálculo se contrasta con los criterios de aceptación del riesgo definidos por la organización. Estos criterios representan los umbrales máximos tolerables según la estrategia corporativa, las exigencias regulatorias y la apetencia al riesgo. Si el riesgo residual se mantiene dentro de estos límites, puede aceptarse y monitorearse. En cambio, si supera los umbrales establecidos, se requiere avanzar hacia la etapa de tratamiento de riesgos, en la que se definirán acciones adicionales como implementar nuevos controles, transferir parte de la exposición mediante seguros o acuerdos contractuales, o incluso rediseñar procesos para evitar la amenaza.

3.2.1.8.3. Tratamiento de riesgos

El tratamiento del riesgo constituye la última fase del proceso de gestión, en la cual se definen y ejecutan las acciones necesarias para reducir la exposición de la organización en términos aceptables. Mientras la evaluación de riesgos permite conocer la magnitud de las amenazas y vulnerabilidades, el tratamiento se orienta a decidir y aplicar las medidas que permitan mitigarlos, transferirlos, evitarlos o, en algunos casos, aceptarlos de manera consciente y justificada.

En esta etapa cobra relevancia la figura del responsable de riesgos, previamente designado por la organización, quien no solo lidera la coordinación de las actividades, sino que también asume la responsabilidad de aprobar el plan de tratamiento propuesto. Este plan constituye el instrumento estratégico que detalla las acciones específicas, los controles seleccionados, los plazos, los recursos y los responsables encargados de su ejecución, garantizando que cada medida se encuentre alineada con la criticidad del riesgo y con la capacidad de respuesta institucional.

Declaración de aplicabilidad

De manera complementaria, el tratamiento de riesgos de seguridad de la información contempla la elaboración de una declaración de aplicabilidad (SoA, Statement of Applicability), en la cual se registran los controles definidos, la justificación de su

inclusión, el estado en que se encuentran (implementados, planificados o no aplicables) y, en su caso, las razones que sustentan su exclusión. Este documento constituye una pieza clave, ya que proporciona trazabilidad y evidencia objetiva sobre las decisiones adoptadas, evitando omisiones y asegurando una respuesta adecuada a los riesgos.

En coherencia con la ISO/IEC 27005:2022, la SoA se convierte en el instrumento que materializa la relación entre los escenarios de riesgo identificados y las medidas de tratamiento adoptadas. Permite documentar de manera estructurada qué controles resultan pertinentes para mitigar amenazas y vulnerabilidades específicas, asegurando que las decisiones estén fundamentadas en el análisis del contexto organizacional y en los criterios de aceptación previamente definidos. Asimismo, la norma enfatiza que este documento debe revisarse y actualizarse de forma periódica, para reflejar cambios en los riesgos, en el entorno tecnológico o en los requisitos regulatorios.

La importancia de la SoA radica en que evita omisiones y asegura coherencia entre el análisis de riesgos, la selección de controles y la gestión de servicios. En el caso de ISO/IEC 27001, la SoA es obligatoria y debe estar alineada con los controles definidos en el Anexo A de la norma, mientras que en ISO/IEC 20000 se articula con la gestión de servicios de TI, en aspectos como continuidad, disponibilidad, gestión de incidentes y cumplimiento de acuerdos de nivel de servicio. En ambos casos, constituye la principal evidencia de que los riesgos residuales han sido evaluados, que las medidas de mitigación son pertinentes y que existe un plan formal de tratamiento y seguimiento.

De manera práctica, la ISO/IEC 27005:2022 sugiere que cada organización construya su propia declaración de aplicabilidad a partir de una plantilla estandarizada, la cual debe adaptarse al contexto, los activos de información y los riesgos identificados. En este sentido, el ANEXO D de la presente investigación incluye una plantilla vacía diseñada para guiar a las organizaciones en el ejercicio de revisión y análisis, facilitando la identificación de controles aplicables y su correspondiente justificación en función de su realidad institucional.

3.2.2. Etapa II: Hacer

La etapa **hacer** constituye el eje operativo del Sistema Integrado de Gestión y representa el momento en el que se materializan las decisiones estratégicas definidas en la planificación. Bajo esta fase, la organización despliega las actividades orientadas a garantizar que los recursos, las competencias, la concienciación, la comunicación y el control operacional se ejecuten de manera efectiva, asegurando la alineación con los requisitos de seguridad de la información y la gestión de servicios de TI.

De acuerdo con Pineda en [57], esta fase implica ejecutar el plan de trabajo diseñado, apoyándose en mecanismos de control que permitan monitorear el avance de las actividades y el cumplimiento de los tiempos, lo cual asegura disciplina, trazabilidad y transparencia en la implementación. En la misma línea, Barquero y Palomino en [58] resaltan que el “Hacer” corresponde al momento en el que se aprueban y aplican las acciones planificadas, incorporando los ajustes necesarios cuando los resultados no alcanzan los niveles esperados. Para ello, resulta esencial registrar los resultados obtenidos y establecer con claridad las responsabilidades del personal involucrado.

El éxito de esta etapa depende de la capacidad organizacional para ejecutar de forma coherente y disciplinada las actividades previamente definidas, garantizando que las directrices estratégicas y objetivos planteados se traduzcan en resultados tangibles. Para facilitar su desarrollo, esta etapa se organiza en las siguientes actividades clave:

3.2.2.1. Gestión de recursos y competencias

La adecuada gestión de recursos y competencias constituye un pilar fundamental para la eficacia del Sistema Integrado de Gestión, ya que permite asegurar la disponibilidad de los medios necesarios para su establecimiento, implementación, mantenimiento y mejora continua. En este sentido, la organización debe garantizar que los recursos humanos, técnicos, financieros y de información se encuentren alineados con los objetivos estratégicos y con los requisitos establecidos por las normas ISO/IEC 27001 e ISO/IEC 20000-1. Esta provisión de recursos no se limita a la asignación presupuestal o tecnológica, sino que abarca también la capacidad de sostener en el tiempo la operación del sistema, respondiendo a las necesidades de seguridad de la información y de gestión de servicios de TI.

Dentro de esta etapa, adquiere un papel protagónico la definición clara de los roles y responsabilidades organizacionales. La estructura del Sistema Integrado de Gestión debe estar soportada en un organigrama que refleje la jerarquía y líneas de autoridad, acompañado de manuales de funciones que describan con precisión las tareas, competencias y responsabilidades de cada cargo. De esta manera, cada colaborador entiende no solo su rol dentro de la organización, sino también la forma en que su labor impacta en el desempeño y eficacia del sistema. Este enfoque favorece la coherencia operativa, evita duplicidad de funciones y garantiza que las actividades de seguridad de la información y gestión de servicios de TI se ejecuten de manera integrada.

La competencia del personal, además de definirse con base en los perfiles establecidos en los manuales de funciones, debe garantizar que quienes participan en la operación del sistema cuenten con el nivel apropiado de educación, formación o experiencia. Esta competencia se fortalece mediante programas de capacitación, procesos de tutoría, reasignación de responsabilidades o, cuando sea necesario, la incorporación de personal especializado, según las necesidades previamente identificadas. La eficacia de estas acciones debe evaluarse de manera sistemática, asegurando que las capacidades adquiridas se traduzcan en resultados concretos y medibles. A su vez, la documentación de dichas competencias, junto con el manual de funciones y el organigrama, constituye una evidencia esencial dentro del Sistema Integrado de Gestión, ya que aporta trazabilidad y transparencia tanto para la gestión interna como para los procesos de auditoría externa.

En conjunto, la provisión de recursos, la definición clara de roles y funciones, el aseguramiento de competencias y la gestión de la evidencia documental conforman una estrategia integral que fortalece la confiabilidad del Sistema Integrado de Gestión. Esto permite no solo garantizar el cumplimiento normativo, sino también consolidar una cultura organizacional donde cada miembro reconoce su responsabilidad en la protección de la información y en la entrega eficaz de los servicios de TI.

3.2.2.2. Concienciación, comunicación y cultura organizacional

En esta actividad, la organización debe garantizar que todas las personas que realizan actividades bajo su control adquieran plena conciencia de la importancia de su rol dentro

del SIG. Esto implica asegurar el conocimiento y apropiación de la política de Seguridad de la Información, así como de la política, los objetivos y los servicios definidos en la gestión del servicio, de manera que cada trabajador entienda cómo su labor diaria aporta a la eficiencia del sistema y a la mejora del desempeño organizacional. Igualmente, resulta fundamental que el personal comprenda las implicaciones derivadas de la no conformidad con los requisitos del sistema, fomentando así una cultura de responsabilidad y compromiso.

Para alcanzar este nivel de concienciación, se deben implementar mecanismos de formación continua, talleres de sensibilización, campañas internas y espacios de retroalimentación que fortalezcan la cultura organizacional orientada a la calidad, la seguridad y la prestación efectiva del servicio. La concienciación no solo se concibe como un proceso informativo, sino como una estrategia de apropiación cultural en la que cada persona asuma de manera clara su contribución al logro de los objetivos colectivos.

En relación con la comunicación, la organización debe estructurar un plan que defina de manera precisa qué información debe comunicarse, en qué momentos y bajo qué medios. Dicho plan debe abarcar tanto la comunicación interna y externa, asegurando que las áreas y equipos dispongan de información clara y oportuna para la toma de decisiones, así como la comunicación es dirigida a las partes interesadas. Este proceso debe establecer no solo los canales y formatos de comunicación, sino también las responsabilidades: quién comunica, quién es responsable de validar los mensajes y cómo garantizar que la información fluya de forma eficaz, transparente y verificable.

De esta manera, la concienciación, la comunicación y la cultura organizacional se convierten en ejes estratégicos del sistema integrado, asegurando que las personas comprendan su rol, asuman su responsabilidad y dispongan de la información necesaria para contribuir al cumplimiento de los objetivos de gestión y al fortalecimiento continuo de la organización.

3.2.2.3. Gestión de la información documentada

La información documentada constituye uno de los pilares del Sistema Integrado de Gestión, ya que permite asegurar la trazabilidad, coherencia y transparencia de todos los procesos. Más allá de un simple requisito normativo, se convierte en un elemento que

facilita la coordinación interna, respalda la toma de decisiones y ofrece evidencia verificable tanto para auditorías internas como externas.

En este sentido, la organización debe garantizar que la creación, actualización y control de la información documentada se realicen de forma estructurada, clara y accesible. Ello implica que cada documento cuente con una identificación adecuada, con versiones controladas y con responsables definidos, asegurando que siempre se disponga de la información correcta y vigente.

Además, la gestión documental debe ser entendida como un mecanismo de preservación del conocimiento institucional. Manuales, políticas, procedimientos, registros y acuerdos con proveedores no solo cumplen la función de demostrar conformidad, sino que también actúan como guías vivas que permiten que la operación diaria se realice de manera consistente, incluso en escenarios de rotación de personal o cambios organizacionales.

De igual forma, es necesario reconocer que la información documentada incluye tanto los documentos internos generados por la organización, como los de origen externo que inciden directamente en la operación (normas técnicas, leyes, reglamentos o contratos). Su control evita el riesgo de trabajar con información obsoleta y permite mantener actualizada la base de conocimiento sobre la cual se soporta el sistema de gestión.

Con el fin de facilitar la aplicación práctica de este requisito, en la tabla No. 9 se han definido las siguientes pautas para la gestión de la información documentada:

Pautas para la gestión de información documental		
Etapa	Aspecto por considerar	Ejemplo practico
Creación y actualización	<ul style="list-style-type: none">- Identificación clara del tipo de documento, código, área responsable, nombre del documento, versión y fecha de emisión- Revisión y aprobación formal	"DOC_001_CAL_Manual de gestión V2.0 25JUL2025" Aprobado por: _____
Control y acceso	<ul style="list-style-type: none">- Garantizar la disponibilidad, confidencialidad e integridad- Definir niveles de acceso, modificación y aprobación de los documentos	Plataforma documental con permisos diferenciados por rol
Almacenamiento y preservación	<ul style="list-style-type: none">- Mantener legibilidad, respaldos periódicos y versiones oficiales.	Copia de seguridad diaria de los manuales en nube corporativa.

Pautas para la gestión de información documental		
Etapa	Aspecto por considerar	Ejemplo practico
Control de cambios	- Registro histórico de modificaciones y responsables	Historial de cambios en el formato de "Archivo maestro de documentos".
Retención y disposición	- Definir tiempos de conservación y métodos de eliminación segura.	Eliminación certificada de documentos obsoletos después de 5 años.
Información externa	- Identificar normas, leyes y contratos vigentes aplicables.	Normograma legal y contractual actualizada semestralmente.

Tabla 9. Gestión de información documentada. Elaboración propia

3.2.2.4. Control operacional y prestación del servicio

La operación constituye el eje central del sistema de gestión, pues es el espacio donde se materializan los objetivos estratégicos, las políticas y los compromisos adquiridos con las partes interesadas. En esta etapa, la organización debe asegurar que la prestación de los servicios se realice de manera controlada, planificada y coherente con los requisitos establecidos. Para ello, se requiere no solo diseñar procesos, sino también implementar mecanismos de control que permitan evaluar su desempeño, gestionar cambios y garantizar que los productos y servicios externos que impactan el sistema de gestión sean monitoreados adecuadamente.

La planificación y control de la operación se convierten en un ejercicio de disciplina organizacional, en el que cada proceso debe estar definido, medido y soportado con la información documentada necesaria. De esta manera, se asegura que la ejecución se realice conforme a lo planeado y que cualquier desviación pueda ser detectada y tratada oportunamente.

Para garantizar que los procesos se desarrollen bajo criterios claros de planificación y control, la organización debe apoyarse en un mapa de procesos que actúe como punto de referencia estructural. Esta herramienta permite visualizar de manera integral la organización, evidenciando cómo cada proceso se articula con los demás y aportan a la generación de valor. Asimismo, facilita la identificación de interacciones, responsabilidades y resultados esperados, fortaleciendo el control operacional y el seguimiento del desempeño.

En este marco, los procesos se clasifican en cuatro niveles que aseguran su coherencia y relevancia dentro del Sistema Integrado de Gestión:

- **Procesos estratégicos:** orientados a la dirección, planeación y toma de decisiones. Incluyen la definición de políticas, objetivos, gestión de riesgos y comunicación con partes interesadas.
- **Procesos tácticos o misionales:** directamente relacionados con la prestación del servicio y el cumplimiento de los requisitos del cliente. Son el núcleo de la operación, donde se concentran los controles de desempeño, gestión de incidentes y continuidad del servicio.
- **Procesos de apoyo:** brindan soporte al desarrollo de las actividades, asegurando los recursos humanos, tecnológicos y financieros necesarios. Aquí se incluyen la gestión del talento, la infraestructura, la seguridad de la información y la gestión documental.
- **Procesos de evaluación y mejora:** permiten el seguimiento, medición, análisis y despliegue de acciones de mejora continua, aportando retroalimentación para la toma de decisiones y garantizando la eficacia del Sistema Integrado de Gestión.

Esta clasificación, además de organizar la operación, fortalece la trazabilidad del sistema, asegurando que cada proceso tenga objetivos claros, entradas, salidas, responsables definidos, indicadores de desempeño y riesgos asociados.

3.2.2.5. Gestión del ciclo de vida del servicio

La etapa de “Hacer” dentro de un Sistema Integrado de Gestión representa el momento en el que las decisiones estratégicas y la planificación se convierten en actividades concretas que sostienen el ciclo de vida de los servicios. Aquí, la organización no solo ejecuta procesos de manera aislada, sino que articula su portafolio de servicios, las relaciones con clientes y proveedores, la gestión de cambios y la administración de recursos de forma coherente, asegurando que cada acción esté alineada con los objetivos estratégicos y con los requisitos normativos. La clave está en comprender que el valor de un Sistema Integrado de Gestión no reside únicamente en la documentación

de procedimientos, sino en la capacidad de movilizar recursos, coordinar áreas y responder de manera resiliente a los desafíos que enfrenta el negocio.

Un primer aspecto fundamental es la gestión del portafolio de servicios, que se convierte en el eje articulador entre la estrategia y la operación. Mantener actualizado el portafolio permite priorizar iniciativas, evaluar riesgos y asignar recursos a servicios que aportan mayor valor al negocio. Por ejemplo, una organización de servicios financieros puede decidir invertir en reforzar la disponibilidad de su plataforma de banca en línea, aun cuando esto implique posponer la incorporación de nuevas funcionalidades, ya que la continuidad de la operación tiene mayor impacto en la confianza del cliente. En este sentido, una buena práctica consiste en realizar revisiones periódicas del portafolio con participación de áreas técnicas, comerciales y de riesgo, asegurando que no existan duplicidades, que los servicios retirados sean reemplazados de manera planificada y que se documenten claramente los criterios de prioridad.

De la mano con el portafolio, la gestión de partes interesadas resulta esencial para lograr una operación integrada. Aunque muchas actividades se deleguen a terceros la responsabilidad de garantizar el servicio recae siempre en la organización. Aquí, el Sistema Integrado de Gestión debe establecer mecanismos de evaluación periódica, auditorías a proveedores críticos y acuerdos que definan no solo entregables, sino también responsabilidades en la gestión de riesgos y seguridad. Para ilustrarlo, pensemos en el caso de un proveedor externo que administra servidores críticos: el contrato no debería limitarse a métricas de disponibilidad, sino incluir tiempos de respuesta ante incidentes, procedimientos de escalamiento y exigencias de pruebas de recuperación.

Por su parte, la gestión de la configuración y los activos aporta un soporte técnico indispensable. No basta con registrar inventarios estáticos de hardware o software; lo que se requiere es una base de datos de configuración viva, que permita identificar dependencias entre componentes y servicios. Una caída en un switch de comunicaciones, por ejemplo, puede ser analizada en términos de qué servicios se verán afectados, a qué clientes impactará y qué medidas de contingencia se deben activar. Para garantizar esta trazabilidad, las organizaciones más maduras adoptan auditorías periódicas de configuración, comparando la información registrada frente a la realidad

operativa, e incorporan herramientas de monitoreo que actualizan de manera automática los cambios detectados.

Un Sistema Integrado de Gestión también debe fortalecer la gestión de relaciones con clientes y usuarios, que va más allá de la satisfacción inmediata y busca construir confianza sostenible. Esto implica contar con canales claros de comunicación, procesos para documentar y escalar quejas, y mecanismos de retroalimentación periódica. Una herramienta adecuada para el estudio es la encuesta de satisfacción, la cual puede convertirse en un insumo poderoso si se complementa con sesiones de retroalimentación directa con usuarios críticos, permitiendo ajustar acuerdos de nivel de servicio antes de que los incumplimientos se materialicen en riesgos reputacionales. En paralelo, la gestión de proveedores debe verse como una extensión de la relación con el cliente: en ambos casos se establecen acuerdos, se miden resultados y se buscan oportunidades de mejora.

En cuanto a la administración de recursos, la gestión financiera, de la demanda y de la capacidad asegura que los compromisos documentados se sostengan en la práctica. Elaborar presupuestos detallados, registrar costos reales y proyectar escenarios de consumo futuro permite tomar decisiones preventivas, como ampliar infraestructura o contratar recursos especializados antes de que la demanda supere la capacidad instalada.

Uno de los procesos más críticos es la gestión del cambio, pues constituye el mecanismo mediante el cual los servicios evolucionan de forma controlada. Implementar cambios sin análisis de riesgos ni planes de reversión puede derivar en interrupciones graves. Por ello, se recomienda clasificar los cambios según su impacto (normal, mayor o de emergencia), someterlos a revisión multidisciplinaria y documentar los resultados de cada implementación.

Finalmente, los procesos de liberación y despliegue consolidan el trabajo previo, garantizando que las versiones de servicios, aplicaciones o componentes lleguen a los usuarios con el menor riesgo posible. Las organizaciones más sólidas realizan pruebas piloto antes de un despliegue masivo, establecen ventanas de mantenimiento previamente comunicadas y documentan los resultados de la liberación para alimentar la

mejora continua. Una práctica recomendada consiste en registrar los aprendizajes de cada despliegue, comparando qué funcionó y qué no, de manera que los siguientes ciclos sean más ágiles y menos propensos a fallas.

3.2.2.6. Gestión de incidentes y problemas

Dentro de un Sistema Integrado de Gestión, la gestión de incidentes, problemas y cambios constituye una actividad esencial para garantizar la estabilidad operativa, la continuidad de los servicios y la confianza de las partes interesadas. No se trata de procesos independientes ni de requisitos fragmentados de distintas normas, sino de un ciclo articulado que, al ser gestionado de manera coordinada, permite responder eficazmente a los eventos que afectan la organización, reducir riesgos y generar aprendizaje para prevenir recurrencias.

La gestión de incidentes representa el punto de partida de este ciclo. Registrar, clasificar, priorizar, escalar, resolver y cerrar de manera ordenada cada evento es fundamental para mantener el control de la operación. Este proceso, lejos de limitarse a una reacción específica, requiere la articulación de todas las áreas involucradas, ya que cada incidente puede tener un impacto directo en el sistema de gestión, en los servicios prestados y en las partes interesadas. La identificación de incidentes mayores y su tratamiento conforme a procedimientos documentados, junto con la obligación de mantener informada a la alta dirección, asegura que las decisiones se tomen con base en información completa y oportuna, fortaleciendo así la capacidad de respuesta de la organización.

Sin embargo, la resolución de incidentes no se limita a “apagar fuegos”. Cada registro constituye una fuente de datos que, al ser analizados, permiten identificar tendencias, comprender las causas profundas de los fallos y dar paso a la gestión de problemas. Esta etapa introduce un enfoque más analítico y preventivo, orientado a descubrir la raíz de las fallas y establecer medidas que eviten su repetición. La actualización constante de los registros, el análisis de errores conocidos y la adopción de acciones de mitigación aseguran que la organización no solo reaccione, sino que evolucione hacia una gestión más robusta y anticipatoria.

De manera complementaria, los problemas identificados que requieren modificaciones en procesos, infraestructuras o servicios encuentran su canal natural en la gestión de

cambios. Esta última garantiza que las soluciones derivadas de la investigación de causas se implementen de forma planificada, controlada y alineada con las políticas del Sistema Integrado de Gestión, evitando que los ajustes introduzcan nuevos riesgos o debilidades. Así, la gestión de cambios cierra el ciclo y lo retroalimenta, integrando de forma armónica la capacidad reactiva con la preventiva y la transformacional.

Cuando se considera de forma integrada, este ciclo de incidentes, problemas y cambios adquiere un carácter maduro y estratégico. La organización ya no se limita a reaccionar ante eventos aislados, sino que desarrolla un mecanismo continuo de detección, análisis y mejora que fortalece la resiliencia del sistema, protege la seguridad de la información, asegura la disponibilidad de los servicios y genera confianza en las partes interesadas. En este sentido, la gestión integrada constituye no solo un requisito normativo de estándares como ISO/IEC 20000-1 e ISO/IEC 27001, sino una práctica organizacional indispensable para consolidar un sistema resiliente, confiable y en permanente mejora continua.

3.2.2.7. Aseguramiento del servicio: Gestión de continuidad y disponibilidad

En el marco de un sistema integrado de gestión, el aseguramiento del servicio se configura como un componente esencial para mantener la estabilidad y confiabilidad de los servicios de TI, asegurando que estos respondan de manera eficaz a las necesidades del negocio y de las partes interesadas en cualquier circunstancia. Este aseguramiento no se limita al cumplimiento normativo, sino que se traduce en la implementación de prácticas articuladas que permiten proteger la operación, fortalecer la confianza y garantizar la resiliencia organizacional. En este contexto, la gestión de la disponibilidad y la gestión de la continuidad del servicio se presentan como pilares complementarios que, al trabajar de manera conjunta, aseguran tanto el funcionamiento ininterrumpido como la capacidad de recuperación frente a eventos que puedan afectar la prestación del servicio.

La gestión de la disponibilidad del servicio constituye el primer paso en el aseguramiento de que los servicios de TI respondan de manera confiable a los compromisos

establecidos con el negocio y con las partes interesadas. Su propósito central es garantizar que los servicios permanezcan operativos y accesibles en los niveles acordados, considerando los Acuerdos de Nivel de Servicio (ANS), los requisitos estratégicos y los riesgos asociados. Para alcanzar este objetivo, la organización debe evaluar y documentar periódicamente los factores que puedan afectar la disponibilidad, establecer metas claras y mantener actualizados los requisitos de servicio, de modo que exista una correspondencia permanente entre la capacidad técnica y las expectativas del negocio.

El seguimiento constante de los indicadores de disponibilidad no solo permite detectar desviaciones y responder con rapidez a fallos no planificados, sino que también ofrece la oportunidad de aprender de cada evento, identificar causas raíz y reducir la probabilidad de recurrencia. De esta manera, la gestión de la disponibilidad se integra de forma natural con la gestión de incidentes y problemas, pues todo evento que afecte la operatividad del servicio debe ser registrado, clasificado, priorizado y tratado de manera articulada entre las áreas técnicas y de gestión. Esta dinámica convierte a la disponibilidad en un insumo estratégico para la toma de decisiones dentro del sistema integrado de gestión, reflejando la capacidad de respuesta y resiliencia de la organización.

Ahora bien, la sola gestión de la disponibilidad no resulta suficiente cuando se presentan interrupciones graves o desastres que comprometen la continuidad del servicio de forma significativa. Aquí entra en juego la gestión de la continuidad, que amplía la visión hacia escenarios de mayor impacto, donde no basta con restaurar la operación diaria, sino que se requiere asegurar la supervivencia de los procesos críticos en condiciones extraordinarias. Para ello, la organización debe evaluar los riesgos de manera planificada, definir requisitos específicos de continuidad y diseñar planes formales que incluyan criterios de activación, responsabilidades, procedimientos de recuperación y estrategias para regresar a la normalidad. Estos planes, que deben ser accesibles y probados periódicamente, se convierten en un recurso fundamental para garantizar que, incluso ante pérdidas importantes, los servicios puedan restablecerse dentro de los plazos definidos como aceptables por el negocio.

La articulación entre disponibilidad y continuidad permite que el aseguramiento del servicio trascienda lo operativo para convertirse en un factor de confianza y resiliencia organizacional. Mientras la disponibilidad aporta estabilidad en las condiciones normales de operación, la continuidad asegura capacidad de reacción y recuperación en escenarios disruptivos. Ambas dimensiones, al integrarse en el marco del sistema de gestión, no solo fortalecen la transparencia y la comunicación con las partes interesadas, sino que consolidan una cultura organizacional orientada al aprendizaje y a la mejora continua.

3.2.2.8. Gestión de políticas y requisitos específicos de la operación

En coherencia con la gestión de la disponibilidad y la continuidad del servicio, la definición y administración de políticas y requisitos específicos se convierten en el elemento articulador que asegura que los procesos de TI operen de manera ordenada, coherente y alineada con los objetivos estratégicos de la organización. Estas políticas no deben entenderse como simples documentos formales, sino como instrumentos vivos que orientan la operación diaria, delimitan responsabilidades y establecen criterios claros para la toma de decisiones. Desde la perspectiva de un sistema integrado de gestión, su valor radica en que permiten armonizar tanto la gestión del servicio como la seguridad de la información, asegurando que ambas dimensiones trabajen de forma conjunta para proteger la operación y responder a las expectativas de las partes interesadas.

En este marco, resulta esencial que la organización adopte políticas de seguridad de la información que regulen, por ejemplo, el acceso a datos sensibles, la gestión de contraseñas, el uso seguro de dispositivos o la clasificación de la información, y que estas se articulen con políticas de gestión del servicio, como las que definen la priorización de incidentes, los tiempos de respuesta comprometidos o los criterios de escalamiento. La integración de ambos enfoques permite responder no solo a la necesidad de proteger la información, sino también de garantizar que los servicios continúen operando bajo parámetros de confiabilidad y eficiencia.

Asimismo, la gestión de requisitos específicos exige mecanismos que aseguren su cumplimiento y actualización. Esto implica evaluar periódicamente riesgos y necesidades del negocio, contrastar dichos requisitos con los acuerdos de nivel de servicio, y

establecer métricas para verificar su efectividad. Por ejemplo, una política de disponibilidad podría complementarse con indicadores de tiempo medio de recuperación (MTTR) o de porcentaje de cumplimiento de los niveles de servicio acordados, mientras que una política de continuidad podría definirse en torno a objetivos de tiempo de recuperación (RTO) y objetivos de punto de recuperación (RPO). Estas métricas no solo permiten medir el desempeño, sino también generar aprendizajes para ajustar planes y fortalecer la resiliencia.

Desde una perspectiva aplicada, la definición de políticas y requisitos también ofrece alternativas de solución frente a situaciones críticas. Ante incidentes recurrentes de indisponibilidad, la organización podría implementar políticas que obliguen a registrar todos los eventos en una base centralizada, clasificarlos según impacto y urgencia, y activar protocolos de escalamiento que garanticen la participación de las áreas adecuadas. De igual manera, frente a amenazas de seguridad, políticas claras sobre gestión de accesos o copias de respaldo aseguran que la organización pueda responder de manera rápida y efectiva.

En síntesis, la gestión de políticas y requisitos específicos constituye el soporte que garantiza la coherencia, la previsibilidad y la capacidad de adaptación del sistema integrado de gestión. Al establecer lineamientos claros, ofrecer alternativas de respuesta y reforzar la articulación entre seguridad de la información y gestión del servicio, estas políticas trascienden el papel normativo para convertirse en un medio estratégico que protege la operación, genera confianza y asegura la sostenibilidad de la organización frente a un entorno cambiante.

3.2.3. Etapa III: Verificar

La etapa **Verificar** representa el momento de contraste y validación dentro del despliegue de un Sistema Integrado de Gestión, diseñado para articular los requisitos normativos de los estándares ISO/IEC 27001 e ISO/IEC 20000-1). En esta fase, la organización debe medir, analizar y evaluar el desempeño de los procesos con respecto a los objetivos previamente establecidos, asegurando que las acciones implementadas generen los resultados esperados y cumplen con los lineamientos normativos.

De acuerdo con Rouse en [59], “Es necesario controlar si lo que se ha definido se desarrolla correctamente. Lo primero que debe hacerse es fijar qué vamos a controlar, cuándo lo haremos y dónde se piensa controlar”. En este sentido, la verificación se convierte en un proceso estructurado que otorga objetividad al sistema, ya que permite identificar desviaciones, documentar brechas y alimentar el ciclo de mejora continua con información confiable.

La etapa de verificación demanda desplegar los datos, revisar los problemas y errores, comprender las diferencias y documentar las lecciones aprendidas, generando así insumos para la mejora. [60] En el marco de un Sistema Integrado de Gestión, este principio cobra especial relevancia al integrar tanto el seguimiento a la seguridad de la información como la gestión de los servicios de TI en un mismo esquema metodológico.

Para efectos de este proyecto, la etapa de Verificar se materializa en las siguientes actividades:

3.2.3.1. Seguimiento, medición, análisis y evaluación.

El seguimiento, la medición, el análisis y la evaluación representan el eje central de la etapa de Verificar, pues constituyen el mecanismo mediante el cual la organización asegura que los procesos del Sistema Integrado de Gestión cumplen con los resultados previstos y con los requisitos establecidos en ambas normas. El cumplimiento de este requisito implica que la entidad debe determinar de manera anticipada qué necesita ser monitoreado y medido, los métodos que se emplearán, la frecuencia de las mediciones y los responsables de llevarlas a cabo, garantizando que la información generada sea fiable y relevante para la toma de decisiones.

Desde la perspectiva de un Sistema Integrado de Gestión, la necesidad de seguimiento se materializa en la verificación continua de la eficacia de los controles de seguridad de la información, así como del cumplimiento de los niveles de servicio comprometidos con los clientes y usuarios. Esto abarca, por ejemplo, el monitoreo de incidentes de seguridad, la evaluación de la eficacia de los planes de concientización, la revisión de accesos otorgados y su consistencia con los perfiles definidos, pero también la validación del tiempo de respuesta frente a incidentes tecnológicos, la disponibilidad de la

infraestructura crítica y la satisfacción de los usuarios respecto a los servicios recibidos. El valor de este ejercicio radica en que permite detectar tempranamente desviaciones que, de no ser atendidas, podrían comprometer la confidencialidad, integridad y disponibilidad de la información o afectar la continuidad de los servicios tecnológicos.

Para responder a estas necesidades, la organización debe definir métodos válidos y consistentes que respalden el monitoreo. Estos pueden incluir el uso de indicadores clave de desempeño que midan: el porcentaje de incidentes resueltos dentro de los tiempos establecidos, la proporción de vulnerabilidades críticas tratadas dentro de los plazos definidos o la disponibilidad mensual de servicios críticos; así como mecanismos de medición automática a través de tableros de control o sistemas de gestión de tickets que permitan evidenciar tiempos de atención. Asimismo, las encuestas de satisfacción y la revisión documental de bitácoras y reportes forman parte de los métodos que complementan la evaluación de la eficacia de los procesos.

El requisito normativo establece también que este seguimiento no puede ser esporádico ni arbitrario, sino que debe planificarse con una frecuencia acorde a la criticidad de los procesos. Así, en algunos casos el monitoreo debe realizarse en tiempo real, como ocurre con la disponibilidad de servicios esenciales o la detección de incidentes de seguridad; en otros, con periodicidad mensual para consolidar métricas sobre niveles de servicio o eficacia de controles; de manera trimestral, para analizar tendencias e identificar patrones de fallas recurrentes; y de forma anual, como insumo indispensable para la revisión por la dirección y la planificación de la mejora continua.

Una vez obtenida la información, el análisis y la evaluación permiten contrastar los resultados frente a los objetivos trazados, los criterios normativos y los compromisos contractuales. Este ejercicio no solo busca determinar si se han alcanzado los niveles de desempeño definidos, sino también identificar causas raíz de las desviaciones, reconocer oportunidades de mejora y valorar su impacto en el riesgo residual aceptado por la organización.

En cuanto a la responsabilidad, las normas establecen que este proceso no es exclusivo de un solo rol, sino que requiere una articulación clara de diferentes actores. Los responsables de cada proceso deben realizar el seguimiento cotidiano de las métricas

asignadas; el gestor del sistema consolida, apoyado por los líderes en seguridad informática y gestión del servicio, valida los indicadores relacionados con la gestión de riesgos y controles, así como la información de desempeño de los servicios y coordina el análisis de cumplimiento de SLA; y finalmente la alta dirección, a través del comité del Sistema Integrado de Gestión, recibe los informes consolidados, evalúa las tendencias, determinando las acciones estratégicas que aseguran la eficacia y la mejora continua del sistema.

3.2.3.2. Auditoría interna.

La auditoría interna constituye uno de los instrumentos más relevantes dentro de la etapa de verificación del Sistema Integrado de Gestión, ya que permite a la organización obtener una visión objetiva y sistemática sobre el grado de cumplimiento de los requisitos propios definidos por la entidad y de aquellos mandatorios establecidos por las normas internacionales que rigen el sistema. Este proceso no se concibe como un ejercicio aislado, sino como una actividad periódica y planificada que garantiza que los lineamientos estratégicos, los controles de seguridad de la información y los compromisos de servicio se implementan y mantienen de manera eficaz en el tiempo.

El valor de la auditoría interna radica en que, más allá de comprobar el cumplimiento normativo, habilita un espacio de revisión crítica que aporta confianza sobre la madurez del sistema, la coherencia de sus procesos y la capacidad de responder a los riesgos y expectativas de las partes interesadas. En este sentido, tanto ISO/IEC 27001:2022 como ISO/IEC 20000-1:2018 requieren que la organización planifique y ejecute auditorías a intervalos definidos, con el fin de verificar que la operación del sistema no solo se ajusta a los requisitos, sino que mantiene una mejora sostenida a lo largo de su implementación.

Para lograrlo, la entidad debe establecer un programa de auditoría interna que especifique de manera clara la frecuencia, el alcance, los métodos y las responsabilidades que rigen el ejercicio. Dicho programa debe considerar la importancia de los procesos a auditar, el impacto de los cambios introducidos en la organización y los resultados de auditorías previas, de modo que se asegure una cobertura pertinente y

alineada con las prioridades estratégicas. Definir los criterios de auditoría y el alcance resulta fundamental, pues de ello depende que el ejercicio sea objetivo y se enfoque en los elementos que realmente determinan la eficacia del sistema.

En el marco del programa, se debe garantizar la selección adecuada de los auditores, procurando su independencia respecto a las áreas evaluadas y su competencia técnica en las normas de referencia. Este principio asegura la imparcialidad del proceso y otorga credibilidad a los resultados. Las actividades de auditoría pueden desarrollarse mediante revisión documental, entrevistas, observación de la operación de procesos y análisis de evidencias objetivas, siempre con el propósito de determinar si los controles y prácticas establecidas cumplen lo esperado.

Un aspecto clave es que los resultados de la auditoría interna no se agotan en la identificación de hallazgos, sino que deben ser comunicados de manera oportuna y pertinente a la dirección y a los responsables de proceso, de forma que se conviertan en insumo directo para la toma de decisiones y para el ciclo de mejora continua. Además, la organización debe asegurar que se dispone de la información documentada como evidencia de la ejecución del programa y de los resultados obtenidos, constituyendo así un registro formal que da trazabilidad y transparencia al sistema.

3.2.3.4. Revisión por la dirección.

La revisión por la dirección constituye una de las actividades más estratégicas dentro del sistema de gestión, ya que permite a la alta dirección evaluar de manera integral la conveniencia, adecuación, eficacia y alineación continua del sistema frente a los diferentes componentes de interés para la organización. Esta revisión se realiza en intervalos planificados y no se limita a un ejercicio formal, sino que representa un espacio de análisis y toma de decisiones que asegura la mejora continua y la sostenibilidad del sistema.

Para su desarrollo, es fundamental que la dirección considere un conjunto de entradas que abarcan tanto factores internos como externos. En primer lugar, se examina el estado de las acciones derivadas de revisiones anteriores, lo que permite verificar si los compromisos previamente asumidos han sido ejecutados y con qué nivel de efectividad. A continuación, se valoran los cambios en el entorno externo e interno que puedan

impactar al sistema, tales como nuevas regulaciones, transformaciones tecnológicas, condiciones del mercado o variaciones en los procesos internos que alteren el contexto de la organización. De igual manera, se incorporan los cambios en las necesidades y expectativas de las partes interesadas, reconociendo que estas evolucionan con el tiempo y que el sistema debe ajustarse para mantener su pertinencia.

La retroalimentación sobre el desempeño y eficacia del sistema de gestión se convierte en un eje central del análisis, donde se estudian las tendencias de no conformidades y acciones correctivas, los resultados obtenidos en actividades de seguimiento y medición, los hallazgos de auditorías internas y externas, así como el nivel de cumplimiento de los objetivos establecidos. Todo ello se complementa con la retroalimentación directa de las partes interesadas, que aporta una visión crítica sobre la percepción de la gestión y de los servicios entregados. Un elemento adicional de gran relevancia lo constituye la evaluación de riesgos y el estado de los planes de tratamiento asociados, cuya revisión permite determinar si las acciones implementadas han sido eficaces o requieren ajustes. En esta misma línea, se consideran las oportunidades de mejora identificadas a lo largo del ciclo operativo y los aspectos específicos del sistema de gestión, incluyendo la adherencia a la política establecida, el desempeño de los servicios, los niveles y capacidades de los recursos disponibles y los cambios que puedan afectar al sistema.

El resultado de este ejercicio no debe quedarse en una constatación descriptiva, sino que debe materializarse en decisiones estratégicas. Las salidas de la revisión por la dirección incluyen la definición de acciones para aprovechar oportunidades de mejora continua, la identificación de necesidades de cambios en el sistema, el ajuste de recursos cuando sea necesario, y la orientación de esfuerzos hacia la consolidación de objetivos estratégicos. Estas decisiones deben quedar documentadas como evidencia del proceso de revisión y servir de guía para el ciclo de gestión subsiguiente. En este sentido, los informes derivados de la revisión adquieren un papel fundamental, pues recogen no solo el desempeño y la eficacia del sistema y de los servicios, sino también las tendencias detectadas que permiten anticipar escenarios futuros. Estos informes sirven como base para la toma de decisiones, la comunicación y la articulación de nuevas acciones de mejora, garantizando que el sistema mantenga su dinámica de actualización permanente y refuerce la confianza de todos los actores vinculados.

3.2.3.5. Informes de desempeño y comunicación de resultados.

La elaboración de informes de desempeño y la comunicación de resultados constituye la actividad final de la etapa de verificación, en la cual se consolidan los hallazgos obtenidos durante el seguimiento, la medición, la auditoría y la revisión por la dirección. Estos informes no solo reflejan el cumplimiento de los objetivos, indicadores y requisitos normativos, sino que además permiten mostrar de manera transparente la eficacia del sistema de gestión y su contribución a la estrategia organizacional. La información debe ser presentada de forma clara, veraz y oportuna, garantizando que llegue a los niveles pertinentes de la organización.

En este proceso, cobra relevancia la capacidad de transformar los datos en información útil para la toma de decisiones. Por ello, los informes deben destacar tanto los resultados alcanzados como las desviaciones encontradas, incluyendo las acciones correctivas y de mejora planificadas. Igualmente, es esencial que los resultados se comuniquen de manera que fomenten la cultura de mejora continua, motivando a los equipos de trabajo y asegurando la alineación con los objetivos estratégicos. De este modo, la organización no solo cumple con un requisito documental, sino que convierte los informes de desempeño en una herramienta de gestión que fortalece la confianza, la transparencia y la sostenibilidad del sistema.

3.2.4. Etapa IV: Actuar

La etapa **Actuar**, correspondiente al cierre del ciclo PHVA, representa el momento en que la organización transforma el aprendizaje derivado de la evaluación en acciones concretas que promueven la mejora continua del Sistema Integrado de Gestión. En esta etapa, estructurada bajo el Capítulo 10 de las normas ISO/IEC 27001 e ISO/IEC 20000-1, se formaliza el tratamiento de no conformidades, la ejecución de acciones correctivas y la sistematización de cambios para fortalecer la eficacia del sistema.

El carácter iterativo del ciclo Deming se expresa plenamente en esta fase, ya que “si al verificar los resultados se logró lo que se tenía planeado, entonces se sistematizan y documentan los cambios que hubo; pero si al hacer una verificación se evidencia que no

se ha logrado lo deseado, entonces hay que actuar rápidamente, corregir lo planteado y establecer un nuevo plan de trabajo, repitiendo el ciclo nuevamente”[57]

En este sentido, la mejora continua se entiende como un proceso sistemático de aprendizaje que permite capitalizar los hallazgos de auditorías, revisiones de desempeño, análisis de riesgos y retroalimentación de las partes interesadas. La aplicación de acciones correctivas y preventivas constituye el eje práctico de esta etapa, donde cada no conformidad debe ser tratada desde su causa raíz, evitando recurrencias y generando ajustes en procedimientos, instructivos y controles. De esta forma, las acciones dejan de ser reactivas y se convierten en mecanismos de fortalecimiento del sistema.[61]

3.2.4.1. Gestión de no conformidades y acciones correctivas.

En el marco de la etapa de actuar, la gestión de las no conformidades y la aplicación de acciones correctivas constituyen un elemento esencial para garantizar la eficacia y sostenibilidad del sistema integrado de gestión. La organización debe reconocer que toda desviación, hallazgo de auditoría, incidente operativo o incumplimiento normativo representa una oportunidad de aprendizaje que exige una respuesta estructurada y documentada. En primer lugar, resulta fundamental reaccionar de manera inmediata ante la detección de una no conformidad, aplicando medidas que permitan contener sus efectos y mitigar posibles consecuencias sobre la seguridad de la información o la continuidad del servicio. Sin embargo, la atención inicial no puede quedarse en la corrección superficial del problema, sino que debe trascender hacia la identificación rigurosa de sus causas, empleando métodos de análisis como “la técnica de los cinco porqués” [62] o el diagrama de Ishikawa [63], con el fin de evitar recurrencias y fortalecer los controles existentes.

Una vez identificada la causa raíz, corresponde definir y ejecutar acciones correctivas que eliminen de manera definitiva el origen del problema, generando ajustes en los procedimientos, instructivos y controles asociados. Este proceso no debe asumirse como una respuesta aislada, sino como parte de un ciclo de retroalimentación que actualiza y robustece al sistema en su conjunto. De igual forma, resulta indispensable evaluar la eficacia de las medidas implementadas, lo cual implica verificar si estas han logrado

resolver la no conformidad y prevenir que vuelva a presentarse, para lo cual se recomienda establecer indicadores, realizar pruebas posteriores o contrastar resultados con auditorías internas.

El requisito también subraya la importancia de mantener evidencia documentada en todo el proceso, registrando desde la naturaleza de la no conformidad y las acciones inmediatas aplicadas, hasta los análisis realizados, las medidas adoptadas y la validación de sus resultados. Esta trazabilidad no solo responde a la exigencia normativa, sino que aporta valor en términos de transparencia y mejora de la cultura organizacional. En este sentido, las acciones correctivas dejan de ser simples reacciones ante fallas y se convierten en mecanismos de fortalecimiento continuo del sistema, pues cada hallazgo tratado en profundidad se transforma en una oportunidad para mejorar la calidad del servicio, la seguridad de la información y la satisfacción de las partes interesadas.

3.2.4.2. Mejora continua del sistema integrado de gestión.

A La mejora continua en un sistema integrado de gestión se concibe como una dinámica permanente que asegura la vigencia, eficacia y pertinencia de los controles, procesos y servicios de la organización frente a los cambios del entorno, las necesidades de las partes interesadas y la evolución de los riesgos. Esta actividad no debe entenderse como un evento aislado, sino como un proceso sistemático donde los hallazgos obtenidos a través de auditorías, revisiones por la dirección, análisis de riesgos y desempeño, así como la retroalimentación de usuarios y clientes, se convierten en oportunidades para fortalecer el sistema. Para que estas oportunidades tengan un impacto real, la organización debe establecer objetivos de mejora en áreas clave como la calidad de los procesos, el valor entregado a los clientes, la capacidad de respuesta, la reducción de costos, el incremento de la productividad, la optimización en la utilización de recursos y la mitigación de riesgos, asegurando que dichas metas estén alineadas con la estrategia organizacional y sean medibles en el tiempo.

Este enfoque se alinea con la filosofía japonesa del kaizen, concebida como un proceso de mejora continua que impulsa cambios graduales, sostenidos y articulados en todos los niveles de la organización, alejándose de la idea de transformaciones aisladas o esporádicas. Más que un método, constituye una forma de gestión que convierte la

mejora en un hábito permanente y en un compromiso cultural orientado a la eficiencia y la calidad. En esta misma línea, Atehortúa en [64] destaca que las prácticas de mejoramiento enfocadas en la excelencia permiten alcanzar incrementos progresivos en la productividad y la competitividad, gracias a la participación de todos los miembros de la organización. Así, la mejora continua se configura como un complemento esencial de los sistemas de gestión basados en normas internacionales, reforzando la noción de que los cambios no deben entenderse únicamente como una exigencia normativa, sino como una estrategia cultural y organizacional que garantiza la sostenibilidad a largo plazo.

La implementación de la mejora continua implica no sólo planificar y priorizar iniciativas, sino también verificar su cumplimiento mediante la medición periódica de los resultados frente a los objetivos definidos. Cuando las acciones no alcanzan las expectativas, resulta indispensable analizar las causas subyacentes y ajustar los planes, evitando que las desviaciones se repitan y garantizando que el sistema evolucione constantemente. De igual forma, comunicar las mejoras implementadas cumple un papel esencial: refuerza la cultura organizacional, motiva la participación de los colaboradores y transmite confianza entre las partes interesadas acerca de la eficacia del sistema.

Tanto la ISO/IEC 27001 como la ISO/IEC 20000-1 reconocen que las mejoras pueden materializarse de diversas formas: desde acciones reactivas para corregir desviaciones hasta iniciativas proactivas que impulsen la innovación en procesos, la adopción de nuevas tecnologías o la reestructuración de prácticas de gestión.

4. Juicio de expertos sobre el Sistema Integrado de Gestión de Tecnologías de la Información.

El último apartado de este trabajo corresponde a la validación de la propuesta en cumplimiento con el tercer objetivo de la investigación, donde se busca evaluar los resultados del Sistema Integrado de Gestión de TI a través del juicio de expertos, con el fin de determinar su pertinencia, claridad, aplicabilidad y coherencia. Este objetivo refleja la necesidad de someter el modelo planteado a la revisión crítica de profesionales con experiencia comprobada en seguridad de la información, gestión de servicios de TI y dirección tecnológica, garantizando así que la propuesta no permanezca únicamente en el plano teórico, sino que cuente con un respaldo académico y práctico que la haga viable en escenarios reales.

La definición de este apartado responde a la necesidad de contar con expertos que puedan evaluar la coherencia del sistema propuesto con los marcos normativos, su aplicabilidad práctica y su potencial para generar valor en las organizaciones. En esta línea, el Project Management Institute señala que, dada la naturaleza única y temporal de los proyectos, una de las estrategias más utilizadas consiste en reunir el juicio de expertos para “llenar los vacíos de información” y orientar la ejecución [65]. Bajo esta lógica, la validación integra miradas diversas y complementarias: la visión normativa y de cumplimiento, la experiencia en gestión de servicios y auditoría, y el enfoque técnico de quienes gestionan infraestructura crítica. Esta combinación enriquece el análisis, al asegurar que la propuesta se examine no solo desde la perspectiva de la norma, sino también desde la realidad práctica de las operaciones tecnológicas.

4.1. Metodología de validación

La validación del Sistema Integrado de Gestión de TI se enfocó en asegurar que el modelo propuesto no solo sea normativamente coherente, sino que también tenga aplicabilidad práctica desde las experiencias de profesionales cualificados. En este sentido, se adoptó la técnica de juicio de expertos, la cual permite verificar la validez de la investigación al apoyarse en el concepto de especialistas capaces de emitir juicios fundamentados sobre el área, entendida como “una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados en éste, y que pueden dar información, evidencia, juicios y valoraciones” [66].

En esta línea, resulta pertinente precisar que la “validez” constituye un criterio central en la investigación, entendido como el grado en que un instrumento de medición evalúa realmente aquello para lo cual fue diseñado y refleja con fidelidad el fenómeno que se pretende estudiar [67]. Al situar la validación del modelo bajo esta perspectiva, el juicio de expertos se convierte en la estrategia metodológica idónea, pues permite contrastar la coherencia y la pertinencia del sistema propuesto con la mirada de profesionales con trayectoria y conocimiento directo en la aplicación de normas y buenas prácticas.

Dentro de esta lógica, el juicio de expertos se aplica como estrategia para reforzar la validez de contenido, en especial cuando la investigación aún no ha sido implementada en escenarios reales. Al recurrir a profesionales con trayectoria y cercanía al despliegue de normas y prácticas, se obtiene un examen crítico que permite confirmar la pertinencia de los elementos incluidos, detectar posibles vacíos y garantizar que el modelo propuesto se ajuste a los marcos normativos y a la práctica organizacional.

El proceso de validación se concibió como un ejercicio progresivo que combinó instancias de interacción directa con espacios de evaluación estructurada. La primera fase permitió un acercamiento personal con cada experto para contextualizarlos en la propuesta, mientras que la segunda buscó consolidar sus valoraciones en un formato homogéneo y comparable. De esta manera, se garantizó que las observaciones recogidas fueran respondieron a las necesidades puntuales identificadas sobre la propuesta.

4.1.1. Selección y designación de expertos

Para garantizar la calidad y la pertinencia de la validación, se definieron criterios claros de selección de los participantes. Los tres expertos convocados cuentan con experiencia comprobada en la gestión de TI, seguridad de la información y gestión de calidad. Cada uno de ellos fue designado teniendo en cuenta su trayectoria académica, profesional y su cercanía con el despliegue de normas y prácticas de certificación, asegurando así la complementariedad de visiones en el proceso.

Con la intención de documentar de manera clara la idoneidad de cada evaluador, se elaboró una ficha técnica individual las cuales permiten evidenciar la pertinencia de los perfiles seleccionados y refuerzan la validez del proceso de juicio de expertos. A continuación, se presentan las tablas No. 10, 11, 12 y 13 correspondientes a cada uno de los expertos participantes:

Zully Escalona Silva	
Cargo Actual:	Consultor Sr en Ciberseguridad, Ciberresiliencia, gestión de TI y Continuidad de Negocios
Institución/empresa:	GM Sectec
Formación:	Ingeniero de Sistemas Magíster en Sistemas de la Calidad
Cursos complementarios:	* ITIL Foundation 4 * Lead Auditor ISO/IEC 27001:2022 * AL ISO 27000:2013 * Google Cloud Computing * Continuidad del Negocio y Recuperación ante Desastres (ISO 22301) * Desarrollo de inteligencia emocional
Experiencia en gestión de TI	Más de 15 años de experiencia liderando proyectos de gestión de servicios de TI, implementación de procesos basados en ITIL e integración de buenas prácticas en entidades financieras y de telecomunicaciones.
Experiencia en seguridad de la información	Diseño e implementación de modelos de seguridad alineados a ISO/IEC 27001 y PCI DSS. Liderazgo en gestión de activos de información, cumplimiento normativo y procesos de auditoría en seguridad.
Experiencia en gestión de servicios de TI	Amplia trayectoria en proyectos de optimización de centros de monitoreo de servicios, implementación de procesos de gestión de incidentes, cambios y problemas bajo ITIL.
Experiencia en continuidad de negocio	Especialista en continuidad (ISO 22301), con experiencia en diseño de planes de continuidad, ejecución de pruebas y construcción de estrategias de resiliencia organizacional.
Experiencia en consultoría y auditoría	Consultor en múltiples proyectos de certificación en seguridad, continuidad y gestión de servicios de TI en sectores financieros, telecomunicaciones y servicios de TI.
Pertinencia para el juicio de expertos	* Dominio en seguridad, continuidad y gestión de servicios. * Liderazgo en proyectos de certificación y cumplimiento normativo. * Relevancia temática: vinculación directa con la integración de normas ISO/IEC 27001 e ISO/IEC 20000. * Trayectoria consolidada en consultoría regional e internacional.

Zully Escalona Silva	
Rol dentro de la validación	Evaluar la solidez normativa y práctica de la propuesta, identificar barreras en la implementación real y aportar recomendaciones para fortalecer la integración en organizaciones complejas.

Tabla 10. Ficha técnica de expertos. Escalona, Z.

Andrés Silva Gómez	
Cargo Actual:	Co-Fundador & Chief Technology Officer
Institución/empresa:	OnePay (Fintech de pagos digitales)
Formación:	Ingeniero de sistemas Formación en emprendimiento y startups
Cursos complementarios:	* Fellow en Latitud (red de fundadores de alto impacto en LATAM) * Formación en liderazgo de equipos de ingeniería y desarrollo de productos digitales
Experiencia en gestión de TI	Más de 10 años de experiencia en desarrollo y liderazgo tecnológico en startups de base tecnológica y fintech. Ha liderado equipos de ingeniería en plataformas de comercio electrónico, pagos digitales y aplicaciones móviles de alto volumen transaccional.
Experiencia en seguridad de la información	Responsable del diseño y supervisión de arquitecturas seguras en fintechs y marketplaces, con experiencia en auditorías técnicas de cumplimiento PCI DSS Nivel 1, garantizando la seguridad de transacciones financieras en entornos críticos.
Experiencia en gestión de servicios de TI	Liderazgo en la implementación de plataformas escalables, resilientes y de alta disponibilidad en empresas como Rondoo, Frubana y OnePay, garantizando la continuidad de los servicios y la experiencia de usuario.
Desarrollos tecnológicos destacados	* Diseño e implementación de arquitecturas serverless y APIs de pagos * Desarrollo de la solución de pagos OnePay, adoptada por +20.000 comercios en LATAM, con mejoras de ~40% en conversión. * Liderazgo técnico en plataformas marketplace con rápidos ciclos de crecimiento y escalamiento. * Proyectos en Taxialife: diseño e implementación de soluciones de movilidad urbana (Co-Founder / CTO / Technical Lead): apps móviles, chatbots integrados a WhatsApp y Messenger, y sistemas IVR * Desarrollo e integración de aplicaciones móviles y sistemas backend escalables para clientes como PriceTravel, Globant y Koombear.
Pertinencia para el juicio de expertos	* Profundo dominio en arquitectura, seguridad y escalabilidad de plataformas. * Trayectoria en fintechs y startups con desafíos reales de disponibilidad y seguridad. * Aporta perspectiva operativa para verificar aplicabilidad del modelo en entornos críticos. * Fundador y líder técnico con resultados comprobables en producción.
Rol dentro de la validación	Evaluar la aplicabilidad técnica del modelo en entornos de alta criticidad, identificar riesgos operativos y proponer mitigaciones técnicas y mejoras para la integración con prácticas y controles normativos

Tabla 11. Ficha técnica de expertos. Silva, A.

Leidy Dayana Pérez Hernández	
Cargo Actual:	Líder de calidad – Líder de producción
Institución/empresa:	Sigma Ingeniería S.A.
Formación:	Administradora de sistemas informáticos Especialista en gerencia de proyecto
Cursos complementarios:	* Curso Implementador para la Norma ISO/IEC 9001:2015 * Auditor líder para la norma ISO/IEC 9001:2015 * Curso Power BI para la toma de decisiones

Leidy Dayana Pérez Hernández	
	<ul style="list-style-type: none"> * Seminario de actualización de las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 * Gestión del servicio - Requisitos del sistema de gestión del servicio ISO/IEC 20000-1 * Auditor interno de sistemas de gestión del servicio ISO/IEC 20000-1 * Curso indicadores de gestión * Formación de auditores internos en sistemas de gestión de seguridad en la información ISO/IEC 27001 * Diplomado: Desarrollo De Aplicaciones Web y Móviles * Diplomado en Sistemas Integrados de Gestión HSEQ con Formación de Auditores Internos ISO 9001:2015, ISO 14001:2015, ISO 45001: 2018 * Diplomado en Docencia Universitaria * Curso Oracle Database 12C – Introduction to SQL * Certificación en COBIT Foundation
Experiencia en gestión de TI	Más de 8 años liderando proyectos de TI, coordinación de equipos de desarrollo de software y gestión de calidad en procesos y productos.
Experiencia en seguridad de la información	Implementación y mantenimiento de sistemas de gestión de seguridad de la información bajo ISO/IEC 27001; auditorías internas y formación de equipos en buenas prácticas de seguridad.
Experiencia en gestión de servicios de TI	Diseño e implementación de procesos de gestión de servicios bajo ISO/IEC 20000-1; liderazgo en optimización de procesos y coordinación de equipos multidisciplinarios.
Experiencia en consultoría, auditoría o implementación de SG	Amplia experiencia en implementación y mejora de sistemas integrados de gestión bajo ISO 9001, ISO 20000-1, ISO 27001 e ISO 29110; auditorías internas y formación de auditores.
Pertinencia para el juicio de expertos	<ul style="list-style-type: none"> * Competencia técnica en normas ISO de gestión y seguridad de la información. * Experiencia práctica en proyectos de implementación y auditoría. * Relevancia temática en la integración de normas ISO. * Reconocimiento profesional mediante certificaciones y liderazgo.
Rol dentro de la validación	Contribuir con su criterio especializado para evaluar la coherencia normativa de la propuesta, identificar limitaciones de aplicabilidad en contextos reales y recomendar acciones de mejora para garantizar su implementación efectiva.

Tabla 12. Ficha técnica de expertos. Hernández, L.

Francisco Javier Valencia Duque	
Cargo Actual:	Profesor Titular – Facultad de Administración
Institución/empresa:	Universidad Nacional de Colombia, Sede Manizales
Formación:	PhD en Ingeniería – Industria y Organizaciones Magíster en Administración de TI Especialista en Diseño de Sistemas de Auditoría Ingeniero de Sistemas Administrador de Empresas
Cursos complementarios:	<ul style="list-style-type: none"> * CISA – Certified Information Systems Auditor (ISACA) * CRISC – Certified in Risk and Information Systems Control (ISACA) * COBIT Foundations Certificate * Lead Auditor ISO/IEC 27001 (ERCA) * ITIL Foundations v4
Experiencia en gestión de TI	Más de 20 años de experiencia en dirección académica, consultoría y proyectos relacionados con gobierno y gestión de TI, incluyendo la coordinación de auditoría y verificación en UNE EPM Telecomunicaciones.
Experiencia en seguridad de la información	Amplia trayectoria como consultor y auditor en proyectos basados en ISO/IEC 27001, gestión de riesgos de TI y seguridad de la información en organizaciones públicas y privadas.
Experiencia en gestión	Experiencia en auditoría y asesoría en empresas de telecomunicaciones,

Francisco Javier Valencia Duque	
de servicios de TI	energía y sector público, aplicando metodologías de gestión de servicios y estándares internacionales como ISO/IEC 20000.
Experiencia en consultoría, auditoría o implementación de SG	* Interventoría Fase II Transmilenio (proyecto de recaudo y control operacional) * Auditoría de sistemas de información en empresas de energía * Consultoría en implementación de sistemas integrados de riesgos y TI * director de proyectos de auditoría continua en organismos de control
Pertinencia para el juicio de expertos	Su formación doctoral, certificaciones internacionales y experiencia en investigación, docencia y proyectos aplicados en gestión de TI, riesgos y seguridad lo posicionan como un referente en la validación de propuestas metodológicas basadas en normas ISO.
Rol dentro de la validación	Experto evaluador, aportando juicio técnico sobre la integración de normas ISO/IEC 27001 e ISO/IEC 20000 desde la perspectiva de auditoría, gestión de riesgos y aplicabilidad académica-práctica.

Tabla 13. Ficha técnica de expertos. Valencia, F

4.1.2. Instrumentos empleados en la validación de los requisitos normativos de las normas NTC ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018

La validación se estructuró con base en dos instrumentos metodológicos complementarios que garantizaron tanto la comprensión del modelo como la recolección de las valoraciones expertas.

El primer instrumento correspondió a entrevistas semiestructuradas realizadas durante las sesiones iniciales con cada experto. Estas reuniones, de aproximadamente una hora, tuvieron como objetivo presentar el sistema integrado de gestión, explicar sus fundamentos metodológicos y resolver inquietudes específicas. Su carácter semiestructurado permitió mantener un guion de exposición general, pero dejando espacio para que los expertos formularan preguntas, señalaran vacíos y ofrecieran recomendaciones espontáneas, lo cual enriqueció el análisis desde la experiencia práctica de cada perfil.

El segundo instrumento aplicado consistió en un formulario en línea elaborado en Google Forms, cuyo contenido completo se encuentra en el ANEXO E. Este cuestionario se estructuró en torno a preguntas que buscaban identificar la percepción de los expertos respecto a la pertinencia, aplicabilidad y suficiencia del modelo propuesto. Entre ellas se incluyeron interrogantes cerrados, como la verificación de si el sistema integra de manera adecuada los requisitos de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018, así

como preguntas abiertas orientadas a recoger recomendaciones específicas sobre aspectos prácticos, limitaciones, acciones de mejora, aplicabilidad en distintos sectores y alternativas de validación.

La combinación de preguntas cerradas y abiertas permitió obtener, por un lado, respuestas homogéneas que confirmaron la coherencia del sistema, y por otro, apreciaciones cualitativas más detalladas que enriquecieron la interpretación de los resultados.

4.2. Resultados presentados tras la validación de los expertos

De manera general, los tres expertos coincidieron en que la propuesta metodológica integra de forma adecuada los requisitos de las normas ISO/IEC 27001 e ISO/IEC 20000, garantizando su coherencia tanto en el plano normativo como en el metodológico. Este hallazgo confirma la validez conceptual del modelo, al estar alineado con estándares internacionales de seguridad de la información y gestión de servicios de TI.

No obstante, la validación también permitió identificar aspectos críticos a fortalecer, especialmente para garantizar su aplicabilidad en escenarios reales:

- **Controles de seguridad de la información:** los expertos señalaron que, aunque la propuesta incluye un marco de seguridad, es necesario reforzar la definición, priorización y despliegue de los controles. Esto implica no solo enunciarlos, sino establecer claramente responsables, evidencias, periodicidad de ejecución y mecanismos de verificación.
- **Plan de implementación detallado:** uno de los puntos más recurrentes fue la necesidad de diseñar un plan estructurado que oriente la transición hacia el sistema integrado. Dicho plan debe contemplar fases progresivas, asignación de recursos, responsables y tiempos estimados. De este modo, se evita que la propuesta quede en un nivel meramente documental y se asegura su viabilidad operativa.
- **Aplicación de la estructura de alto nivel (HLS):** los expertos recomendaron dar mayor énfasis al uso de la HLS, ya que esta estructura común facilita la

integración de distintos sistemas de gestión, siendo integrable con cualquier norma ISO, reduce duplicidades en procesos y simplifica auditorías. Un aprovechamiento más explícito de la HLS permitirá que la propuesta sea más intuitiva y adaptable a diferentes organizaciones.

Respecto a las limitaciones de aplicación en entornos reales, se identificaron tres grandes retos:

1. **Complejidad en la integración de procesos diversos:** organizaciones con estructuras rígidas, jerárquicas o con alta resistencia al cambio pueden encontrar barreras importantes para adoptar un modelo integrado.
2. **Ausencia de un plan formal de seguimiento:** sin un esquema de control y monitoreo posterior a la implementación, el sistema puede diluirse con el tiempo o perder efectividad.
3. **Necesidad de una estrategia organizacional previa:** el modelo requiere un contexto de planificación estratégica definido, de lo contrario se corre el riesgo de que la integración carezca de orientación y no se articule con los objetivos institucionales.

En cuanto a acciones de mejora y oportunidades de integración, las recomendaciones más destacadas fueron:

- Definir indicadores de desempeño claros, así como mecanismos de medición continua para garantizar la mejora.
- Fortalecer la documentación y la unificación de procesos, lo que permitirá consolidar la trazabilidad y simplificar la gestión integrada.
- Realizar diagnósticos previos al despliegue, con el fin de adaptar la metodología a distintos contextos organizacionales y reducir riesgos de implementación.

Respecto a la aplicabilidad y replicabilidad del modelo, se coincidió en que puede potenciarse mediante:

- La incorporación de herramientas diagnósticas iniciales que permitan establecer el punto de partida de la organización.
- El desarrollo de procesos de socialización interna en diferentes niveles, generando apropiación del modelo.
- Una mayor flexibilidad metodológica, lo que facilita su ajuste a sectores y organizaciones de distinta naturaleza.

En síntesis, los resultados de la validación muestran que la propuesta tiene viabilidad conceptual y técnica, aunque requiere ajustes estratégicos y metodológicos que la preparen para un entorno real.

4.3. Recomendaciones

Del análisis comparado de las respuestas se derivan recomendaciones concretas que orientan la optimización de la propuesta:

1. **Planificación de la implementación:** Elaborar un plan estructurado que contemple fases de despliegue, asignación de recursos, responsables y cronograma. Este plan debe incluir también mecanismos de seguimiento y control, de manera que la integración no quede en lo documental, sino que se convierta en un proceso operativo y sostenible.
2. **Definición de indicadores de desempeño:** Incorporar métricas claras y medibles que permitan evaluar: El grado de integración entre los sistemas de gestión, a efectividad de los controles de seguridad de la información y la contribución del sistema a los objetivos estratégicos de la organización. Estos indicadores actuarán como un sistema de alerta temprana para identificar áreas de mejora y garantizar la mejora continua.
3. **Fortalecimiento documental:** Consolidar procesos, registros y evidencias en un esquema unificado, alineado con la estructura de alto nivel (HLS). Esto no solo simplifica auditorías y certificaciones, sino que también reduce la carga

documental innecesaria y facilita la comprensión del modelo por parte de los usuarios.

4. **Marco estratégico claro:** Garantizar que, antes de iniciar la implementación, la organización cuente con una estrategia clara y definida. Este marco estratégico debe servir como base para alinear la integración de los sistemas de gestión con los objetivos organizacionales, evitando esfuerzos aislados o desarticulados.

En conclusión, estas recomendaciones no solo validan la pertinencia de la investigación, sino que también aportan una hoja de ruta práctica para fortalecer el modelo y llevarlo del ámbito académico al terreno de la aplicación organizacional, asegurando su impacto real en la gestión de la información y de los servicios de TI.

5. Conclusiones

El desarrollo de esta investigación permitió demostrar que la estructuración de un Sistema Integrado de Gestión enfocado en TI, soportado en la integración de los marcos normativos ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018, constituye una alternativa viable para armonizar la seguridad de la información y la gestión de servicios de TI bajo un modelo unificado y coherente. A partir del análisis realizado y de la validación por juicio de expertos, se evidencia que el modelo propuesto logra responder a los objetivos planteados en la investigación, aportando un marco metodológico replicable y flexible.

En primer lugar, el estudio alcanzó el propósito de fundamentar el contexto teórico y normativo mediante la revisión narrativa de literatura, la cual permitió reconocer la relevancia de las normas ISO en la consolidación de buenas prácticas de gestión y seguridad. Esta revisión confirmó la necesidad de contar con propuestas metodológicas que reduzcan duplicidades, fortalezcan la trazabilidad y simplifiquen los procesos de auditoría y certificación en organizaciones con altos niveles de dependencia tecnológica.

En segundo lugar, la formulación de la propuesta metodológica mostró que es posible mapear y armonizar los requerimientos obligatorios de ambas normas, articulándolos en torno al ciclo PHVA. Este enfoque ofrece una estructura práctica y clara para implementar acciones de planeación estratégica, ejecución operativa, verificación del cumplimiento y mejora continua. No obstante, los expertos señalaron que, para lograr efectividad, el modelo debe complementarse con un plan de implementación detallado, el cual defina fases, recursos y responsables, evitando que se limite al plano documental.

En tercer lugar, la validación realizada mediante juicio de expertos permitió corroborar la coherencia técnica y normativa de la propuesta, al tiempo que puso en evidencia los retos más relevantes en su aplicación práctica. Entre ellos destacan la complejidad de integrar procesos en organizaciones rígidas, la ausencia frecuente de planes de

seguimiento y la necesidad de que las organizaciones cuenten con una estrategia institucional clara y definida que oriente la integración de los sistemas de gestión. Estos hallazgos no solo confirman la pertinencia del modelo, sino que también abren un espacio para futuras investigaciones enfocadas en estrategias de cambio organizacional y gestión del talento en entornos tecnológicos.

De manera transversal, las conclusiones reflejan que el aporte principal del trabajo consiste en una guía metodológica aplicable y adaptable. La propuesta no pretende ser un manual cerrado, sino un marco flexible que puede ajustarse a distintos sectores y niveles de madurez organizacional. En este sentido, se resalta la importancia de tres elementos críticos: la definición de indicadores de desempeño que midan la efectividad del sistema y orienten la mejora continua, la unificación documental como medio para garantizar trazabilidad y reducir cargas de gestión, y la incorporación de diagnósticos previos que permitan adaptar el modelo a cada contexto antes de su despliegue.

En síntesis, el trabajo confirma que la integración de normas internacionales bajo un Sistema Integrado de Gestión de TI es posible y pertinente, siempre que se combine el rigor metodológico con la flexibilidad necesaria para adaptarse a la realidad de las organizaciones. Así, se contribuye no solo al fortalecimiento de la gestión tecnológica, sino también a la construcción de un entorno organizacional más confiable, resiliente y orientado a la calidad en los servicios de TI.

ANEXO A: Correspondencia entre ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018

ISO/IEC 27001:2022	ISO/IEC 20000-1:2018
0. Introducción y 1. Objeto y campo de aplicación	
0.1. Generalidades	1.1. Generalidades
0.2. Compatibilidad con otras normas de Sistemas de gestión	1.2. Campo de aplicación
2. Referencias normativas	
3. Términos y definiciones	
<i>Nota: se aplican los términos y las definiciones dadas en la norma ISO/IEC 27000.</i>	3.1. Términos específicos de las normas de sistemas de gestión
	3.2. Términos específicos a la gestión del servicio
4. Contexto de la organización	
4.1. Comprensión de la organización y su contexto	
4.2. Comprensión de las necesidades y expectativas de las partes interesadas	
4.3. Determinación del alcance del Sistema de gestión de seguridad de la Información	4.3. Determinación del alcance del Sistema de Gestión de Servicios
4.4. Sistema de gestión de Seguridad de la Información	4.4. Sistema de Gestión del Servicio
5. Liderazgo	
5.1. Liderazgo y compromiso	
5.2. Política	5.2.1. Establecimiento y 5.2.2. Comunicación de la política de gestión del servicio
5.3. Roles, responsabilidades y autoridades de la organización	
6. Planificación	
6.1. Acciones para abordar riesgos y oportunidades	
6.1.1. Generalidades	6.1.1. Cuestiones para considerar.
6.1.2. Evaluación y 6.1.3. Tratamiento de riesgos de seguridad de la información	6.1.2. Determinar y documentación por parte de la organización
<i>Nota: En el contexto del numeral deben utilizarse los controles de seguridad de la información (se derivan directamente y están alineados con aquellos citados en los numerales 5 a 8)</i>	6.1.3. Planificación de la organización
6.2. Objetivos de seguridad de la información y planificación para alcanzarlos	6.2. Objetivos de la gestión del servicio y planificación para lograrlos
	6.2.1. Establecer objetivos
	6.2.2. Plan para logro de objetivos
6.3. Planificación de los cambios	6.3. Plan de gestión del servicio
7. Apoyo	
7.1. Recursos	
7.2. Competencia	

ISO/IEC 27001:2022	ISO/IEC 20000-1:2018
7.3. Toma de conciencia	
7.4. Comunicación	
7.5. Información documentada	
7.5.1. Generalidades	
7.5.2. Creación y actualización	
7.5.3. Control de la información documentada	
	7.6. Conocimiento
8. Operación	
8.1. Planificación y control operacional	
	8.2. Portafolio de servicios
	8.2.1. Entrega del servicio
	8.2.2. Plan de servicios
	8.2.3. Control de las partes involucradas en el ciclo de vida del servicio
	8.2.4. Gestión del catálogo de servicio
	8.2.5. Gestión del activo
	8.2.6. Gestión de configuración
	8.3. Relación y acuerdo
	8.3.1. General
	8.3.2. Gestión de relación con el negocio
	8.3.3. Gestión de nivel del servicio
	8.3.4. Gestión de proveedores
	8.3.4.1. Gestión de proveedores externos
	8.3.4.2. Gestión de proveedores internos y clientes actuando como un proveedor
	8.4. Oferta y demanda
	8.4.1. Presupuesto y contabilidad de los servicios
	8.4.2. Gestión de la demanda
	8.4.3. Gestión de la capacidad
	8.5. Diseño, desarrollo y transición del servicio
	8.5.1. Gestión del cambio
	8.5.1.1. Política de gestión del cambio
	8.5.1.2. Inicio de la gestión del cambio
	8.5.1.3. Actividades de la gestión del cambio
	8.5.2. Diseño y transición del servicio
	8.5.2.1. Plan de servicios nuevos y modificados
	8.5.2.2. Diseño
	8.5.2.3. Desarrollo y transición
	8.5.3. Gestión de liberación y despliegue
	8.6. Resolución y cumplimiento
	8.6.1. Gestión de incidentes
	8.6.2. Gestión de solicitudes de servicio
	8.6.3. Gestión de problemas
	8.7. Aseguramiento del servicio
	8.7.1. Gestión de disponibilidad del servicio
	8.7.2. Gestión de continuidad del servicio
8.2. Evaluación y 8.3. Tratamiento de riesgos de seguridad de la información	8.7.3. Gestión de seguridad de la información
	<i>Nota: Integración con la familia de normas ISO/IEC 27001:2022</i>

ISO/IEC 27001:2022	ISO/IEC 20000-1:2018
9. Evaluación de desempeño	
9.1. Seguimiento, medición, análisis y evaluación	
9.2. Auditoría interna	
9.2.1. Generalidades	
9.2.2. Programa de auditoría interna	
9.3. Revisión por la dirección	
9.3.1. Generalidades	
9.3.2. Entradas de la revisión por la dirección	
9.3.3. Salidas de la revisión por la dirección	
	9.4. Informes del servicio
10. Mejora	
10.1. Mejora continua	10.2. Mejora continua
10.2. No conformidad y acción correctiva	10.1. No conformidad y acción correctiva

Tabla 14. Tabla de correspondencia entre las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 (Elaboración propia)

A continuación, se referencian los controles de seguridad de la información presentados en la Norma ISO/IEC 27002:2022, los cuales se encuentran relacionados en la Tabla No. 15.

Controles Organizacionales		
5.1	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas asociadas deben ser definidas, aprobadas por la dirección, publicadas, comunicadas y reconocidas por el personal pertinente y partes interesadas pertinentes, y revisadas a intervalos planificados y cuando ocurran cambios significativos en la organización
5.2	Roles y responsabilidad en la seguridad de la información	Los roles y responsabilidades de seguridad de la información se deben definir y asignar de acuerdo con las necesidades de la organización.
5.3	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto deberían segregarse
5.4	Responsabilidades de la dirección	La Alta Dirección debe exigir a todo el personal la aplicación de la seguridad de la Información de acuerdo con la política de seguridad de la Información establecida, las políticas y los procedimientos específicos de la organización en los aspectos correspondientes
5.5	Contacto con las autoridades	La organización debe establecer y mantener contacto con las autoridades pertinentes.
5.6	Contacto con grupos de interés especial	La organización debe establecer y mantener contacto con grupos de interés especial u otros foros y asociaciones profesionales especializados en Seguridad
5.7	Inteligencia de amenazas	La información relativa a las amenazas a la seguridad de la información se debe recopilar y analizar para producir inteligencia de las amenazas.
5.8	Seguridad de la Información en la gestión de proyectos	La seguridad de la información se debe integrar en la gestión de proyectos.
5.9	Inventario de información y otros activos asociados	Se debe elaborar y mantener un inventario de la información y otros activos asociados, incluidos los propietarios
5.10	Uso aceptable de la información y otros activos asociados	Se deben identificar, documentar y implementar normas para el uso aceptable y procedimientos para el tratamiento de la información y otros activos asociados.

5.11	Devolución de activos	El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización en su posesión al cambiar o terminar su empleo, contrato o acuerdo.
5.12	Clasificación de la información	La información se debe clasificar de acuerdo con las necesidades de seguridad de la información de la organización sobre la base de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas
5.13	Etiquetado de la información	Se debe elaborar y implementar un conjunto adecuado de procedimientos para el etiquetado de la información de conformidad con el sistema de clasificación de la información adoptado por la organización
5.14	Transferencia de información	Las reglas, procedimientos o acuerdos de transferencia de información deben estar vigentes para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes
5.15	Control de acceso	Las normas para controlar el acceso físico y lógico a la información y otros activos asociados se deben establecer e implementar sobre la base de los requisitos de seguridad empresarial y de la información
5.16	Gestión de identidades	Se debe gestionar el ciclo de vida completo de las identidades
5.17	Información de autenticación	La asignación y gestión de la información de autenticación se debe controlar mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación
5.18	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados se deben aprovisionar, revisar, modificar y eliminar de acuerdo con la política y reglas específicas de la organización para el control de acceso
5.19	Seguridad de la información en las relaciones con proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Los requisitos pertinentes de seguridad de la información se deben establecer y acordar con cada proveedor en función del tipo de relación con el proveedor
5.2 1	Gestión de seguridad de la información en la cadena de suministro de TI y las telecomunicaciones (TIC)	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados a la cadena de suministro de productos y servicios de TIC.
5.2 2	Seguimiento, revisión y gestión del cambio de los servicios de los proveedores	La organización debe monitorear, revisar, evaluar y gestionar regularmente el cambio en las prácticas de seguridad de la información de los proveedores y la prestación de servicios.
5.2 3	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer, de acuerdo con los requisitos de seguridad de la información de la organización
5.2 4	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición, el establecimiento y la comunicación de procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.
5.2 5	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y debe decidir si clasificarse como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información se deben responder de conformidad con los procedimientos documentados
5.27	Aprender de los incidentes	Los conocimientos adquiridos a partir de incidentes de seguridad

	de seguridad de la información	de la información se deben utilizar para reforzar y mejorar los controles de seguridad de la información
5.28	Recopilación de evidencias	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
5.29	Seguridad de la información durante una interrupción	La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.
5.30	Preparación de las TIC para la continuidad de negocio	La preparación para las TIC se debe planificar, implementar, mantener y probar basado en los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC
5.31	Requisitos legales, legales, reglamentarios y contractuales	Los requisitos legales, reglamentarios y contractuales pertinentes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos se deben identificar, documentar y mantener actualizados.
5.32	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger derechos de propiedad intelectual
5.33	Protección de registros	Los registros deben estar protegidos contra pérdida, destrucción, falsificación, acceso y liberación no autorizados
5.34	Privacidad y protección de la información de identificación personal (PII, por sus siglas en inglés)	La organización debe identificar y cumplir con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y regulaciones aplicables y los requisitos contractuales
5.35	Revisión independiente de la seguridad de la información	El enfoque de la organización para administrar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se debe revisar de forma independiente a intervalos planificados o cuando ocurran cambios significativos.
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	El cumplimiento de la política de seguridad de la información, el tema, las políticas específicas, las reglas y los estándares de la organización se debe revisar periódicamente.
5.37	Procedimientos operativos documentados	Los procedimientos operativos de las instalaciones de procesamiento e la información se deben documentar y poner a disposición del personal que los necesite.
Controles de personas		
6.1	Selección	Las verificaciones de antecedentes de todos los candidatos para convertirse en personal se deben llevar a cabo antes de unirse a la organización y de forma continua teniendo en cuenta las leyes, regulaciones y ética aplicables y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
6.2	Términos y condiciones de empleo	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización para la seguridad de la información.
6.3	Conciencia de seguridad de la información, educación y formación	El personal de la organización y las partes interesadas pertinentes deben recibir información, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos del tema, según sea pertinente para su función laboral
6.4	Proceso disciplinario	Se debe formalizar y comunicar un proceso disciplinario para tomar medidas contra el personal y otras partes interesadas pertinentes que hayan cometido una violación de la política de seguridad de la información.
6.5	Responsabilidades después de la terminación o cambio de empleo	Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se debe definir, hacer cumplir y comunicar al personal

		pertinente y a otras partes interesadas.
6.6	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados y firmados periódicamente por el personal y otras partes interesadas pertinentes
6.7	Trabajo remoto	Las medidas de seguridad se deben implementar cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones
6.8	Informes de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe oportunamente sobre los eventos de seguridad de la información observados o sospechosos a través de los canales apropiados.
Controles Físicos		
7.1	Perímetros de seguridad física	Los perímetros de seguridad se deben definir y utilizar para proteger las zonas que contengan información y otros activos asociados.
7.2	Entrada física	Las zonas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.
7.3	Asegurar oficinas, habitaciones e instalaciones	Se debe diseñar e implementar la seguridad física de las oficinas, salas e instalaciones
7.4	Monitoreo de la seguridad física	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados
7.5	Protección contra amenazas físicas y ambientales	Se debe diseñar e implementar la protección contra las amenazas físicas y medioambientales, como las catástrofes naturales y otras amenazas físicas intencionadas o no intencionadas a las infraestructuras.
7.6	Trabajar en áreas seguras	Se deben diseñar e implementar medidas de seguridad para trabajar en zonas seguras
7.7	Escritorio y pantalla limpios	Se deben definir e implementar adecuadamente normas claras para los papeles y los soportes de almacenamiento extraíbles y normas claras sobre pantallas claras para las instalaciones de tratamiento de la información
7.8	Emplazamiento y protección de equipos	El equipo debe estar situado de forma segura y protegida
7.9	Seguridad de los activos fuera de las instalaciones	Los activos externos deben estar protegidos
7.10	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y disposición de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
7.11	Servicios públicos de apoyo	Las instalaciones de procesamiento de la información deben estar protegidas contra los cortes de energía y otras interrupciones causadas por fallos en los servicios públicos de apoyo.
7.12	Seguridad del cableado	Los cables que transporten energía, datos o servicios de información de apoyo deben estar protegidos contra la interceptación, las interferencias o los daños
7.13	Mantenimiento de equipos	El equipo se debe mantener correctamente para asegurar la disponibilidad, integridad y confidencialidad de la información
7.14	Disposición o reutilización segura de los equipos	Los elementos de los equipos que contengan medios de almacenamiento se deben verificar para asegurarse de que los datos sensibles y el software con licencia se han eliminado o sobrescrito de forma segura antes de su disposición o reutilización
Controles tecnológicos		
8.1	Dispositivos de punto final de usuario	Se debe proteger la información almacenada, procesada o accesible a través de los dispositivos de punto final del usuario.
8.2	Derechos de acceso	La asignación y el uso de los derechos de acceso privilegiado

	privilegiado	deben estar restringidos y gestionados.
8.3	Restricción de acceso a la información	El acceso a la información y a otros activos asociados se debe restringir de acuerdo con la política específica establecida sobre el control de acceso.
8.4	Acceso al código fuente	El acceso para leer o escribir sobre un código fuente, las herramientas de desarrollo, y las librerías de software se deben gestionar apropiadamente
8.5	Autenticación segura	Se deben implementar tecnologías y procedimientos de autenticación seguros basados en restricciones de acceso a la información y en la política específica del tema sobre control de acceso.
8.6	Gestión de la capacidad	El uso de los recursos se debe monitorear y ajustar en función de las necesidades de capacidad actuales y previstas.
8.7	Protección contra malware	La protección contra el malware se debe implementar y respaldar mediante la conciencia adecuada del usuario.
8.8	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben adoptar las medidas apropiadas.
8.9	Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes se deben establecer, documentar, implementar, monitorear y revisar.
8.10	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se debe eliminar cuando ya no sea necesario
8.11	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre control de acceso y otras políticas relacionadas con temas específicos, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
8.12	Prevención de fugas de datos	Las medidas de prevención de fugas de datos se deben implementar a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
8.13	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se deben mantener y probar periódicamente de conformidad con la política específica sobre copias de seguridad sobre temas específicos.
8.14	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de la información se deben implantar con redundancia suficiente para cumplir los requisitos de disponibilidad
8.15	Registro	Los registros que guarden actividades, excepciones, fallas y otros eventos pertinentes se deben producir, almacenar, proteger y analizar.
8.16	Actividades de seguimiento	Se debe monitorear el comportamiento anómalo de las redes, los sistemas y las aplicaciones y se deben adoptar las medidas adecuadas para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización se deben sincronizar con las fuentes de tiempo aprobadas
8.18	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan ser capaces de anular los controles del sistema y de la aplicación debe restringirse y controlarse estrictamente.
8.19	Instalación de software en sistemas operativos	Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de programas informáticos en los sistemas operativos.
8.20	Seguridad de redes	Las redes y los dispositivos de red deben estar asegurados,

		gestionados y controlados para proteger la información de los sistemas y las aplicaciones
8.21	Seguridad de los servicios de red	Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
8.22	Segregación de redes	Los grupos de servicios de información, los usuarios y los sistemas de información deben estar segregados en las redes de la organización.
8.23	Filtrado web	El acceso a sitios web externos se debe gestionar para reducir la exposición a contenido malicioso.
8.24	Uso de la criptografía	Se debe definir e implementar normas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	Se deben establecer e implementar normas para el desarrollo seguro de software y sistemas.
8.26	Requisitos de seguridad de las aplicaciones	Los requisitos de seguridad de la información se deben identificar, especificar y aprobar al desarrollar o adquirir aplicaciones.
8.27	Arquitectura de sistemas seguros y principios de ingeniería	Los principios para la ingeniería de sistemas seguros se deben establecer, documentar, mantener y implementar a cualquier actividad de desarrollo de sistemas de información.
8.28	Codificación segura	Los principios de codificación segura se deben implementar al desarrollo de programas informáticos.
8.29	Pruebas de seguridad en el desarrollo y aceptación	Los procesos de ensayo de seguridad se deben definir y implementar en el ciclo de vida del desarrollo
8.30	Desarrollo externalizado	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
8.31	Separación de entornos de desarrollo, evidencia y producción	Los entornos de desarrollo, ensayo y producción deben estar separados y protegidos.
8.32	Gestión del cambio	Los cambios en las instalaciones de procesamiento de la información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.
8.33	Información de las pruebas	La información de las pruebas se debe seleccionar, proteger y gestionar adecuadamente
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de los sistemas operativos se deben planificar y acordar conjuntamente entre el probador y la dirección adecuada

Tabla 15. Controles de Seguridad de la Información. Adaptado de [37]

ANEXO B: Matriz comparativa de requerimientos normativos ISO/IEC 27001:2022 – ISO/IEC 20000-1:2018

Con el fin de facilitar la comprensión del análisis de correspondencia, se adoptó un sistema de clasificación en el que cada requisito normativo se identifica con una letra según su grado de integración: **(I)** para los requisitos plenamente integrables, **(P)** para los parcialmente integrables y **(E)** para los requisitos exclusivos de cada norma. Esta codificación permite visualizar de manera rápida el nivel de coincidencia o diferenciación entre los capítulos analizados.

CAPITULO 4. CONTEXTO DE LA ORGANIZACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
4.1	Comprensión de la organización y su contexto. La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión. <i>Nota: Se refiere a los factores con impactos positivos o negativos</i>		I
4.2	Comprensión de las necesidades y expectativas de las partes interesadas La organización debe determinar: a. Las partes interesadas que son pertinentes para el sistema de gestión		I
	b. los requisitos pertinentes de estas partes interesadas		
	c. Cuáles de estos requisitos se abordarán a través del SGSI	<i>Nota: Los requisitos pueden incluir; servicio, desempeño, requisitos legales y obligaciones contractuales del sistema</i>	
4.3	Determinación del alcance del Sistema de Gestión. La organización debe determinar los límites y la aplicabilidad del sistema de gestión para establecer su alcance. Al determinar este alcance, la organización debe considerar:		E
	a. las cuestiones externas e internas mencionadas en el numeral 4.1		
	b. los requisitos mencionados en el numeral 4.2		
	c. las interfaces y dependencias entre las actividades realizadas por la organización y las realizadas por otras organizaciones.	c. los servicios prestados por la organización.	
	<i>Nota: El alcance debe estar disponible como información documentada.</i>		
	<i>Nota SGS: La definición del alcance debe incluir los servicios y el nombre de la organización que gestiona y presta los servicios. Puede corresponder a todos los servicios prestados por la organización, o a algunos de ellos. La norma ISO/IEC 20000-3 proporciona orientación sobre la definición del alcance</i>		
4.4	Sistema de Gestión. La organización debe establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.		P

Tabla 16. Capítulo 4. Contexto de la organización (Elaboración propia)

Nota: En el ANEXO C: Instructivo para el levantamiento del Contexto Organizacional y elementos de Gestión del Sistema Integrado, se incluyen instructivos y orientaciones que complementan la aplicación de este capítulo, cubriendo la mayoría de los puntos requeridos y facilitando su puesta en práctica.

CAPITULO 5. LIDERAZGO			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
5.1	Liderazgo y compromiso. La alta dirección debe demostrar su liderazgo y compromiso con respecto al Sistema de Gestión, mediante:		P
	a. Asegurar que la política y los objetivos sean compatibles con la dirección estratégica de la organización		
	b. Asegura la integración de los requisitos del sistema de gestión en los procesos de la organización		
	c. Asegurar la disponibilidad de los recursos necesarios para el sistema de gestión		
	d. Comunicando la importancia de la gestión eficaz, logrando los objetivos, entregando valor y cumpliendo los requisitos del SG		
	e. Asegurar que el sistema de gestión logre los resultados previstos		
	f. Dirigir y apoyar a las personas para que contribuyan a la eficacia del SG		
	g. Promover la mejora continua		
	h. Apoyando otras funciones de gestión pertinentes para demostrar su liderazgo en lo que respecta a sus áreas de responsabilidad.		
	5.2.1	<p>Nota: La referencia al "negocio" para ambas normas puede interpretarse de forma amplia para significar aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.</p>	
j. Asegurando que se asignen los niveles apropiados de autoridad para tomar decisiones			
k. Asegurando que se determine qué constituye valor para la organización y para sus clientes			
l. Asegurando que haya control de otras partes involucradas en el ciclo de vida del negocio			
Política. Establecimiento de la política de gestión. La alta dirección debe establecer una política de gestión que: a. sea apropiada para el propósito de la organización			
5.2.1	b. proporcione un marco para el establecimiento de los objetivos de la gestión del servicio y de la seguridad de la información		P
	c. incluya el compromiso de satisfacer los requisitos aplicables		
	d. incluya el compromiso de mejora continua		
5.2.2	Comunicación de la política de gestión debe:		I
	a. estar disponible como información documentada		
	b. comunicarse dentro de la organización		
	c. estar disponible para las partes interesadas, según corresponda.		

CAPITULO 5. LIDERAZGO			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
5.3	Roles, responsabilidades y autoridades de la organización		I
	La alta dirección debe asegurar que las responsabilidades y autoridades para los roles pertinentes son asignados y comunicados dentro de la organización.		
	La alta dirección debe asignar la responsabilidad y autoridad para:		
	a. asegurarse de que el sistema de gestión es conforme con los requisitos de este documento		
	b. informar sobre el desempeño del sistema de gestión a la alta dirección		
<i>Nota: La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión dentro de la organización.</i>			

Tabla 17. Capítulo 5. Liderazgo (Elaboración propia)

Nota: En el ANEXO C: Instructivo para el levantamiento del Contexto Organizacional y elementos de Gestión del Sistema Integrado, se incluyen instructivos y orientaciones que complementan la aplicación de este capítulo, cubriendo la mayoría de los puntos requeridos y facilitando su puesta en práctica.

CAPITULO 6. PLANIFICACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
6.1	Acciones para abordar riesgos y oportunidades		P
6.1.1	Generalidades. Al planificar el sistema de gestión, la organización debe considerar las cuestiones mencionadas en el numeral 4.1 y los requisitos mencionados en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan abordarse para:		
	a. Asegurar que el sistema de gestión pueda lograr sus resultados previstos		
	b. Prevenir o reducir los efectos no deseados		
	c. Lograr la mejora continua		
	La organización debe planificar:		
	a. Las acciones para abordar estos riesgos y oportunidades		
	b. La manera de integrar e implementar las acciones en sus procesos del sistema de gestión de seguridad de la información; y evaluar la eficacia de estas acciones		
	<i>Nota: las opciones para abordar los riesgos y las oportunidades pueden incluir: evitar el riesgo, tomar o incrementar el riesgo para buscar oportunidades, eliminar la fuente de riesgo, cambiar la probabilidad o la consecuencia de riesgo, mitigar el riesgo mediante acciones acordadas, compartir el riesgo o aceptar el riesgo con base en decisiones bien fundamentadas.</i>		
	La organización debe determinar y documentar		
	NA	a. Riesgos relacionados a:	
	1. La organización		
	2. No cumplir con los requisitos del servicio.		
	3. El involucramiento de otras partes en el ciclo de vida del servicio		
	b. El enfoque que se asume para la gestión de riesgos		
	c. El impacto de los riesgos y oportunidades para los SGS y los servicios a los clientes		

CAPITULO 6. PLANIFICACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
6.1.2	Evaluación del riesgo de seguridad de la información. La organización debe definir y aplicar un proceso de evaluación de riesgos de Seguridad de la Información que:	La metodología implementada para la evaluación de riesgos de seguridad de la información puede ser desplegada en la evaluación de riesgos en gestión del servicio	P
	a. Establezca y mantenga criterios de riesgo de SI que incluyan:		
	1. Los criterios de aceptación del riesgo		
	2. Los criterios para la realización de evaluaciones de riesgos para la SI		
	b. Asegure que las evaluaciones repetidas de los riesgos para la seguridad de la información produzcan resultados coherentes, válidos y comparables		
	c. Identifique los riesgos de la SI		
	1. Aplicar el proceso de evaluación de riesgos de SI para identificar los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del SGSI		
	2. Identificar a los propietarios de los riesgos		
	d. Analiza los riesgos de SI		
	1. Evalúe las consecuencias potenciales que se producirían si se materializaran los riesgos identificados en el numeral 6.1.2	NA	
	2. Evaluar la probabilidad realista de que se produzcan los riesgos identificados en el numeral 6.1.2		
	3. Determinar los niveles de riesgo		
	e. Valore los riesgos para la seguridad de la información		
	1. Comparar los resultados del análisis de riesgos con los criterios de riesgo establecidos en el numeral 6.1.2		
2. Priorizar los riesgos analizados para su tratamiento.			
La organización debe conservar información documentada sobre el proceso de evaluación de los riesgos para la seguridad de la información de la información.			
6.1.3	Tratamiento de los riesgos de seguridad de la información. La organización debe definir y aplicar un proceso de tratamiento de riesgos de SI para:	La metodología implementada para el tratamiento de riesgos de seguridad de la información puede ser desplegada en el tratamiento de riesgos identificados para la gestión del servicio	P
a. Seleccionar las opciones de tratamiento de riesgos de SI adecuadas, teniendo en cuenta los resultados de la evaluación de riesgos			

CAPITULO 6. PLANIFICACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
	<p>b. Determinar todos los controles necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información</p> <p><i>Nota: Las organizaciones pueden diseñar los controles necesarios o identificarlos a partir de cualquier fuente</i></p> <p>c. Comparar los controles determinados en el numeral anterior y verificar que no se ha omitido ningún control necesario</p> <p><i>Nota: Los controles de seguridad de la información no son exhaustivos y pueden incluirse controles de seguridad de la información adicionales si es necesario</i></p> <p>d. Producir una declaración de aplicabilidad que contenga: los controles necesarios, la justificación de su inclusión, si los controles necesarios están implementados o no, la justificación para excluir cualquiera de los controles</p> <p>e. Formular un plan de tratamiento de los riesgos de seguridad de la información</p> <p>f. Obtener, de parte de los dueños de los riesgos, la aprobación del plan de tratamiento de riesgos de la seguridad de la información, y la aceptación de los riesgos residuales de la SI</p> <p><i>Nota: El proceso de evaluación y tratamiento de los riesgos de seguridad de la información en este documento se alinea con los principios y directrices genéricas proporcionadas en la norma ISO 31000[5].</i></p>		
6.2	Objetivos y planificación para alcanzarlos		
	Establecer objetivos. La organización debe establecer objetivos en las funciones y niveles pertinentes.		P
	Los objetivos deben:		
	a. Ser coherentes con la política		
	b. Ser medibles (si es posible)		
6.2.1	c. Tener en cuenta los requisitos aplicables y los resultados de la evaluación y el tratamiento de riesgos		
	d. Ser monitoreados		
	e. Ser comunicados		
	f. Actualizarse cuando sea necesario		
	g. Estar disponibles como información documentada		
	La organización debe conservar información documentada sobre los objetivos		
6.2.2	Plan para el logro de objetivos. Cuando se hace la planificación para lograr sus objetivos, la organización debe determinar:		I
	a. Qué se hará		

CAPITULO 6. PLANIFICACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
	b. Qué recursos se necesitarán		
	c. Quién será el responsable		
	d. Cuándo se completará		
	e. Cómo se evaluarán los resultados		
	Planificación de los cambios	Plan de gestión del servicio	
	Quando la organización determine la necesidad de realizar cambios al sistema de gestión de seguridad de la información, éstos se llevarán a cabo de forma planificada.	La organización debe de crear, implementar y mantener un plan de gestión del servicio. La planificación debe de tener en cuenta la política de gestión de servicio, los objetivos de la gestión del servicio, los riesgos y las oportunidades, los requisitos del servicio especificados en este documento	
6.3	NA	El plan de gestión de servicio debe incluir los siguientes ítems o contener una referencia de ellos:	E
		a. Una lista de servicios	
		b. Las limitaciones conocidas que puedan afectar el SGS y los servicios	
		c. Las obligaciones tales como las políticas, las normas, los requisitos legales, de reglamentaciones y contractuales pertinentes, y cómo estas obligaciones se aplican al SGS y a los servicios	
		d. Las autoridades y las responsabilidades en relación con el SGS y los servicios	
		e. Los recursos humanos, técnicos, de información y financieros necesarios para operar el SGS y servicios	
		f. El enfoque que se asume con otras partes para trabajar con otras partes involucradas en el ciclo de vida del servicio	
		g. La tecnología utilizada para apoyar al SGS	
		h. Cómo se medirá, auditará, informará y mejorará la eficacia del SGS y de los servicios	
		Otras actividades de planificación deben mantener la alineación con el plan de gestión del servicio.	

Tabla 18. Capítulo 6. Planificación (Elaboración propia)

Nota: En el ANEXO C: Instructivo para el levantamiento del Contexto Organizacional y elementos de Gestión del Sistema Integrado, se incluyen instructivos y orientaciones que complementan la aplicación de este capítulo, cubriendo la mayoría de los puntos requeridos y facilitando su puesta en práctica.

CAPITULO 7. APOYO DEL SISTEMA DE GESTIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
7.1	Recursos. La organización debe determinar y proporcionar los recursos humanos, técnicos, de información y financieros necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión, para cumplir con los requisitos y lograr los objetivos de gestión.		I
7.2	Competencia. La organización debe: a. Determinar la competencia necesaria de la(s) persona(s) que realice(n) bajo su control un trabajo que afecte al desempeño y eficacia del sistema de gestión		I
	b. Asegurarse de que estas personas son competentes sobre la base de una educación, formación o experiencia adecuadas		
	c. Cuando proceda, tomar medidas para adquirir la competencia necesaria y evaluar la eficacia de las medidas adoptadas		
	d. Conservar la información documentada adecuada como evidencia de la competencia		
	<i>Nota: Las acciones aplicables pueden incluir, por ejemplo: la provisión de formación, la tutoría o la reasignación de los empleados actuales; o la contratación de personas competentes.</i>		
7.3	Toma de conciencia. Las personas que realizan trabajos bajo el control de la organización deben tomar conciencia de:		P
	a. La política de Seguridad de la Información	a. La política - los objetivos de gestión del servicio y los servicios pertinentes a su trabajo	
	b. Su contribución a la eficiencia del sistema de gestión, incluidos los beneficios de la mejora desempeño		
	c. Las implicaciones de la no conformidad con los requisitos del sistema de gestión		
7.4	Comunicación. La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión, incluyendo		I
	a. Sobre qué comunicar		
	b. Cuándo comunicar		
	c. Con quién comunicarse		
	d. Cómo comunicar		
	e. Quien es responsable de la comunicación		
	f. Quien comunica		
7.5	Información documentada		
7.5.1	Generalidades. El sistema de gestión de la organización debe incluir		P
	a. La información documentada requerida por este documento		
	b. La información documentada que la organización determine como necesaria para la eficiencia del sistema de gestión.		
	<i>Nota: El alcance de la información documentada para un sistema de gestión puede diferir de una organización a otra debido a: el tamaño de la organización y su tipo de actividades, procesos, productos y servicios, la complejidad de los procesos y sus interacciones; y la competencia de las personas</i>		
7.5.2	Creación y actualización. Cuando se crea y actualiza información documentada, la organización debe asegurar apropiadamente:		P
	a. Identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia)		
	b. El formato (por ejemplo, el idioma, la versión del software, los gráficos) y el medio (por ejemplo, papel, electrónico)		
	c. Revisión y aprobación de la idoneidad y adecuación.		

CAPITULO 7. APOYO DEL SISTEMA DE GESTIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
7.5.3	Control de la información documentada		P
	La información documentada requerida por el Sistema de Gestión y por este documento debe ser controlada para asegurarse de que:		
7.5.3.1	a. Está disponible y es adecuada para su uso, donde y cuando se necesite b. Está adecuadamente protegida (por ejemplo, contra pérdida de confidencialidad, uso indebido o pérdida de integridad)		
	Para el control de la información documentada, la organización debe abordar las siguientes actividades, según sea aplicable:		P
	a. Distribución, acceso, recuperación y uso		
	b. El almacenamiento y la preservación, incluida la preservación de la legibilidad		
	c. Control de cambios (por ejemplo, control de versiones)		
7.5.3.2	d. Retención y disposición		
	La información documentada de origen externo que la organización ha determinado que es necesaria para la planificación y operación del sistema de gestión, se debe identificar y controlar según sea apropiado		
	Nota: El acceso puede implicar una decisión sobre el permiso para ver la información documentada solamente, o el permiso y la autoridad para ver y cambiar la información documentada, etc.		
7.5.4	NA	Información documentada del sistema de gestión del servicio. La información documentada para el SGS debe de incluir: a. El alcance del SGS b. La política y los objetivos para la gestión del servicio c. El plan de gestión del servicio d. La política de gestión del cambio, la política de la seguridad e la información y los planes de la continuidad del servicio e. Los procesos del SGS de la organización f. Los requisitos del servicio g. El (los) catálogo(s) de servicios h. El (los) acuerdo(s) de nivel de servicio i. Los contratos con proveedores externos j. Los acuerdos con proveedores internos o clientes que actúan como proveedores k. Los procedimientos que exigen este documento l. Los registros exigidos para demostrar evidencia de conformidad con los requisitos de este documento o con el SGS de la organización Nota: El numeral 7.5.4 proporciona una lista de los documentos clave para un SGS. Existen otros requisitos especificados para la información se mantenga como info. documentada, por documentar o registrar. La norma ISO/ IEC 20000-2 proporciona orientación adicional	P

CAPITULO 7. APOYO DEL SISTEMA DE GESTIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
7.6	NA	Conocimiento. La organización debe de determinar y mantener el conocimiento necesario para apoyar la operación de los SGS y los servicios	P
		El conocimiento debe de ser pertinente, utilizable y estar disponible para las personas apropiadas	
		<i>Nota: el conocimiento es específico de la organización, SGS, servicios y partes interesadas. El conocimiento se utiliza y comparte para apoyar el logro de los resultados previstos y la operación del SGS y de los servicios.</i>	

Tabla 19. Capítulo 7. Apoyo del sistema de gestión. (Elaboración propia)

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
8.1		Planificación y control de la operación. La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos, y para implementar las acciones determinadas en el Numeral 6, mediante: Estableciendo criterios de desempeño para los procesos	P
		a. Implementando control de los procesos de acuerdo con los criterios.	
		b. los requisitos pertinentes de estas partes interesadas	
		c. El mantenimiento de la información documentada en la extensión necesaria para tener confianza de que los procesos se llevan a cabo según lo planeado.	
		La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando medidas para mitigar cualquier efecto adverso, según sea necesario.	
	La organización debe asegurarse de que se controlan los procesos, productos o servicios suministrados externamente que sean pertinentes para el sistema de gestión		
8.2	Evaluación de los riesgos para la seguridad de la información	Portafolio del servicio	P
8.2.1	La organización debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.	La organización debe operar el SMS asegurando la coordinación de las actividades y los recursos. La organización debe realizar las actividades requeridas para prestar los servicios.	E
		<i>Nota: Un portafolio de servicios se usa para gestionar el ciclo de vida de todos los servicios, incluidos los servicios propuestos, los que están en desarrollo, los que se están prestando y están definidos en los catálogos de servicios y los que se van a eliminar. La gestión del portafolio de servicios garantiza que el proveedor del servicio tenga la combinación adecuada de servicios. Las actividades del portafolio de servicios en este documento incluyen la planificación de los servicios, el control de las partes involucradas en el ciclo de vida del servicio, la gestión del catálogo de servicios, la gestión de activos y la gestión de la configuración.</i>	

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
8.2.2	NA	Planificación de los servicios	E
		Se deben determinar y documentar los requisitos del servicio para los servicios existentes, los servicios nuevos y los cambios hechos a los servicios.	
		La organización debe determinar la criticidad de los servicios en función de las necesidades de la organización, de los clientes, de los usuarios y de otras partes interesadas. La organización debe determinar y gestionar las dependencias y la duplicación entre servicios.	
		La organización debe proponer cambios cuando sea necesario, para alinear los servicios con la política de gestión del servicio, los objetivos de gestión del servicio y los requisitos del servicio, teniendo en cuenta las limitaciones y los riesgos conocidos.	
8.2.3	NA	Control de las partes involucradas en el ciclo de vida del servicio	E
8.2.3.1	NA	La organización es la que debe rendir cuentas por los requisitos especificados en este documento y por la prestación de los servicios, independientemente de qué parte esté involucrada en la realización de actividades que apoyen el ciclo de vida del servicio.	
		La organización debe determinar y aplicar criterios para la evaluación y la selección de otras partes involucradas en el ciclo de vida del servicio. Otras partes pueden ser un proveedor externo, un proveedor interno o un cliente que actúa como proveedor.	
		Las otras partes no deben prestar ni operar todos los servicios, componentes o procesos de servicio, dentro del alcance del SGS.	
		La organización debe determinar y documentar:	
		a. Los servicios prestados u operados por otras partes;	
b. Los componentes de servicio que prestan u operan otras partes;			
c. Los procesos o parte de ellos en el SGS de la organización, que son operados por otras partes.			

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		La organización debe integrar en el SGC los servicios, los componentes de servicio y los procesos que presta u opera la organización u otras partes para cumplir con los requisitos del servicio. La organización debe coordinar las actividades con otras partes involucradas en el ciclo de vida del servicio, incluida la planificación, el diseño, la transición, la prestación y la mejora de los servicios.	
8.2.3.2	NA	<p>La organización debe definir y aplicar controles pertinentes a otras partes, a partir de lo siguiente:</p> <p>a. La medición y evaluación del desempeño del proceso;</p> <p>b. La medición y la evaluación de la eficacia de los servicios y de los componentes del servicio para cumplir los requisitos del servicio</p>	E
8.2.4	NA	<p>Gestión del catálogo de servicios</p> <p>La organización debe crear y mantener uno o más catálogos de sus servicios. Estos catálogos de servicios deben incluir información para la organización, los clientes, los usuarios y otras partes interesadas, en los que se describan los servicios, los resultados esperados y las dependencias entre los servicios.</p> <p>La organización debe proporcionar acceso a las partes apropiadas de los catálogos de servicios a sus clientes, usuarios y otras partes interesadas.</p>	E
8.2.5	NA	<p>Gestión de activos</p> <p>La organización se debe asegurar de que los activos asegurados se gestionen para el cumplimiento de los requisitos del servicio y las obligaciones del numeral 6.3</p> <p><i>Nota: Consulte la gestión de la configuración cuando el activo también sea un elemento de configuración (EC)</i></p>	E
8.2.6	NA	<p>Gestión de la configuración</p> <p>Se deben definir los tipos de elementos de la configuración. Los servicios se deben de clasificar</p> <p>La información de la configuración se debe de registrar a un nivel de detalle apropiado a la criticidad y al tipo de servicios. El acceso a la información de la configuración debe de ser controlado. La información de la configuración registrada para EC debe incluir:</p> <p>a. Una identificación única</p> <p>b. El tipo EC</p>	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		<p>c. La descripción del EC</p> <p>d. Su relación con otros EC</p> <p>e. Su estado</p> <p>Los EC se deben de controlar. Los cambios en los EC deben de ser trazables y auditables para mantener la integridad de la información de la configuración.</p> <p>La organización debe de verificar, a intervalos planificados, la exactitud de la información de la configuración. Cuando se encuentran deficiencias, la organización debe de tomar las medidas necesarias.</p> <p>La información de la configuración debe de estar disponibles para otras actividades de gestión del servicio, según sea apropiado.</p>	
8.3	Tratamiento de riesgos de SI	Relación y acuerdo	P
	La organización debe implementar el plan de tratamiento de los riesgos para la SI	Generalidades. La organización puede usar proveedores para:	
8.3.1	La organización debe conservar información documentada de los resultados del tratamiento de los riesgos para la seguridad de la información.	<p>a. Prestar u operar servicios</p> <p>b. Proporcionar u operar componentes del servicio</p> <p>c. Operar procesos o partes de procesos que están en el SGS de la organización.</p>	E
8.3.2	NA	<p>Gestión de relación de negocios</p> <p>Se deben de gestionar e identificar los clientes y los usuarios de los servicios y otras partes interesadas en ellos. La organización debe asignar una o más personas responsables de gestionar las relaciones con los clientes y mantener la satisfacción de estos.</p> <p>La organización debe de establecer disposiciones para comunicarse con sus clientes y con otras partes interesadas. La comunicación debe promover la comprensión del entorno de negocio en evolución en el que operan los servicios y debe de permitir a la organización responder a los requisitos del servicio nuevo o modificado.</p> <p>La organización debe, a intervalos planificados, medir la satisfacción con los servicios tomando como base una muestra representativa de clientes. Los resultados se deben de analizar, revisar para identificar oportunidades de mejora e informar.</p> <p>Las quejas sobre el servicio se deben de registrar, gestionar hasta que se solucionen e informar. Cuando una queja sobre el servicio no se resuelva a través de los canales normales, se debe de proporcionar un</p>	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		método de escalamiento.	
8.3.3	NA	Gestión de nivel del servicio	E
		La organización y el cliente deben acordar los servicios que se presentarán.	
		Para cada servicio prestado, la organización debe crear uno o más ANS con base en los requisitos de servicios documentados. Los ANS deben de incluir los objetivos del nivel de servicio, los límites de carga de trabajo y las excepciones.	
		La organización debe, a intervalos planificados, hacer seguimiento, revisar e informar sobre:	
		a. El desempeño, con base en los objetivos del nivel de servicio	
		b. Los cambios reales y periódicos en la carga de trabajo en comparación con los límites de carga de trabajo de los ANS.	
		Cuando no se cumplen los objetivos del nivel de servicio, la organización debe identificar oportunidades de mejora.	
		<i>Nota el acuerdo sobre los servicios que se prestarán, establecido entre la organización y sus clientes, pueden ser de muchas formas, por ejemplo, puede ser: actas de un acuerdo verbal realizado en una reunión, un acuerdo informado por correo electrónico o un acuerdo con los términos del servicio.</i>	
8.3.4	NA	Gestión de proveedores	
8.3.4.1	NA	Gestión de proveedores externos	E
		La organización debe tener asignadas una o más personas responsables de gestionar la relación, los contratos y el desempeño de los proveedores externos.	
		La organización y el proveedor externo deben acordar un contrato documentado. Este contrato debe de incluir o contener una referencia a:	
		a. El alcance de los servicios, los componentes del servicio, los procesos o partes de los procesos que va a entregar u operar el proveedor externo	
		b. Los requisitos que ha de cumplir el proveedor externo	
c. Los objetivos del nivel de servicio u otras obligaciones contractuales;			
d. Las autoridades y responsabilidades de la organización y del proveedor externo			

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		<p>La organización debe evaluar la alineación de los objetivos del nivel de servicio o de otras obligaciones contractuales del proveedor externo, con base en los ANS con los clientes, y debe de gestionar los riesgos identificados.</p> <p>La organización debe de definir, y gestionar las interfaces con el proveedor externo</p> <p>La organización debe, a intervalos planificados, hacer seguimiento del desempeño de los proveedores externos. Cuando no se cumplan los objetivos del nivel de servicio u otras obligaciones contractuales, la organización debe asegurar que se identifiquen oportunidades de mejora.</p> <p>La organización debe, a intervalos planificados, revisar el contrato contra los requisitos de servicios actuales. Cuando se identifiquen cambios para incluir el contrato, antes de aprobarlos se deben evaluar en cuanto a su impacto en el SGS y los servicios.</p> <p>Las disputas entre la organización y el proveedor externo se deben registrar y gestionar hasta que se solucionen.</p>	
8.3.4.2	NA	<p>Gestión de proveedores internos y clientes actuando como un proveedor</p> <p>Para cada proveedor interno o cliente que actúe como proveedor, la organización debe desarrollar, acordar y mantener un acuerdo documentado para definir los objetivos del nivel de servicio, otros compromisos, actividades e interfaces entre las partes.</p> <p>La organización debe, a intervalos planificados, hacer seguimiento del desempeño del proveedor interno o cliente que actúe como proveedor. Cuando no se cumplan los objetivos del nivel de servicios u otros compromisos acordados, la organización debe asegurar que se identifiquen oportunidades de mejora.</p>	E
8.4	NA	Oferta y demanda	
8.4.1	NA	<p>Presupuesto y contabilidad de los servicios</p> <p>La organización debe contar con un presupuesto y se debe llevar la contabilidad de los servicios o grupos de servicios de acuerdo con sus políticas y procesos de gestión financiera.</p> <p>Los costos se deben presupuestar para posibilitar un control financiero y toma de decisiones eficaces en relación con los servicios.</p>	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		La organización debe, con intervalos planificados, hacer seguimiento e informar los costos reales en comparación con el presupuesto, revisar las previsiones financieras y gestionar los costos.	
8.4.2	NA	<p>Gestión de la demanda</p> <p>A intervalos planificados, la organización debe:</p> <p>a. determinar la demanda actual y pronosticar la demanda futura de servicios</p> <p>b. hacer seguimiento e informar sobre la demanda y el consumo de servicios</p> <p><i>Nota la gestión de la demanda es responsable de comprender la demanda actual y futura de los clientes en relación con los servicios. La gestión de la capacidad trabaja con la gestión de la demanda para planificar y proporcionar la capacidad suficiente para satisfacer la demanda.</i></p>	E
8.4.3	NA	<p>Gestión de la capacidad</p> <p>Los requisitos de capacidad en relación con los recursos humanos, técnicos, de información y financieros se deben determinar, documentar y mantener teniendo en cuenta los requisitos de servicio y el desempeño.</p> <p>La organización debe de planificar su capacidad para incluir:</p> <p>a. la capacidad actual y prevista en función de la demanda de los servicios;</p> <p>b. El impacto esperado sobre la capacidad e los objetivos del nivel de servicio acordados, sobre los requisitos de disponibilidad del servicio y sobre la continuidad del servicio</p> <p>c. Cronogramas de tiempo y umbrales para cambios en la capacidad del servicio</p> <p>La organización debe de proporcionar la capacidad suficiente para cumplir los requisitos de capacidad y de desempeño acordados, y debe hacer seguimiento del uso de la capacidad, analizar la capacidad, y los datos de desempeño e identificar oportunidades para mejorar el desempeño.</p>	E
8.5	NA	Diseño, construcción y transición del servicio	
8.5.1	NA	Gestión del cambio	
8.5.1.1	NA	<p>Política de gestión del cambio</p> <p>Se debe de establecer y documentar una política de gestión del cambio que defina:</p> <p>a. Los componentes del servicio y otros elementos que están bajo el control de la gestión del cambio;</p>	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		b. Las categorías del cambio, que incluya los cambios de emergencia, y cómo se ha de gestionar c. Los criterios para determinar los cambios con el potencial de tener un impacto importante en los clientes o servicios.	
8.5.1.2	NA	Inicio de la gestión del cambio La organización debe de usar el diseño del servicio y la transición mencionados en el numeral 8.5.2 para: a. Nuevos servicios con potencial de tener un impacto importante en los clientes, u otros servicios según lo determinado por la política de gestión de cambio b. Cambios en los servicios con potencial de tener un impacto importante en los clientes, u otros servicios según lo determinado por la política de gestión cambio c. Categorías de cambio que van a hacer gestionadas mediante el diseño y la transición del servicio de acuerdo con la política de gestión del cambio d. Eliminación de un servicio e. Transferencia de un servicio existente de la organización a un cliente u otra parte f. transferencia de un servicio existente de un cliente u otra parta de la organización. La evaluación, aprobación, programación y revisión de los servicio nuevos y modificados en el alcance del numeral 8.5.2 se deben gestionar mediante las actividades de gestión del cambio mencionadas en el numeral 8.5.1.3	E
8.5.1.3	NA	Actividades de gestión del cambio La organización y las partes interesadas deben de tomar decisiones sobre la aprobación y la prioridad de las solicitudes de cambio. Al tomar decisiones se deben tener en cuenta los riesgos, beneficios para el negocio, la viabilidad y el impacto financiero. Además. al tomar decisiones también se deben de considerar los impactos potenciales del cambio en: a. los servicios existentes b. los clientes, usuarios y otras partes interesadas c. las políticas y planes exigidos en este documento d. la capacidad, la disponibilidad del servicio y la seguridad de la información; e. otras solicitudes de cambios, versiones y planes de implementación	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		<p>Los cambios aprobados se deben de preparar, verificar y, cuando sea posible, ponerse a prueba. Las fechas propuestas para la implementación y otros detalles de ella en relación con los cambios aprobados se deben comunicar a las partes interesadas</p> <p>Las actividades para revertir o corregir un cambio no exitoso se debe de planificar y, cuando sea posible, se deben de poner a prueba. Los cambios no exitosos se deben de investigar y se deben de emprender las acciones acordadas.</p> <p>La información de la configuración se debe de actualizar después de la implementación de los cambios de los EC.</p> <p>La organización debe revisar los cambios para determinar su eficacia y tomar las medidas acordadas con las partes interesadas.</p>	
8.5.2	NA	Diseño y transición del servicio	
		Plan de servicios nuevos y modificados	
		En la planificación se deben usar los requisitos del servicio para los servicios nuevos o modificados determinados en el numeral 8.2.2 y se deben incluir los siguientes elementos o una referencia a ellos:	
		a. Las autoridades y responsabilidades para las actividades de diseño, construcción y transición	
		b. Las actividades que realizará la organización u otras partes, con sus cronogramas;	
		c. Los recursos humanos, técnicos, de información y financieros;	
		d. Las dependencias de otros servicios;	
		e. Las pruebas necesarias para los servicios nuevos o modificados;	
		f. Los criterios de aceptación de servicios	
		g. Los resultados previstos de la prestación de los servicios nuevos o modificados, expresados en términos medibles;	
		h. El impacto en el SGS, en otros servicios, en los cambios planificados, en los clientes, en los usuarios y en otras partes interesadas	
8.5.2.1	NA	Para los servicios que se vayan a retirar, la planificación debe de incluir además las fechas para el retiro de los servicios y para las actividades de archivo, eliminación o transferencia de datos, información documentada y componentes del servicio.	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		Para los servicios que vayan a transferir, la planificación debe de incluir además las fechas para la transferencia de los servicios y actividades para la transferencia de datos, información documentada, conocimiento y componentes del servicio.	
		Los EC afectados por los servicios nuevos o modificados se deben abordar por medio de la gestión de la configuración	
8.5.2.2	NA	<p>Diseño</p> <p>Los servicios nuevos o modificados se deben diseñar y documentar para cumplir con los requisitos del servicio documentados en el numeral 8.2.2 el diseño debe de incluir los elementos pertinentes de los siguientes:</p> <p>a. las autoridades y responsabilidades de las partes involucradas en la prestación de los servicios nuevos o modificados;</p> <p>b. los requisitos relativos a cambios en los recursos humanos, técnicos, de información y financieros</p> <p>c. los requisitos relativos a una educación, formación y experiencia apropiadas;</p> <p>d. ANS, contratos y otros acuerdos documentados, nuevos y modificados, que respalden los servicios;</p> <p>e. cambios en el SGS, incluidas las políticas, los planes, los procesos, los procedimientos, las medidas y los conocimientos, nuevos y modificados;</p> <p>f. el impacto en otros servicios;</p>	E
8.5.2.3	NA	<p>Construcción y transición</p> <p>Los servicios nuevos o modificados se deben construir y poner a prueba para verificar que cumplen con los requisitos del servicio, con el diseño documentado y con los criterios de aceptación del servicio acordados. Si no se cumplen los criterios de aceptación del servicio, la organización y las partes interesadas deben tomar decisiones sobre las acciones necesarias y su implementación.</p> <p>La gestión de liberación y despliegue se debe usar para implementar servicios nuevos o modificados aprobados en el entorno de producción.</p> <p>Una vez finalizadas las actividades de transición, la organización debe de informar a las partes interesadas sobre los logros en relación con resultados previstos.</p>	E
8.5.3	NA	<p>Gestión de liberación y despliegue</p> <p>La organización debe definir los tipos de liberación, incluida la liberación de emergencia, su frecuencia y la forma en que se va a gestionar.</p>	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		<p>La organización debe de planificar el despliegue de los servicios nuevos o modificados y de componentes del servicio en el entorno de producción. La planificación se debe coordinar con la gestión del cambio y debe de incluir referencias a las solicitudes de cambio relacionadas, los errores o problemas conocidos que se cierran por medio de la liberación</p> <p>La planificación debe incluir las fechas para el despliegue de cada liberación, entregables y métodos de despliegue</p> <p>La liberación se debe de verificar contra criterios de aceptación documentados y se debe aprobar antes del despliegue. Si no se cumplen los criterios de aceptación, la organización, y las partes interesadas deben tomar una decisión sobre las acciones necesarias y sobre el despliegue</p> <p>Previo al despliegue de una liberación en el entorno de producción, se debe de tomar una línea base de los elementos de configuración afectados.</p> <p>La liberación se debe desplegar en el entorno de producción de manera que se mantenga la integridad del servicio o de los componentes del servicio.</p> <p>El éxito o falla de las liberaciones se debe monitorear y analizar. Las mediciones deben incluir los incidentes relacionados con una liberación en el período posterior al despliegue de una liberación. Los resultados y conclusiones extraídos del análisis se deben registrar y revisar para identificar oportunidades de mejora.</p> <p>La información sobre el éxito o el fracaso de las liberaciones y las fechas de las futuras de liberación se debe de poner a disposición para otras actividades de gestión del servicio, según corresponda.</p>	
8.6	NA	Resolución y cumplimiento	
		Gestión de incidentes	
		Los incidentes se deben	
		a. registrar y clasificar	
		b. priorizar, teniendo en cuenta el impacto y la urgencia;	
		c. escalar, si es necesario;	
		d. solucionar;	
		e. cerrar	
		Los registros de incidentes se deben actualizar con las acciones tomadas	
8.6.1	NA		E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		La organización debe determinar los criterios para identificar un incidente importante. Los incidentes mayores se deben de clasificar y gestionar de acuerdo con un procedimiento documentado. Se debe mantener informada la alta dirección sobre incidentes importantes. La organización debe asignar la responsabilidad de la gestión de cada incidente importante. Una vez resuelto el incidente, el incidente principal se debe informar y revisar para identificar oportunidades de mejora.	
8.6.2	NA	<p>Gestión de solicitudes de servicio</p> <p>Las solicitudes de servicio se deben:</p> <ul style="list-style-type: none"> a. registrar y clasificar; b. priorizar; c. cumplir; d. Cerrar. <p>Los registros de las solicitudes de servicio se deben actualizar en las acciones tomadas.</p> <p>Las instrucciones para el cumplimiento de las solicitudes de servicio se deben de poner a disposición de las personas involucradas en el cumplimiento de solicitudes de servicio.</p>	E
8.6.3	NA	<p>Gestión de problemas</p> <p>Para identificar los problemas, la organización debe analizar los datos y las tendencias en los incidentes. La organización debe llevar a cabo un análisis de la causa de raíz y determinar las posibles acciones para prevenir que ocurran incidentes o que se repitan.</p> <ul style="list-style-type: none"> a. registrar y clasificar; b. priorizar; c. escalar, si es necesario; d. resolver, si es posible; e. cerrar. <p>los registros de los problemas se deben actualizar con las acciones tomadas. Los cambios necesarios para la resolución de los problemas se deben gestionar de acuerdo con la política de gestión del cambio.</p>	E

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		<p>Cuando se haya identificado la causa raíz, pero no se haya resuelto el problema en forma permanente, la organización debe determinar las acciones para reducir o eliminar el impacto del problema sobre los servicios. Se deben registrar los errores conocidos y se debe poner a disposición de las otras actividades de gestión de información actualizada sobre los errores conocidos y la resolución de problemas,</p> <p>Se debe hacer seguimiento, revisar e informar la eficacia de la resolución de problemas, a intervalos planificados.</p>	
8.7	NA	Aseguramiento del servicio	E
8.7.1	NA	Gestión de disponibilidad del servicio	
		Se deben evaluar y documentar los riesgos para la disponibilidad del servicio, a intervalos planificados. La organización debe determinar los requisitos y los requisitos de disponibilidad del servicio. Los requisitos acordados deben tener en cuenta los requisitos de negocio pertinentes, los requisitos del servicio, los ANS y los riesgos.	
		Documentar y mantener los requisitos y los objetivos de disponibilidad de servicio.	
		<p>Seguimiento de la disponibilidad del servicio, y los resultados se deben registrar y comparar con los objetivos. Se debe investigar la falla de disponibilidad no planificada y emprender las acciones necesarias.</p> <p><i>Nota Los riesgos identificados en el numeral 6.1 pueden proporcionar entradas sobre los riesgos para la disponibilidad del servicio, la continuidad del servicio y la seguridad de la información.</i></p>	
8.7.2	NA	Gestión de la continuidad del servicio	E
		Se deben evaluar y documentar los riesgos del servicio, a intervalos planificados. La organización debe determinar los requisitos para la continuidad del servicio. Los requisitos acordados deben tener en cuenta los requisitos pertinentes del negocio, los requisitos del servicio, los ANs y los riesgos.	
		La organización debe crear, implementar y mantener uno o más planes de continuidad del servicio. El(los) plan (es) de continuidad del servicio deben de incluir los siguientes elementos o contener una referencia a ellos:	
		<p>a. los criterios y las responsabilidades para invocar la continuidad del servicio;</p> <p>b. los procedimientos para implementar en caso de una pérdida importante en el servicio;</p>	

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		<p>c. los objetivos de la disponibilidad del servicio cuando se invoca el plan de continuidad del servicio;</p> <p>d. los requisitos para la recuperación del servicio;</p> <p>e. los procedimientos para regresar a las condiciones normales de trabajo.</p> <p>El(los) plan (es) de continuidad del servicio se deben poner a prueba contra los requisitos para a la continuidad del servicio, a intervalos planificados. El plan de continuidad del servicio se debe poner a prueba nuevamente después de realizar cambios importantes en el entorno del servicio, y se deben registrar los resultados de estas pruebas. Se deben hacer revisiones después de cada prueba y después de que se hayan invocado los planes de continuidad del servicio. Cuando se encuentran deficiencias, la organización debe tomar las medidas necesarias.</p> <p>Cuando se haya(n) invocado El(los) plan (es) de continuidad del servicio, la organización debe informar sobre la causa, el impacto y la recuperación.</p>	
8.7.3	Gestión de seguridad de la información		
	Política de seguridad de la información		
	La dirección con la autoridad apropiada debe aprobar una política de seguridad pertinente para la organización. Esta política de seguridad de la información se debe documentar y debe tener en cuenta los requisitos del servicio y las obligaciones del numeral 6.3 c).		
8.7.3.1	La política de seguridad de la información debe estar disponible según corresponda. La organización debe comunicar la importancia de cumplir con la política de seguridad de la información y su aplicabilidad para el SGS y los servicios, a las personas apropiadas:		I
	a. en la organización		
	b. los clientes y los usuarios;		
	c. los proveedores externos, los proveedores internos y otras partes interesadas.		
	Controles de seguridad de la información		
	Se deben evaluar y documentar los riesgos de seguridad de la información para el SGS y los servicios, a intervalos planificados. Los controles de seguridad de la información se deben determinar, implementar, y operar para respaldar la política de seguridad de la información y hacer frente a los riesgos de seguridad de la información identificados. Las decisiones sobre los controles de seguridad de la información se deben documentar.		I
8.7.3.2	La organización debe acordar e implementar controles de seguridad de la información para hacer frente a los riesgos de seguridad de la información relacionados con organizaciones externas.		
	La organización debe hacer seguimiento y revisar la eficacia de los controles de seguridad de la información y tomar las acciones necesarias.		
	Incidentes de seguridad de la información		
8.7.3.3	Los incidentes de la seguridad de la información se deben:		I
	a. registrar y clasificar;		
	b. priorizar, teniendo en cuenta el riesgo de seguridad de la información;		

CAPITULO 8. OPERACIÓN			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
	c. escalar, si es necesario;		
	d. resolver y cerrar		
	La organización debe analizar los incidentes de seguridad de la información por tipo, volumen e impacto en el SGS, en los servicios y en las partes interesadas. Los incidentes de seguridad de información se deben de informar y revisar para identificar oportunidades de mejora.		
	Nota: La serie ISO/ IEC 27000 especifica los requisitos y proporciona orientación para apoyar la implementación y la operación de un sistema de gestión de la seguridad de la información. La Norma ISO/IEC 27013 proporciona orientación sobre la integración de las normas ISO/ IEC 27001 e ISO/ IEC 20000-1		

Tabla 20. Capítulo 8. Operación. (Elaboración propia)

CAPITULO 9. EVALUACIÓN DEL DESEMPEÑO			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
9.1	Seguimiento, medición, análisis y evaluación. La organización debe determinar:		I Puede hacerse transv.
	a. Qué necesita seguimiento y ser medido, incluidos los procesos y controles		
	b. Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos. Los métodos seleccionados deberían producir resultados comparables y reproducibles para ser considerados válidos		
	c. Cuándo se debe realizar el seguimiento y la medición		
	d. Quién debe realizar el seguimiento y la medición		
	e. cuándo se deben analizar y evaluar los resultados del seguimiento y la medición		
	f. quién analizará y evaluará estos resultados	La organización debe de evaluar el desempeño del Sistema de Gestión del Servicio contra los objetivos del sistema y evaluar la eficacia del Sistema de Gestión del Servicio	
	La organización debe evaluar el desempeño de la seguridad de la información y la eficiencia del sistema de gestión de seguridad de la información.		
	Se debe disponer de información documentada como evidencia de los resultados		
9.2	Auditoría interna		P
9.2.1	Generalidades. La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión		
	a. Es conforme con:		
	1. Los requisitos propios de la organización para su sistema de gestión		
	2. Los requisitos de la norma		
	b. Se implementa y mantiene eficazmente		
9.2.2	Programa de auditoría interna. La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo frecuencia, métodos, responsabilidades, requisitos de planificación e informes.		I
	Al establecer el programa o programas de auditoría interna, la organización debe considerar la importancia de los procesos involucrados, los cambios que afecten a la organización y los resultados de las auditorías previas. La organización debe:		
	a. Definir los criterios de auditoría y el alcance de cada auditoría		
	b. Seleccionar a los auditores y realizar auditorías que aseguren la objetividad e imparcialidad del proceso de auditoría		

CAPITULO 9. EVALUACIÓN DEL DESEMPEÑO			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
	c. Asegurarse de que los resultados de las auditorías se comunican a la dirección pertinente		
	e. Se debe disponer de información documentada como evidencia de la implementación del (los) programa (s) de auditoría y de los resultados de auditoría.		
9.3	Revisión por la dirección		I
9.3.1	Generalidades. La alta dirección debe revisar el sistema de gestión de la organización a intervalos planificados para asegurar su continua conveniencia, adecuación, eficacia y alineación continuas.		
9.3.2	Entradas de la revisión por la dirección. La revisión por la dirección debe considerar:		P
	a. El estado de las acciones provenientes de previas revisiones por la dirección		
	b. Los cambios en las cuestiones externas e internas que sean pertinentes para el sistema de gestión		
	c. Los cambios en las necesidades y expectativas de las partes interesadas que sean pertinentes		
	d. La retroalimentación sobre el desempeño y eficacia del sistema de, incluyendo las tendencias en:		
	1. Las no conformidades y las acciones correctivas		
	2. Los resultados del seguimiento y la medición		
	3. Resultados de las auditorías		
	4. El cumplimiento de los objetivos		
	e. La retroalimentación de las partes interesadas		
	f. Los resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos, junto con la eficacia de las acciones tomadas		
NA	g. Las oportunidades de mejora continua		
	h. La adherencia e idoneidad de la política de gestión del servicio		
	i. El desempeño de los servicios		
	j. Niveles de recursos humanos, técnicos, de información y financieros actuales y previstos y las capacidades de recursos humanos y técnicos.		
	k. Los cambios que pueden afectar el SGS y los servicios		
9.3.3	Salidas de la revisión por la dirección. Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el sistema de gestión		P
	Se debe tener disponible información documentada como evidencia de los resultados de las revisiones por la dirección.		
9.4	NA	Informes del servicio. La organización debe determinar los requisitos de presentación de informes y el propósito de estos	E
		Los informes sobre el rendimiento y la eficacia del SGS y los servicios se deben elaborar utilizando la información de las actividades del SGS y la prestación de los servicios. Los informes de servicios deben de incluir las tendencias	

CAPITULO 9. EVALUACIÓN DEL DESEMPEÑO			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
		La organización debe tomar decisiones y emprender acciones basadas en los hallazgos en los informes de servicios. Las acciones acordadas se deben comunicar a las partes interesadas	

Tabla 21. Capítulo 9. Evaluación de desempeño. (Elaboración propia)

CAPITULO 10. MEJORA			
No.	ISO/IEC 27001:2022	ISO/IEC 20000-1:2018	
10.1	No conformidad, acción correctiva. Cuando ocurra no conformidad, la organización debe		I
	a. Reaccionar ante la no conformidad y, cuando sea aplicable		
	1. Tomar acciones para controlarla y corregirla		
	2. Hacer frente a las consecuencias		
	b. Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante		
	1. La revisión de la no conformidad		
	2. Determinando las causas de la no conformidad		
	3. Determinando si existen no conformidades similares, o que potencialmente podrían ocurrir		
	c. Implementar cualquier acción necesaria		
	d. Revisar la eficacia de cualquier acción correctiva tomada		
	e. Hacer cambios en el sistema de gestión, si es necesario		
	Las acciones correctivas deben ser apropiadas para los efectos de las no conformidades encontradas.		
	La información documentada debe estar disponible como evidencia de:		
	a. La naturaleza de las no conformidades y cualquier acción subsecuente tomada		
b. Los resultados de cualquier acción correctiva.			
10.2	Mejora continua. La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión.		I
	La organización debe determinar criterios de evaluación que se aplicarán a las oportunidades de mejora, cuando se toman decisiones sobre su aprobación. Los criterios de evaluación deben incluir la alineación de la mejora con los objetivos		
	Las oportunidades de mejora deben de estar documentadas. La organización debe:		
	a. Establecer objetivos de mejora de alguno de los siguientes ítems, o en varios de ellos: Calidad, valor, capacidad, costo, productividad, utilización de recursos y reducción de riesgos		
	b. Asegurar que las mejoras sean priorizadas, planificadas e implementadas		
	c. Hacer cambios del SGS, si es necesario		
	d. Medir las mejoras implementadas contra los objetivos establecidos y cuando no se cumplan los objetivos, tomar las medidas necesarias		
	e. Informar sobre las mejoras implementadas		
Nota: las mejoras pueden incluir acciones reactivas y proactivas tales como corrección, acción correctiva, acción preventiva, mejoras, innovación y reorganización.			

Tabla 22. Capítulo 10. Mejora. (Elaboración propia)

ANEXO C: Instructivo para el levantamiento del Contexto Organizacional y elementos de Gestión del Sistema Integrado

1. OBJETIVO DEL PLAN DE GESTIÓN

En este apartado, la organización debe definir el propósito que contiene la elaboración del documento, orientando su descripción hacia el aporte que brinda la implementación de un plan de gestión sobre la operación de la entidad. Se recomienda la elaboración de un párrafo corto y conciso donde se exprese el objetivo principal del despliegue de un Sistema de Gestión y su impacto en las actividades.

***Ejemplo:** El propósito principal que tiene NOMBRE DE LA EMPRESA al estructurar un Sistema Integrado de Gestión, que contempla las buenas prácticas frente a la seguridad de la información y la calidad en la gestión del servicio, se encuentra enfocado hacia la entrega y prestación de productos/servicios de alta calidad, considerando los requerimiento, recursos y limitaciones necesarias para lograrlo.*

NOMBRE DE LA EMPRESA declara su compromiso frente a la implementación de buenas prácticas en sus procesos al tomar en consideración los requisitos normativos previstos en la norma ISO/IEC 27001 y la norma ISO/IEC 20000-1 y aplicarlos en sus actividades.

2. CONTEXTO DE LA ORGANIZACIÓN

2.1. Introducción

Al momento de estructurar el contexto de la organización, es necesario comenzar con un texto introductorio que describa brevemente a que se dedica la organización,

especificando su actividad y el enfoque que tiene hacia sus clientes a partir de su propuesta de valor. Adicionalmente, se recomienda mencionar aspectos como lo son: su trayectoria, los pilares que impulsan su operación y dan estabilidad en su estructura, así como características que le permitan al lector proyectar una imagen sobre la organización que se le está presentando.

2.2. Misión y Visión

La misión de toda organización debe describir su propósito fundamental, contemplando su razón de ser. Esta declaración debe comunicar lo que hace la organización, hacia quien va dirigida su operación y como logra realizarlo, teniendo en cuenta las acciones concretas que realiza la organización para cumplir con sus objetivos.

Rivera en [68] “Misión organizacional es el propósito por el cual una organización existe. En general, contiene información como, qué tipos de productos o servicios produce la organización, quienes son sus clientes, y qué valores importantes tiene. Es un amplio informe de dirección organizacional. Para un desarrollo apropiado, la dirección debe realizar un análisis completo y debe considerar la información generada durante el proceso de análisis del entorno”

Por otro lado, la visión es una declaración aspiracional dentro de la cual se contempla el estado que se desea a futuro para la organización, junto con el impacto a largo plazo que se quiere alcanzar. Representa un objetivo claro que la dirección estratégica plantea a largo plazo, motivando a los miembros de la organización y orientándolos hacia el logro de objetivos.

2.3. Valores institucionales.

Los valores institucionales son principios rectores que guían el comportamiento de una organización y posibilitan la toma de decisiones por parte de sus miembros; estos conceptos reflejan la cultura organizacional que se vive en toda entidad y son esenciales para la creación de un ambiente laborar coherente, que se encuentre alineado con la misión, la visión y el propósito estratégico de la organización.

2.4. Propósito

El propósito estratégico es un concepto que incluye un estado futuro deseable, una meta definida en términos competitivos y una definición estratégica. Este concepto identifica una posición de liderazgo y establece los criterios que la organización va a utilizar para canalizar su progreso, partiendo de una ambición, la cual incluye un proceso activo de dirección en orientar la atención de la organización sobre los factores clave de éxito, motivar a las personas comunicando el valor de la meta y sostener el entusiasmo a través del suministro de nuevas definiciones operativas cuando las circunstancias cambian.[68]

Algunas organizaciones diferencian su propósito general de actividades específicas, teniendo en cuenta los plazos de consecución y la amplitud de las metas, por lo que objetivos con mayor facilidad de alcance o con una segmentación frente a un área o tema específico son contemplados dentro de propósitos a corto plazo que contribuyen en el cumplimiento del propósito central de la organización.

2.5. Estructura Organizacional

2.5.1. Definición de roles, responsabilidades y autoridades de la organización

La definición clara de los roles, responsabilidades y autoridades dentro de la organización constituye un elemento esencial para garantizar el adecuado funcionamiento del sistema de gestión. La norma establece que la alta dirección debe asegurar que las responsabilidades y autoridades para los roles pertinentes sean debidamente asignadas y comunicadas en todos los niveles, de manera que no existan vacíos ni duplicidades en la gestión. Asimismo, recae en la alta dirección la obligación de designar responsabilidades específicas que permitan, por un lado, asegurar el cumplimiento de los requisitos del sistema de gestión y, por otro, garantizar que se informe periódicamente sobre su desempeño, facilitando la toma de decisiones basada en información confiable. Adicionalmente, la alta dirección puede extender la delegación de estas responsabilidades para que la retroalimentación y el control del desempeño se realicen de forma descentralizada, fortaleciendo así la eficacia y el compromiso en cada área.

En este sentido, la definición de roles y autoridades se convierte en el pilar sobre el cual se estructura la organización, ya que clarifica los niveles de responsabilidad, los flujos de comunicación y las jerarquías de decisión.

Para representar de manera tangible esta distribución de funciones, la estructura organizacional puede verse reflejada a partir de un organigrama el cual es una representación gráfica de la estructura orgánica de una empresa u organización que refleja, en forma esquemática, la posición de las áreas que la integran, sus niveles jerárquicos, líneas de autoridad y de asesoría.[69]

Hay múltiples tipos de organigrama, por lo que es recomendado que cada organización consulte autores y expertos en su formulación, quienes puedan brindarles bases sólidas que contribuyan en su desarrollo, y condensen la totalidad de su estructura en un diagrama sólido, entendible para quien lo lea.

A continuación, en la ilustración No. 9 se presenta un ejemplo de organigrama general expuesto por Franklin en su obra, el cual Contienen información representativa de una organización hasta determinado nivel jerárquico, según su magnitud y características. A su vez se complementa la definición de los roles por medio de una plantilla de manual de función presentado en la tabla No. 23

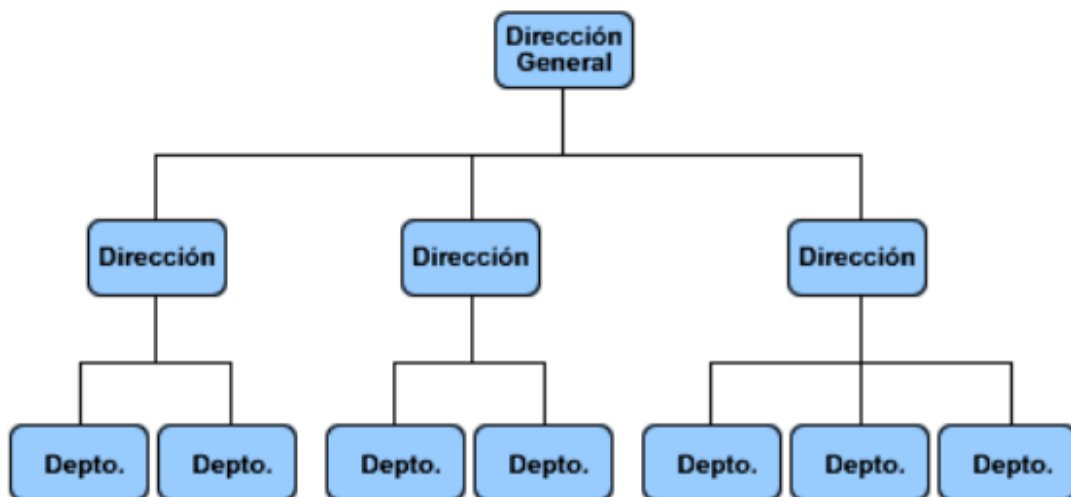


Ilustración 9. Organigrama general. Adaptado de [69]

Código: Versión:	MANUAL DE FUNCIONES			Espacio para el logo
Denominación del Cargo				
Área a la que pertenece				
Cargos a quien reporta				
Cargos bajo su supervisión				
Nivel del Cargo	Estratégico		Táctico	Operativo
OBJETIVO DEL CARGO				
COMPETENCIA DEL CARGO				
NIVEL EDUCATIVO ACTUAL	Educación base			
	Educación complementaria			
	Certificaciones:			
EXPERIENCIA	Tiempo certificable			
EXCEPCIONES				
FUNCIONES Y RESPONSABILIDADES DENTRO DEL SISTEMA INTEGRADO DE GESTIÓN				
1				
2				
3				
4				
RIESGO DEL CARGO		PROBABILIDAD DEL RIESGO		
		ALTA	MEDIA	BAJA
1				
2				
3				
COMPETENCIAS REQUERIDAS				
GENERALES		DEFINICIÓN		NIVEL
1				
2				
3				
4				
ELEMENTOS ASIGNADOS				
HERRAMIENTA		ESPECIFICACIÓN		PROGRAMAS
1				
ENTREGA Y SOCIALIZACIÓN DE FUNCIONES Y RESPONSABILIDADES				
FIRMA		Datos	Funcionario que capacita	Funcionario que recibe capacitación
		Nombre		
		Cargo		

Tabla 23. Formato Manual de funciones. Adaptado de [70]

3. JUSTIFICACIÓN PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN

La organización debe identificar las cuestiones internas y externas relacionadas con su propósito, ya que estas influyen directamente en su capacidad para alcanzar los resultados previstos en el sistema de gestión. En este sentido, se determinan los factores que pueden generar impactos tanto positivos como negativos en el desarrollo de sus actividades, estableciendo así la base para la planificación estratégica y la alineación de la alta dirección con el cumplimiento de los requisitos del sistema integrado.

3.1. Planeación y alineación estratégica

La planeación estratégica nace del ejercicio que realiza la alta dirección, representando el esfuerzo invertido en el proceso de caracterización de los objetivos y la formación de un plan a futuro, donde se establece la estrategia que permitirá materializar los logros esperados por la organización. Este proceso se encarga de determinar el liderazgo, definiendo la plataforma estratégica a partir del análisis de factores internos y externos que determinan el contexto al cual se encuentra sujeto la organización, integrando esfuerzos en la generación de valor agregado para los involucrados en las diferentes etapas de su proceso.

En este marco, la alineación estratégica asegura que los recursos, capacidades, estructuras y acciones se encuentren en consonancia con la estrategia definida, permitiendo que todos los componentes de la organización trabajen de manera coherente y sinérgica hacia los objetivos a largo plazo. De esta forma, se establecen los pasos para el desarrollo, la implementación y la medición de las metas, apoyados en la información y los datos derivados del propio ejercicio de gestión. Así, planeación y alineación no solo constituyen un ejercicio de liderazgo de la alta dirección, sino también una herramienta de integración que garantiza la sostenibilidad del sistema de gestión y su capacidad de respuesta ante los desafíos internos y externos.

Dentro de la alineación estratégica se contemplan las herramientas que exponen la intención de la alta dirección frente al logro de objetivos, las cuales se enlistan a continuación:

3.1.1. Gestión por procesos

La gestión por procesos se centra en la descripción y orientación de los propósitos que tiene cada proceso hacia los objetivos generales de la organización, logrando mejorar el rendimiento y eficiencia de las actividades que se realizan, alcanzando una mayor fluidez en el desarrollo de las tareas.

Dentro de este ítem, la norma exige que se definan **la gestión del proceso de Seguridad de la información y de Gestión del servicio como parte de la estrategia**, considerando sus aportes en el cumplimiento de objetivos, teniendo en cuenta la influencia de sus actividades sobre los resultados alcanzados en el escenario del Sistema de Gestión Integrado.

Gestión de la Seguridad de la Información	Gestión del servicio
<p>Ejemplo. “Como parte de la planeación estratégica de NOMBRE DE LA EMPRESA, que la alta dirección dispuso para el año XXXX, se establece para los procesos de seguridad de la información y de gestión del servicio los siguientes objetivos:”</p>	
<p>Objetivo general: Aumentar la satisfacción del cliente a partir de una potenciación de la propuesta de valor, implementando mejoras frente a la disponibilidad, confidencialidad e integridad en el manejo de su información y a su vez, sobre la disponibilidad y confiabilidad de los servicios ofrecidos por la empresa.</p>	
<p>Actividades específicas:</p> <ul style="list-style-type: none"> • Identificar y evaluar riesgos derivados de las nuevas tendencias tecnológicas • Establecer directrices claras frente a la custodia y protección de la información • Aumentar los índices de capacitaciones, generando mayor conciencia frente al acceso y uso de la información • Asegurar una operación ininterrumpida 	<p>Actividades específicas:</p> <ul style="list-style-type: none"> • Mejorar el tiempo de respuesta frente al soporte brindado en el servicio • Reducir el número de incidentes • Aumentar la tasa de resolución en el primer contacto • Incrementar la satisfacción del cliente • Garantizar una continua disponibilidad del servicio

Tabla 24. Ejemplo gestión por procesos. Fuente: Elaboración propia

3.1.2. Red de Valor

La Red de valor es una herramienta analítica que permite descifrar la capacidad de cooperación entre los actores que la integran, con el objetivo de generar riqueza. La articulación eficiente de la red es un elemento clave para impulsar la competitividad de la misma en el ámbito nacional e internacional, a partir de su conocimiento sobre el

mercado y demanda específica del consumidor; sus proveedores (internos y externos) y los servicios con enfoque hacia una oferta diversificada y calificada. [71]

Los atributos que componen la red de valor son características fundamentales en la entrega de una propuesta de valor a las partes interesadas de una organización, brindando la diferenciación y satisfacción de necesidades y expectativas que estas tiene sobre el producto o servicio.

En la ilustración No. 10 se presenta un ejemplo grafico de red de valor aplicable en la definición del contexto organizacional de cualquier empresa

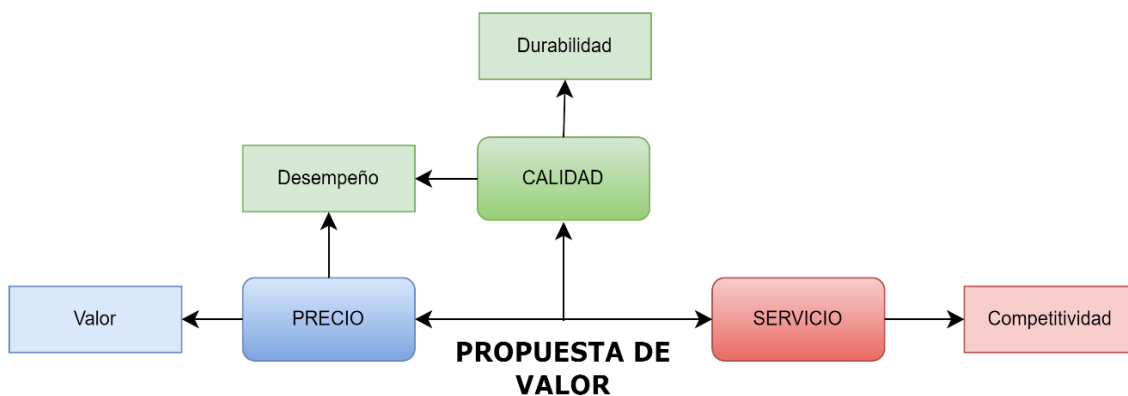


Ilustración 10. Ejemplo grafico – red de valor (Elaboración propia)

3.1.3. Balanced Scorecard para sistemas de Información

El Balanced Scorecard (BSC) o Cuadro de Mando Integral es una herramienta de gestión estratégica que permite medir y mejorar el rendimiento en las organizaciones; este modelo de gestión que traduce la estrategia en objetivos relacionados, medidos a través de indicadores y ligados a unos planes de acción, permiten alinear el comportamiento de los miembros de la organización y materializar el logro de objetivos a partir de actividades coordinadas.[72]

En el contexto de la seguridad de la información, el BSC se adapta para evaluar y mejorar el desempeño en áreas críticas relacionadas con la protección de datos y activos informáticos. Este enfoque integra marcos de gobernanza y control como COBIT,

SABSA, ISG, ITIL y ISO 27000, proporcionando una visión integral de la gestión de la seguridad de la información, tal como se muestra en la ilustración No. 11. [73]



Ilustración 11. Perspectiva del Balanced Scorecard para sistemas de información,

Adaptado de [73]

3.1.4. Matriz DOFA

La matriz DOFA es una herramienta estratégica utilizada para identificar y analizar las Fortalezas, Oportunidades, Debilidades y Amenazas de una organización. Esta matriz ayuda a las organizaciones a comprender sus capacidades internas y su entorno externo, desarrollando estrategias efectivas basadas en este análisis, dado que permite ubicar la información en un orden lógico que ayuda a comprender, presentar, discutir y tomar decisiones. Puede ser utilizado en cualquier tipo de toma de decisiones, ya que la plantilla estimula a pensar proactivamente, en lugar de las comunes reacciones instintivas.[74]

A continuación, la ilustración No. 12 se presenta un ejemplo grafico de los conceptos planteados por López para la definición de la matriz DOFA.

<p>fortalezas</p> <ul style="list-style-type: none"> • ¿Ventajas de la sistema? • ¿Capacidades? • ¿Ventajas competitivas? • ¿PUV's (propuesta única de vetas)? • ¿Recursos, activos, gente? • ¿Experiencia, conocimiento, datos? • ¿Reservas financieras, retorno probable? • ¿Marketing – alcance, distribución, awareness? • ¿Aspectos innovadores? • ¿Ubicación geográfica? • ¿Precio, valor, calidad? • ¿Acreditaciones, calificaciones, certificaciones? • ¿Procesos, sistemas, TI, comunicaciones? • ¿Cultural, actitudinal, de comportamiento? • ¿Cobertura gerencial, sucesión? 	<p>debilidades</p> <ul style="list-style-type: none"> • ¿Desventajas de sistema? • ¿Brechas en la capacidad? • ¿Falta de fuerza competitiva? • ¿Reputación, presencia y alcance? • ¿Aspectos Financieros? • ¿Vulnerabilidades propias conocidas? • ¿Escala de tiempo, fechas tope y presiones? • ¿Flujo de caja, drenaje de efectivo? • ¿Continuidad, robustez de la cadena de suministros? • ¿Efectos sobre las actividades principales, distracción? • ¿Confiabilidad de los datos, predictibilidad del plan? • ¿Motivación, compromiso, liderazgo? • ¿Acreditación, etc? • ¿Procesos y sistemas, etc? • ¿Cobertura gerencial, sucesión?
<p>oportunidades</p> <ul style="list-style-type: none"> • ¿Desarrollo de nuevos sistemas? • ¿Desarrollos del mercado? • ¿Vulnerabilidades de los competidores? • ¿Tendencias de la industria o de estilo de vida? • ¿Desarrollos tecnológicos e innovaciones? • ¿Influencias globales? • ¿Nuevos mercados, verticales, horizontales? • ¿Mercados objetivo nicho? • ¿Geografía, exportación, importación? • ¿Nuevas propuestas únicas de venta? • ¿Tácticas - sorpresa, grandes contratos, etc? • ¿Desarrollo de negocios o de productos? 	<p>amenazas</p> <ul style="list-style-type: none"> • ¿Efectos políticos? • ¿Efectos legislativos? • ¿Efectos ambientales? • ¿Desarrollos de TI? • ¿Intenciones de los competidores? • ¿Demanda del mercado? • ¿Nuevas tecnologías, servicios, ideas? • ¿Contratos y alianzas vitales? • ¿Mantener las capacidades internas? • ¿Obstáculos enfrentados? • ¿Debilidades no superables? • ¿Pérdida de personal clave? • ¿Respaldo financiero sostenible? • ¿Economía – local o extranjera?

Ilustración 12. Guía matriz DOFA, Adaptado de [74]

4. PARTES INTERESADAS

Las partes interesadas que son pertinentes para el sistema de gestión deben ser identificadas y descritas a partir del contexto en el que interactúan con la organización, teniendo en cuenta los requisitos que abordan a partir del Sistema Integrado de Gestión, donde se consideran las necesidades y expectativas frente a: el servicio, el resguardo y el uso correcto de la información, el desempeño del sistema, los requisitos legales y las obligaciones contractuales que tiene la organización con estas, o viceversa.

Las partes interesadas son todos aquellos actores que se ven afectados de manera positiva o negativa a partir de la implementación de decisiones que se encuentren relacionadas con las actividades empleadas en el SGSI y en el SGS. Dependiendo del direccionamiento que tengan las actividades comerciales de la organización, se hace indispensable su comprensión dada la influencia que poseen sobre el cumplimiento de los objetivos, teniendo en cuenta su interacción y como podrían ejercer un fuerte dominio en el correcto desarrollo del plan de funcionamiento de la empresa.

A continuación, se presenta un ejemplo de grupos de interés que podrían ser identificados por las organizaciones, clasificándolos según el entorno en el que interactúan con su actividad, especificando algunas de las necesidades y expectativas que deben ser cubiertas por la organización.

4.1. Contexto Externo

Grupo de interés	Necesidad	Expectativa
Gobierno	Ejemplo: Cumplimiento de la normativa legal vigente para el sector tecnológico, teniendo en cuenta los requerimientos comerciales y laborales en la operación de la organización y despliegue de actividades.	Ejemplo: Crecimiento de la industria tecnológica en mercados nacionales e internacionales, mejorando la gestión de servicios prestados a la comunidad y potenciando las actividades que se encuentran enfocadas al desarrollo social.
Cliente	Pudiendo segmentarse en clientes nacionales e internacionales:	
	Ejemplo: Cumplimiento de los acuerdos contractuales y de las garantías del servicio prestado, garantizando el correcto uso y resguardo de su información, mejorando la entrega de la propuesta de valor.	Ejemplo: Prestación de un servicio continuo que dé solución a las problemáticas de su negocio, con una amplia confianza en los datos que posibilitan la toma de decisiones, aumentando la percepción de valor a partir de mejoras en el servicio.
Proveedor	Ejemplo: cumplimiento de acuerdos y requisitos establecidos entre las partes	Ejemplo: Mejorar relación costo beneficio donde ambas partes obtengan los resultados esperados
Competencia	Ejemplo: Evaluación de impacto de los competidores sobre la estrategia actual de la organización	Ejemplo: Identificación oportuna de competidores y toma de decisiones frente a la gestión de relaciones.

Tabla 25. Contexto externo, partes interesadas. Fuente: Elaboración propia

4.2. Contexto Interno

Grupo de interés	Necesidad	Expectativa
Accionistas	Ejemplo: cumplimiento de las metas empresariales; atracción de nuevos clientes, incremento de los beneficios generales para todas las partes interesadas, implementación de un sistema que mejore los procesos de la organización	Ejemplo: Expansión del mercado, consolidación de relaciones a largo plazo con las partes interesadas, aumento de la percepción de satisfacción de sus clientes, potenciación en el valor ofrecido
Colaboradores	Ejemplo: Crecimiento en la percepción de bienestar, garantías frente al desarrollo de sus actividades y la estabilidad laboral	Ejemplo: Crecimiento profesional dentro de la organización, aumento en los beneficios percibidos por cada colaborador.

Tabla 26. Contexto interno, partes interesadas. Fuente: Elaboración propia

5. ALCANCE DEL SISTEMA INTEGRADO DE GESTIÓN

Uno de los requerimientos normativos que mayor influencia posee sobre el correcto despliegue del sistema de gestión, es la determinación del alcance del sistema, donde la organización define los límites y la aplicabilidad de las actividades de cada modelo en su organización; las cuestiones que abordan su desarrollo pueden visualizarse en la tabla No. 27:

Cuestiones que deben ser consideradas	Validación	
	SI	NO
Análisis de contexto y requisitos		
¿Se ha revisado el análisis de contexto interno y externo de la organización?		
¿Se han identificado las necesidades y expectativas de las partes interesadas?		
¿Se han incorporado los requisitos legales, regulatorios y contractuales que afectan los procesos, servicios o activos?		
Cobertura Organizacional		
¿El alcance aplica a toda la organización o solo a determinadas unidades?		
¿Se han identificado los procesos incluidos en el alcance?		
¿Las funciones o procesos excluidos cuentan con justificación verificable?		
Cobertura de activos de información		
¿Se han identificado los sistemas, aplicaciones, plataformas e infraestructuras críticas que soportan los procesos y servicios?		
¿Los activos excluidos cuentan con justificación y su exclusión no compromete la seguridad ni la gestión de servicios?		
Cobertura de servicios		
¿Se han identificado todos los servicios prestados por la organización?		

Cuestiones que deben ser consideradas	Validación	
	SI	NO
Relación con proveedores y terceros		
¿Se han identificado los servicios/procesos subcontratados que impactan la operación?		
¿Los servicios de terceros se encuentran incluidos en el alcance o gestionados bajo condiciones específicas?		
Cobertura temporal		
¿El alcance incluye únicamente servicios estables en operación o también proyectos transitorios?		
Evidencia documental		
¿Existe una declaración formal del alcance aprobada por la alta dirección?		
¿El documento describe procesos, servicios, activos, ubicaciones y funciones incluidas?		
¿Se documentan exclusiones y sus justificaciones?		
Validación y aprobación		
¿La definición del alcance ha sido revisada y aprobada por la alta dirección?		
¿El alcance definido refleja coherencia con la estrategia institucional y la operación real?		
Actualización y mejora continua		
¿Existe un procedimiento para revisar y actualizar periódicamente el alcance?		
¿Se conservan evidencias de revisiones, auditorías o cambios aplicados al alcance?		

Tabla 27. Checklist de aspectos claves para la formulación del alcance del SIG. Fuente: Elaboración propia

Nota: Para el adecuado entendimiento del alcance se recomienda anexar la definición de los productos o servicios que son ofrecidos en términos comerciales por la organización.

6. ESTRUCTURA SISTEMA INTEGRADO DE GESTIÓN

La estructura del Sistema Integrado de Gestión se configura como el marco que organiza y articula los procesos de la organización, permitiendo su desarrollo ordenado y alineado con los objetivos estratégicos. Este sistema responde a la necesidad de contar con un modelo que asegure la implementación, mantenimiento y mejora continua de las actividades clave, integrando la gestión de la seguridad de la información y la gestión del servicio de TI en un conjunto de procesos interrelacionados. De esta manera, se garantiza que cada área conozca su rol, se promueva la eficiencia en la operación, y se establezcan mecanismos de control y seguimiento que faciliten la toma de decisiones y el cumplimiento de los requisitos normativos aplicables.

En este sentido, es necesario que las organizaciones definan con precisión los aspectos clave de su sistema de gestión, lo que implica identificar los procesos relevantes, establecer sus interacciones y designar los responsables de su ejecución y seguimiento. Dicho ejercicio debe reflejar cómo los procesos aportan al cumplimiento de los objetivos, así como a la aplicación de los requisitos normativos y contractuales. Para facilitar su comunicación y comprensión en todos los niveles de la organización, se recomienda complementar esta definición con desarrollos gráficos (tales como mapas de procesos, diagramas de interacción o esquemas de flujo) que permitan visualizar de forma clara la dinámica del sistema. De esta manera, al describir su sistema de gestión, las organizaciones no solo delimitan su alcance, sino que también establecen los criterios de control y los mecanismos de seguimiento necesarios para garantizar su efectividad y mejora continua.

7. POLÍTICA INTEGRADA DE GESTIÓN

Con el fin de dar cumplimiento a los lineamientos establecidos en las normas internacionales de gestión y a lo dispuesto por la alta dirección, se presenta a continuación un ejemplo de Política Integrada de Gestión. Este modelo refleja cómo una organización puede consolidar en un solo documento sus compromisos estratégicos, garantizando la alineación con su propósito, la satisfacción de los requisitos aplicables, el fortalecimiento de la gestión del servicio y la protección de la información. Además, la política establece el marco necesario para orientar los objetivos institucionales y comunicar de manera clara el compromiso hacia la mejora continua, asegurando su difusión tanto al interior de la organización como entre las partes interesadas pertinentes.

Ejemplo: *[Nombre de la organización] se compromete a gestionar de manera integrada la calidad de sus procesos, la seguridad de la información, la continuidad de las operaciones y la gestión eficiente de los servicios se articulen como un solo marco de trabajo, siendo parte fundamental de su responsabilidad con clientes, colaboradores, socios estratégicos y demás partes interesadas.*

Esta política es coherente con el propósito institucional y constituye el marco de referencia para la definición de los objetivos de gestión, orientando la toma de decisiones hacia la creación de valor sostenible y el logro de resultados medibles.

Para ello, la organización asegura el cumplimiento de los requisitos legales, contractuales, regulatorios y normativos aplicables, garantizando prácticas responsables y transparentes en cada una de sus operaciones.

La alta dirección y todos los colaboradores asumen el compromiso de fomentar una cultura de mejora continua, que permita optimizar procesos, adaptándose a las dinámicas del entorno y respondiendo con oportunidad y eficacia a las necesidades y expectativas de las partes interesadas. Asimismo, consolidar el deber de garantizar la seguridad de la información, preservando su confidencialidad, integridad y disponibilidad, y gestionando los riesgos asociados a su tratamiento.

Esta política se encuentra disponible como información documentada, es comunicada en todos los niveles de la organización para asegurar su comprensión y aplicación, y se mantiene accesible a las partes interesadas externas que así lo requieran, contribuyendo al fortalecimiento de la confianza y a la sostenibilidad de la organización.

8. OBJETIVOS DEL SISTEMA INTEGRADO DE GESTIÓN

La definición de objetivos dentro del Sistema Integrado de Gestión constituye un paso fundamental para garantizar la alineación entre la estrategia organizacional, los requisitos normativos y las expectativas de las partes interesadas. Estos objetivos no solo orientan la acción de la organización hacia el cumplimiento de su política y de los compromisos adquiridos, sino que también sirven como instrumento de medición del desempeño, de priorización de recursos y de fortalecimiento de la mejora continua.

Para asegurar su eficacia, es indispensable que la alta dirección asigne y comunique claramente las responsabilidades y autoridades, asegurándose de que los objetivos definidos respondan a los requisitos normativos, sean coherentes con la política, se encuentren documentados y dispongan de mecanismos claros para su seguimiento.

A continuación, en la tabla No. 28 se presentan una guía metodológica para la definición de objetivos:

Ejemplo *“Optimizar la gestión de los servicios tecnológicos y reforzar la seguridad de la información mediante la implementación de procesos estandarizados y*

controles efectivos, logrando una reducción del 25% en incidentes de servicio y de seguridad reportados en el periodo anual”

Preguntas claves		Análisis ejemplo practico
1	¿Está alineado con la política organizacional y con los compromisos asumidos con clientes?	Este objetivo responde de manera directa a la política del Sistema Integrado de Gestión, que establece el compromiso de garantizar la continuidad, disponibilidad y seguridad de los servicios TI.
2	¿Qué requisitos normativos o contractuales soportan la necesidad de este objetivo?	* ISO/IEC 27001: requisitos sobre evaluación y tratamiento de riesgos de seguridad de la información. * ISO/IEC 20000-1: requisitos sobre gestión de incidentes, cumplimiento de niveles de servicio y mejora continua.
3	¿Qué recursos se requieren para su cumplimiento?	* Herramientas de monitoreo y gestión de incidentes * Personal capacitado en gestión de riesgos, continuidad y atención de incidentes. * Campañas de concienciación para usuarios finales en buenas prácticas de seguridad y uso de servicios
4	¿Qué área o rol dentro de la organización será responsable de su ejecución y seguimiento?	Áreas de Seguridad de la Información, Gestión de servicios y el comité de dirección del Sistema Integrado de Gestión
5	¿Qué indicadores o métricas se establecerán para medir su cumplimiento?	* Número de incidentes de seguridad y servicio registrados mensualmente. * Porcentaje de reducción frente al periodo anterior. * Nivel de cumplimiento de los acuerdos de servicio
6	¿Cuál es el plazo establecido para alcanzarlo?	12 meses
7	¿Qué riesgos pueden afectar el logro del objetivo y cómo serán gestionados?	En caso de presentarse fallas graves en la continuidad del servicio o incidentes críticos de seguridad, se activarán los planes de continuidad y contingencia definidos en el Sistema Integrado de Gestión.
8	¿Cómo se informará a la alta dirección y a las partes interesadas sobre el desempeño asociado a este objetivo?	Reportes trimestrales al Comité de Dirección Sistema Integrado de Gestión y presentaciones ejecutivas a la Alta Dirección, con propuestas de mejora y acciones correctivas en caso de incumplimiento.

Tabla 28. Guía metodológica para la definición de objetivos (Elaboración propia)

ANEXO D: Plantilla. Declaración de aplicabilidad

Declaración de aplicabilidad				
No.	Control (2022)	Tipo	Exclusión (SI / NO)	Justificación
5.1	Políticas de seguridad de la información	Organización		
5.2	Roles y responsabilidad en la seguridad de la información	Organización		
5.3	Separación de deberes	Organización		
5.4	Responsabilidades de la dirección	Organización		
5.5	Contacto con las autoridades	Organización		
5.6	Contacto con grupos de interés especial	Organización		
5.7	Inteligencia de amenazas	Organización		
5.8	Seguridad de la Información en la gestión de proyectos	Organización		
5.9	Inventario de información y otros activos asociados	Organización		
5.10	Uso aceptable de la información y otros activos asociados	Organización		
5.11	Devolución de activos	Organización		
5.12	Clasificación de la información	Organización		
5.13	Etiquetado de la información	Organización		
5.14	Transferencia de información	Organización		
5.15	Control de acceso	Organización		
5.16	Gestión de identidades	Organización		
5.17	Información de autenticación	Organización		
5.18	Derechos de acceso	Organización		
5.19	Seguridad de la información en las relaciones con proveedores	Organización		
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	Organización		
5.21	Gestión de seguridad de la información en la cadena de suministro de la TI y las telecomunicaciones (TIC)	Organización		
5.22	Seguimiento, revisión y gestión de cambio servicios de proveedores	Organización		
5.23	Seguridad de la información para el	Organización		

Declaración de aplicabilidad				
No.	Control (2022)	Tipo	Exclusión (SI / NO)	Justificación
	uso de servicios en la nube			
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Organización		
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Organización		
5.26	Respuesta a incidentes de seguridad de la información	Organización		
5.27	Aprender de los incidentes de seguridad de la información	Organización		
5.28	Recopilación de evidencias	Organización		
5.29	Seguridad de la información durante una interrupción	Organización		
5.30	Preparación de las TIC para la continuidad de negocio	Organización		
5.31	Requisitos legales, legales, reglamentarios y contractuales	Organización		
5.32	Derechos de propiedad intelectual	Organización		
5.33	Protección de registros	Organización		
5.34	Privacidad y protección de la información de identificación personal (PII, por sus siglas en ingles)	Organización		
5.35	Revisión independiente de la seguridad de la información	Organización		
5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	Organización		
5.37	Procedimientos operativos documentados	Organización		
6.1	Selección	Personas		
6.2	Términos y condiciones de empleo	Personas		
6.3	Conciencia de seguridad de la información, educación y formación	Personas		
6.4	Proceso disciplinario	Personas		
6.5	Responsabilidades después de la terminación o cambio de empleo	Personas		
6.6	Acuerdos de confidencialidad o no divulgación	Personas		
6.7	Trabajo remoto	Personas		
6.8	Informes de eventos de seguridad de la información	Personas		
7.1	Perímetros de seguridad física	Físicos		
7.2	Entrada física	Físicos		
7.3	Asegurar oficinas, habitaciones e instalaciones	Físicos		
7.4	Monitoreo de la seguridad física	Físicos		
7.5	Protección contra amenazas físicas y ambientales	Físicos		
7.6	Trabajar en áreas seguras	Físicos		

Declaración de aplicabilidad				
No.	Control (2022)	Tipo	Exclusión (SI / NO)	Justificación
7.7	Escritorio y pantalla limpios	Físicos		
7.8	Emplazamiento y protección de equipos	Físicos		
7.9	Seguridad de los activos fuera de las instalaciones	Físicos		
7.10	Medios de almacenamiento	Físicos		
7.11	Servicios públicos de apoyo	Físicos		
7.12	Seguridad del cableado	Físicos		
7.13	Mantenimiento de equipos	Físicos		
7.14	Disposición o reutilización segura de los equipos	Físicos		
8.1	Dispositivos de punto final de usuario	Tecnología		
8.2	Derechos de acceso privilegiado	Tecnología		
8.3	Restricción de acceso a la información	Tecnología		
8.4	Acceso al código fuente	Tecnología		
8.5	Autenticación segura	Tecnología		
8.6	Gestión de la capacidad	Tecnología		
8.7	Protección contra malware	Tecnología		
8.8	Gestión de vulnerabilidades técnicas	Tecnología		
8.9	Gestión de la configuración	Tecnología		
8.10	Eliminación de información	Tecnología		
8.11	Enmascaramiento de datos	Tecnología		
8.12	Prevención de fugas de datos	Tecnología		
8.13	Copia de seguridad de la información	Tecnología		
8.14	Redundancia de las instalaciones de procesamiento de información	Tecnología		
8.15	Registro	Tecnología		
8.16	Actividades de seguimiento	Tecnología		
8.17	Sincronización de reloj	Tecnología		
8.18	Uso de programas de utilidad privilegiados	Tecnología		
8.19	Instalación de software en sistemas operativos	Tecnología		
8.20	Seguridad de redes	Tecnología		
8.21	Seguridad de los servicios de red	Tecnología		
8.22	Segregación de redes	Tecnología		
8.23	Filtrado web	Tecnología		
8.24	Uso de la criptografía	Tecnología		
8.25	Ciclo de vida de desarrollo seguro	Tecnología		
8.26	Requisitos de seguridad de las aplicaciones	Tecnología		
8.27	Arquitectura de sistemas seguros y principios de ingeniería	Tecnología		
8.28	Codificación segura	Tecnología		
8.29	Pruebas de seguridad en el desarrollo y aceptación	Tecnología		

Declaración de aplicabilidad				
No.	Control (2022)	Tipo	Exclusión (SI / NO)	Justificación
8.30	Desarrollo externalizado	Tecnología		
8.31	Separación de entornos de desarrollo, evidencia y producción	Tecnología		
8.32	Gestión del cambio	Tecnología		
8.33	Información de las pruebas	Tecnología		
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Tecnología		

Tabla 29. Plantilla Declaración de aplicabilidad

La Declaración de Aplicabilidad (SoA) permite establecer qué controles de la norma ISO/IEC 27001:2022 son aplicables a la organización, cuáles pueden excluirse y cómo se justifican estas decisiones. A continuación, se presentan algunos ejemplos prácticos para ilustrar su uso:

En organizaciones que operan de forma 100% remota y en la nube, ciertos controles pueden ser excluidos. Por ejemplo, los relacionados con la seguridad física y ambiental no son pertinentes si no se administran centros de datos propios, siempre que el proveedor Cloud demuestre cumplimiento mediante certificaciones como ISO/IEC 27001 o SOC 2. De forma similar, los controles de medios removibles (USB, discos externos) pueden excluirse cuando la política interna prohíbe su uso, acompañando la exclusión con medidas como bloqueo técnico de puertos y cifrado obligatorio en la nube.

Por el contrario, algunos controles deben fortalecerse en este tipo de entornos. Entre ellos destacan: la gestión de accesos, que requiere autenticación multifactor y revisiones periódicas de privilegios; la gestión de incidentes, que debe apoyarse en un Playbook con roles y tiempos de respuesta claros; la formación en seguridad, orientada a mitigar riesgos humanos como phishing o el mal uso de dispositivos personales.

En conclusión, la SoA no debe asumirse como una lista estática, sino como una herramienta que permite adaptar la norma a la realidad operativa de la organización, justificando exclusiones y fortaleciendo controles clave para garantizar seguridad y confianza en los servicios de TI.

ANEXO E: Formulario utilizado en la validación por expertos

El presente anexo contiene el instrumento de evaluación utilizado para la validación de los requisitos normativos y las correspondientes respuestas proporcionadas por los expertos. Este formulario fue diseñado con el objetivo de recolectar información precisa y objetiva sobre la aplicabilidad y cumplimiento de los criterios establecidos en las normas bajo estudio.

A continuación, se presentan las ilustraciones del formulario completo, así como los registros de las respuestas diligenciadas por cada experto, lo que permite evidenciar de manera clara y detallada el proceso de validación y análisis realizado.

Validación de expertos: Estructuración de un sistema integrado de gestión de tecnologías de la información basado en la familia de normas ISO/IEC 27000 e ISO/IEC 20000

La presente validación hace parte del trabajo de investigación titulado "**Estructuración de un Sistema Integrado de Gestión de Tecnologías de la Información basado en la familia de normas ISO/IEC 27000 e ISO/IEC 20000**", desarrollado en el marco de la Maestría en Administración.

El propósito de este formulario es recopilar la opinión y las recomendaciones de expertos en gestión tecnológica y en la implementación de sistemas de gestión bajo estándares internacionales, con el fin de evaluar la pertinencia, coherencia y aplicabilidad del modelo propuesto.

Sus aportes resultan fundamentales para enriquecer el estudio, fortalecer el diseño metodológico y garantizar que la propuesta responda a las necesidades reales de las organizaciones en materia de seguridad de la información y calidad en los servicios de TI.

Le agradecemos el tiempo dedicado y el valor de sus comentarios, los cuales serán incorporados en el proceso de ajuste y consolidación final de la investigación.

Ilustración 13. Presentación del formulario

1. ¿Considera que el sistema propuesto integra de manera adecuada los requisitos de las normas ISO/IEC 27001 e ISO/IEC 20000?



Ilustración 14. Ponderada pregunta (1) Formulario de evaluación

¿Qué requisitos de las normas considera que no han sido cubiertos de forma suficiente?

3 respuestas

Todos se consideran
Ninguno
NA

Ilustración 15. Respuestas pregunta (1.1) Formulario de evaluación

¿Qué acciones propondría para fortalecer esta integración?

3 respuestas

Ver sobre el mapa de procesos organizacional o sobre la estructura organizacional (organigrama) la aplicación del sistema integrado y participación de los diferentes roles correspondientes, demostrando su fácil integración con la operación organizacional y transversalidad de los requisitos integrables

Definir un grupo de participantes modelo, que serían los involucrados desde el inicio de la implementación de los sistemas de gestión integrados. Considerando que la organización donde se aplique tendrá actores comunes como un responsable de TI y un responsable de seguridad que tendrán roles y responsabilidades predefinidos para la implementación.

unificar procesos y documentación, definir indicadores comunes, e impulsar la capacitación y comunicación interna

Ilustración 16. Respuestas pregunta (1.2) Formulario de evaluación

2. ¿Qué aspectos prácticos deberían fortalecerse en el diseño de la propuesta metodológica para la implementación de un sistema integrado de gestión?

¿Qué aspectos prácticos deberían fortalecerse en el diseño de la propuesta metodológica para la implementación de un sistema integrado de gestión?

3 respuestas

Mayor énfasis en la estructura de alto nivel, consideración de otros aspectos de implementación de las normas tales como contratación del servicio con el organismo certificador

Fortalecer la implementación de los controles de seguridad establecidos en el Anexo de la norma ISO 27001 y los procesos de gestión de servicios de TI que se detallan en la norma ISO 20000

En la propuesta metodológica se deben fortalecer la integración de procesos, la definición clara de roles y recursos, así como mecanismos de seguimiento con indicadores y auditorías que aseguren mejora continua.

Ilustración 17. Respuestas pregunta (2) Formulario de evaluación

3. ¿Qué limitaciones identifica en la propuesta al aplicarse en una organización real?

¿Qué limitaciones identifica en la propuesta al aplicarse en una organización real?

3 respuestas

La organización debe tener muy clara su estrategia enfocada en áreas de TI como generadoras de valor para sus objetivos

Ausencia de un plan de implementación de ambos sistemas de gestión integrados

la complejidad en integrar procesos diversos y la dificultad para mantener la disciplina en el seguimiento y mejora continua.

Ilustración 18. Respuestas pregunta (3) Formulario de evaluación

4. ¿Qué acciones o prácticas recomendaría añadir para optimizar la integración y mejora continua del sistema propuesto?

¿Qué acciones o prácticas recomendaría añadir para optimizar la integración y mejora continua del sistema propuesto?

3 respuestas

Diagnóstico previo a la implementación de la metodología que permita identificar la brecha con respecto al sistema integrado

Definir un plan de implementación global de los sistemas de gestión integrados, por ejemplo seccionar las fases de implementación en aquello que forma parte central de la norma como el contexto de la organización, políticas, gestión de riesgos y oportunidades, liderazgo y luego abordar la fase de implementación de controles de forma detallada.

Recomiendo incorporar mecanismos de medición del impacto del marco en los procesos, junto con espacios de retroalimentación periódica y ajustes ágiles que aseguren una integración real y sostenida en el tiempo.

Ilustración 19. Respuestas pregunta (4) Formulario de evaluación

5. ¿Cómo podría mejorarse la aplicabilidad y replicabilidad del modelo en diferentes sectores?

¿Cómo podría mejorarse la aplicabilidad y replicabilidad del modelo en diferentes sectores?

3 respuestas

Mediante procesos de socialización en competitividad para las organizaciones generada a partir de Marcos de gestión como los presentados en la propuesta; adicionalmente, mediante implementación de pilotos iniciando con alcances realistas para las organizaciones que les permita una implementación escalonada

Contar con herramientas diagnósticas del estado actual en el que se encuentra la organización, como punto de partida real sin perder de vista una línea base ya establecida en la entidad.

Podría mejorarse mediante la flexibilización del modelo, incorporando lineamientos generales adaptables a cada sector y buenas prácticas transversales, junto con guías prácticas y casos de referencia que faciliten su replicabilidad.

Ilustración 20. Respuestas pregunta (5) Formulario de evaluación

6. ¿El enfoque metodológico facilita la validación de los resultados en escenarios organizacionales?



Ilustración 21. Ponderada pregunta (6) Formulario de evaluación

¿Qué limitaciones observa en la metodología?

3 respuestas

Para su implementación será requerido involucrar personas conocedoras de procesos de TI, dado su enfoque a la mejora de prácticas en esta área de conocimiento, o perfiles con la capacidad de reconocer valor en procesos soportados en herramientas tecnológicas

Observo como limitación la falta de un plan para la implementación de la propuesta.

NA

Ilustración 22. Respuestas pregunta (6.1) Formulario de evaluación

¿Qué alternativas recomendaría para facilitar la validación?

3 respuestas

Definir objetivos estratégicos claros y factores de éxito de acuerdo a las necesidades propias organizacionales dentro de un alcance determinado para la implementación de la metodología que permitan evaluar la implementación de los mismos.

Considerar casos de estudio reales de organizaciones donde se hayan aplicado ambos modelos.

indicadores de desempeño claros

Ilustración 23. Respuestas pregunta (6.2) Formulario de evaluación

ANEXO F: Plantilla Diagnóstico Inicial

La integración de las normas ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018 en un Sistema Integrado de Gestión exige que las organizaciones cuenten con herramientas que les permitan identificar su nivel actual de madurez y las brechas frente a los requisitos normativos. Con este propósito se presenta una matriz de diagnóstico en formato de plantilla básica, concebida como un instrumento inicial que toma como referencia requisitos de ambas normas.

La matriz está construida sobre una escala de madurez de 0 a 1 en intervalos de 0,25, que permite evaluar de manera gradual el cumplimiento alcanzado:

- * **0**: No documentado/no existente.
- * **0.25**: Se aplica, pero no está documentado.
- * **0.5**: Está documentado, pero no se aplica.
- * **0.75**: Documentado y aplicado de manera consistente.
- * **1**: Documentado, aplicado y con mecanismos de medición y mejora continua.

$$Madurez\ Global = \frac{\sum Puntajes}{N^{\circ}\ de\ requisitos}$$

Aunque se trata de una herramienta de carácter introductorio y no exhaustivo, su valor radica en que constituye una base metodológica sobre la cual la organización puede construir una matriz más elaborada y personalizada, ajustada a sus procesos, riesgos y objetivos estratégicos.

De esta forma, la matriz presentada se posiciona como un punto de partida profesional y estructurado que facilita a las organizaciones proyectar un plan de integración progresivo, evolucionando hacia un diagnóstico más detallado y adaptado a su realidad empresarial.

Capítulo	Requisito clave	27001	20000-1	Nivel 1 Inicial	Nivel 2 Parcial	Nivel 3 Definido	Nivel 4 Gestionado	Nivel 5 Optimizado
Contexto de la organización	Identificación de partes interesadas y alcance	Identificación de riesgos información	Identificación de clientes y servicios	No se identifican	Identificación básica sin análisis	Identificación y análisis documentado	Revisiones periódicas con responsables	Integrado a la estrategia corporativa
Liderazgo	Política y roles	Política de SGSI aprobada	Política de gestión de servicios	No existe liderazgo	Liderazgo informal	Políticas y roles documentados	Comité de dirección con seguimiento	Liderazgo visible y proactivo en estrategia
Planificación	Riesgos y objetivos	Análisis de riesgos de seguridad	Planificación de servicios y continuidad	Sin metodología	Riesgos analizados	Matriz de riesgos documentada	Planes de tratamiento actualizados	Modelo predictivo con indicadores
Soporte	Competencias y recursos	Competencia ciberseguridad	Capacitación y procesos	No se gestionan	Capacitación aislada	Plan de formación definido	Evaluación periódica de competencias	Mejora continua de competencias
Operación	Procesos operativos	Controles de seguridad	Gestión del ciclo de vida del servicio	No hay procesos	Procesos básicos no controlados	Procedimientos documentados	Procesos medidos y monitoreados	Procesos automatizados y mejorados
Evaluación de desempeño	Auditorías internas y métricas	Auditorías SGSI	Auditorías y KPIs	No se realizan	Auditorías ocasionales	Programa anual definido	Auditorías sistemáticas seguimiento	Auditoría continua con dashboards
Mejora	Acciones correctivas y mejora	Acciones sobre incidentes	Mejora en servicios TI	No se gestionan	Acciones reactivas	Acciones correctivas documentadas	Seguimiento a efectividad	Cultura de mejora continua

Tabla 30. Plantilla Matriz Diagnostico

Bibliografía

- [1] M. A. Calvo Carmona and M. A. Zapata Rivas, "Desarrollo de un modelo de Sistema Integrado de Gestión mediante un enfoque basado en procesos," *XIV Congreso de Ingeniería de Organización Donostia- San Sebastián*, 2010.
- [2] "Sistemas de Gestión Integrados," NQA Organismo de certificación global. Accessed: Apr. 14, 2024. [Online]. Available: <https://www.nqa.com/es-co/certification/systems/integrated-management-systems>
- [3] Unctad, "Informe sobre tecnología e información 2023 (Panorama general)," 2023.
- [4] S. Cots and M. Casadesús, "Exploring the service management standard ISO 20000," *Total Quality Management and Business Excellence*, vol. 26, no. 5–6, pp. 515–533, Jun. 2015, doi: 10.1080/14783363.2013.856544.
- [5] "The iso survey of management system standard certifications – 2022 – The latest results of the Survey are for 2022." Accessed: Oct. 31, 2023. [Online]. Available: <https://www.iso.org/the-iso-survey.html>
- [6] "THE ISO SURVEY OF MANAGEMENT SYSTEM STANDARD CERTIFICATIONS-2023-EXPLANATORY NOTE The ISO Survey," 2024. [Online]. Available: <https://www.iso.org/the-iso-survey.html>.
- [7] E. C. Miranda, G. Rodríguez, and P. De Agreda, "Importance of Integrating Management Systems and its Connection with Development," *Facultad Latinoamericana de Ciencias Sociales*, vol. 8, no. Facultad Latinoamericana de Ciencias Sociales, 2020.
- [8] J. López Casarín, "La importancia y necesidad de las certificaciones en el proceso de innovación," *Forbes*. Accessed: Jul. 26, 2023. [Online]. Available: <https://www.forbes.com.mx/la-importancia-y-necesidad-de-las-certificaciones-en-el-proceso-de-innovacion/>
- [9] "tendencias ciberseguridad 2023," *CCN-CERT IA.35/23*, 2023.
- [10] Centro Criptológico Nacional, "CCN-CERT-IA-04-24_Ciberamenazas_y_Tendencias_2024," 2024, Accessed: Jul. 19, 2025. [Online].

Available: <https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html>

- [11] World Economic Forum, "Global Cybersecurity Outlook 2025," 2025.
- [12] M. V. Herrera, "ESTRUCTURACIÓN E IMPLEMENTACIÓN DE UN MODELO PARA LA INTEGRACIÓN AL SISTEMA GESTIÓN DE CALIDAD, DE LA GESTIÓN AMBIENTAL Y DE SEGURIDAD, EN LA EMPRESA ELÉCTRICA QUITO," Quito, Sep. 2014.
- [13] C. Pinto, P. Domingues, P. Sampaio, and O. Oliveira, "Integrated Management Systems in Industry 4.0: Literature Review," in *International Conference on Quality Engineering and Management*, 2022.
- [14] "Certificaciones de calidad para exportar: convocatoria de cofinanciación para empresas y laboratorios que deseen obtener certificaciones y acreditaciones internacionales," Colombia productiva. Accessed: Jul. 29, 2023. [Online]. Available: <https://www.colombiaproductiva.com/ptp-servicios/ptp-convocatorias/paraempresas/calidad-paraexportar>
- [15] "Universidad Nacional de Colombia Sede Manizales: Naturaleza, Fines y Principios." Accessed: Nov. 06, 2023. [Online]. Available: <https://www.manizales.unal.edu.co/menu/institucional/naturaleza-fines-y-principios/>
- [16] "Universidad Nacional de Colombia Sede Manizales: Administración de sistemas informáticos. Descripción", Accessed: Nov. 06, 2023. [Online]. Available: <http://www.manizales.unal.edu.co/menu/programas-academicos/carreras/administracion-desistemas-informaticos/>
- [17] Cristina, "TFM. PARTE I. Estado del Arte de los Sistemas de Gestión de la Calidad y el Medio Ambiente. Cristina Guzmán Aguilar."
- [18] J. M. Juran, Jr. Franc M. Gryna, and Jr. R. S. Bingham, *Manual de Control de la Calidad.*, Segunda., vol. 1. 1990.
- [19] C. A. Garzón, *Aseguramiento de la Calidad e Indicadores de Gestión*. 2017. [Online]. Available: <http://www.areandina.edu.co>
- [20] M. Constanza, C. Rodríguez, D. Rozo Rodríguez, and D. Rozo Rodríguez, "El concepto de calidad: Historia, evolución e importancia para la competitividad." [Online]. Available: <https://ciencia.lasalle.edu.co/ruls>
- [21] J. Perdomo Ortiz and J. González Benito, "MEDICIÓN DE LA GESTIÓN DE LA CALIDAD TOTAL: UNA REVISIÓN DE LA LITERATURA," Bogotá (Colombia), 2004.
- [22] "¿Qué son los sistemas de gestión basados en normas ISO? Ejemplos de normas ISO como la 18788, 22301 y 30300." Accessed: May 06, 2024. [Online]. Available:

<https://www.bvtrainingcommunity.com/es/blog/sistemas-de-gestion/que-son-los-sistemas-de-gestion-basados-en-normas-iso-ejemplos-de-normas>

- [23] A. López Neira and J. Ruiz Spohr, "SGSI. Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información." Accessed: Jul. 26, 2025. [Online]. Available: <https://www.iso27000.es/sgsi.html>
- [24] J. C. Oidor Gonzalez, "DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION-SGSI BAJO LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA 'EN LINEA FINANCIERA' DE LA CIUDAD DE CALI-COLOMBIA," 2016.
- [25] J. H. Quintero, "PARA LA INSTITUCIÓN EDUCATIVA LUIS CARLOS GALÁN DE VILLAGARZÓN PUTUMAYO JAIRO HERNANDO QUINTERO UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA," 2015.
- [26] D. Topalovic, "Historia de ITIL e ISO/IEC 20000: Mundos paralelos." Accessed: Jul. 26, 2025. [Online]. Available: https://advisera.com/20000academy/blog/2013/05/01/itil-isoiec-20000-history-parallel-worlds/?utm_source=chatgpt.com
- [27] International Organization for Standardization., "ISO/IEC 20000-1:2005 - Information technology - Service management - Part 1: Specification.," 2005.
- [28] M. Allue, B. Delgado, and C. M. Fernández, "Dar respuesta a la revolución digital con la ISO/IEC 20000-1," *AENOR: La revista de la evaluación de la conformidad*, Sep. 2019, Accessed: Jul. 26, 2025. [Online]. Available: <https://revista.aenor.com/351/dar-respuesta-a-la-revolucion-digital-con-la-isoiec-20000-1.html#:~:text=Tabla%201.,base%20de%20datos%20de%20configuraci%C3%B3n>).
- [29] T. V. Nunhes and O. J. Oliveira, "Analysis of Integrated Management Systems research: identifying core themes and trends for future studies," Aug. 17, 2018, *Routledge*. doi: 10.1080/14783363.2018.1471981.
- [30] BSI: bsigroup.es, "Documento técnico Introducción al Anexo SL: La nueva estructura de alto nivel para todas las futuras normas de sistemas de gestión".
- [31] T. V. Nunhes, T. L. R. Campos, F. E. Francisco, and O. J. de Oliveira, "Contributions of Annex SL to Corporate Sustainability," *Frontiers in Sustainability*, vol. 2, 2021, doi: 10.3389/frsus.2021.745350.

- [32] ISO, "SOBRE NOSOTROS." Accessed: Jul. 26, 2025. [Online]. Available: <https://www.iso.org/es/sobre#:~:text=ISO%2C%20la%20Organizaci%C3%B3n%20Internacional%20de,fabricar%20productos%20hasta%20gestionar%20procesos.>
- [33] International Organization for Standardization., "The Integrated Use of Management System Standards (IUMSS).," 2018.
- [34] R. A. López, *Sistema de Gestión de la Seguridad Informática*. 2017. [Online]. Available: <http://www.areandina.edu.co>
- [35] F. L. Landeta Guachamin and D. F. Quille Simbaña, "Análisis y diseño de un sistema de gestión de seguridad de la información en base a las normas ISO 27001 y 27002 para la superintendencia de control del poder de mercado," 2016.
- [36] F. J. Valencia Duque, *Sistema de gestión de seguridad de la información basado en la familia de normas iso/iec 27000*. 2021.
- [37] "Referencias Normativas ISO 27000," *ISO 27001*, Accessed: Jul. 26, 2025. [Online]. Available: <https://www.normaiso27001.es/referencias-normativas-iso-27000/#def37>
- [38] ISO, "ISO/IEC 20000-10:2018 Information technology — Service management — Part 10: Concepts and vocabulary," 2018.
- [39] S. Cots and M. Casadesús, "Implementing Service Management Standards: Motivations and Key Factors," 2018, pp. 83–96. doi: 10.1007/978-3-319-65675-5_5.
- [40] Revista Panorama Contable. Universidad EAFIT, "NORMAS ISO Y SU COBERTURA." Accessed: Jul. 19, 2025. [Online]. Available: <https://universidadeafit.widen.net/s/njlz5tsmrt/normas-iso-y-su-cobertura>
- [41] F. J. Valencia-Duque and M. Orozco-Alzate, "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000," *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, no. 22, pp. 73–88, Jun. 2017, doi: 10.17013/risti.22.73-88.
- [42] NQA, "Guía de transición ISO 27001:2022." Accessed: Jun. 19, 2025. [Online]. Available: <https://www.nqa.com/es-co/transitions/iso-27001-2022>
- [43] Normas ISO, "ISO 20000 Calidad de los Servicios TI." Accessed: May 20, 2025. [Online]. Available: <https://www.normas-iso.com/iso-20000/>
- [44] ISO - International Organization for Standardization, *ISO/IEC 27013:2021 Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*. 2021.
- [45] J. Villa, "ISO/IEC 27013 integración del SGSI y SGS," 2014.

- [46] Organización Internacional de Normalización, “ISO 31000:2018 Gestión de riesgos: directrices,” 2018.
- [47] C. Veritier, “ITIL E ISO / IEC 20000-ANÁLISIS, COMPARACIÓN Y SU RELACIÓN CON AGILE,” 2020.
- [48] M. Alshar'e, “CYBER SECURITY FRAMEWORK SELECTION: COMPARISON OF NIST AND ISO27001,” *Applied computing Journal*, pp. 245–255, Feb. 2023, doi: 10.52098/acj.202364.
- [49] Y. Fuentes Castillo, Y. Trujillo Casañola, and A. Velázquez Cintra, “Desarrollo de los requisitos según CMMI para la actividad productiva de la UCI,” *Revista Cubana de Ciencias Informáticas*, vol. 17, no. 3, 2023, [Online]. Available: <http://rcci.uci.cu>Pág.14-30
- [50] The CMMI Product Team, “CMMI Version 3.0 Model Overview: Domains and Practice Areas.” Accessed: Aug. 02, 2025. [Online]. Available: https://www.theoris.com/unlocking-the-power-of-cmmi-version-3-0-a-framework-for-organizational-performance/?utm_source=chatgpt.com
- [51] C. S. Guerrero Vega and N. Niño Meza, “Diseño de un Sistema Integrado de Gestión a partir de la integración de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013 para la empresa AMOVIL S.A.S,” 2023.
- [52] Sánchez - Toledo, “Correspondencia entre ISO 9001:2015, ISO 14001:2025 e ISO 45001:2018,” 2019.
- [53] G. Pallas Mega, “Metodología de Implantación de un SGSI en un grupo empresarial jerárquico,” 2009.
- [54] V. Nguyen, N. Nguyen, B. Schumacher, and T. Tran, “Article practical application of plan-do-check-act cycle for quality improvement of sustainable packaging: A case study,” *Applied Sciences (Switzerland)*, vol. 10, no. 18, Sep. 2020, doi: 10.3390/APP10186332.
- [55] International Organization for Standardization, *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. 2022.
- [56] Edenred, “Eficiencia, eficacia y efectividad: diferencias y cálculo.” Accessed: Aug. 09, 2025. [Online]. Available: <https://www.edenred.es/blog/eficiencia-eficacia-y-efectividad-diferencias-y-calculo/>
- [57] Lady Castillo Pineda, “El modelo Deming (PHVA) como estrategia competitiva para realzar el potencial administrativo,” 2019.

- [58] G. E. Barquero Huamani and M. M. Palomino Wong, "El Ciclo Deming en la calidad de servicio de los colaboradores, en un establecimiento de grifo, Ica – 2024," 2025.
- [59] D. V. Macedo Ramirez, R. Macedo Inuma, and K. Panaifo Gallardo, "Ciclo deming," Pucallpa, 2018.
- [60] M. García, C. Quispe, and L. Páez, "MEJORA CONTINUA DE LA CALIDAD EN LOS PROCESOS," 2003.
- [61] M. E. Álava Cuadra and H. A. Choez Salazar, "Diseño de un SGSI basado en el estándar ISO 27001 para la empresa Invimedica S.A.," 2023.
- [62] O. Serrat, "The Five Whys Technique," in *Knowledge Solutions*, Springer Singapore, 2017, pp. 307–310. doi: 10.1007/978-981-10-0983-9_32.
- [63] M. S. Hilasaca Zea, "Influencia del diagrama ISHIKAWA (causa - efecto) en la mejora de la productividad en el área de pre-fabricados en la empresa SUPERMIX S.A.," Universidad Andina "Néstor Cáceres Velásquez," Juliaca, 2018.
- [64] Y. A. Atehortua Tapias, "Estudio y aplicación del kaizen," Universidad Tecnológica de Pereira , Pereira, 2010.
- [65] P. S. . Szwed, *Expert judgment in project management : narrowing the theory-practice gap*. Project Management Institute, 2016.
- [66] J. Escobar Pérez and A. Cuervo Martínez, "Validez de contenido y juicio de expertos: una aproximación a su utilización en avances en medición," 2008. Accessed: Sep. 13, 2025. [Online]. Available: http://www.humanas.unal.edu.co/psicometria/files/7113/8574/5708/Articulo3_Juicio_de_expertos_27-36.pdf
- [67] P. Robles Garrote and M. del C. Rojas, "La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada," 2015, Accessed: Sep. 13, 2025. [Online]. Available: <https://revistas.nebrija.com/revista-linguistica/article/view/259/227>
- [68] M. Bustamante and O. Rivera, "LOS CONCEPTOS DE: MISIÓN, VISIÓN Y PROPOSITO ESTRATEGICO," 1991.
- [69] J. Fleitman, *Negocios exitosos: cómo empezar, administrar y operar eficientemente un negocio*. 2000.
- [70] G. A. Villaroel Mayorga, "Manual de funciones y procedimientos ejemplos."
- [71] B. A. I. Rodríguez, D. M. J. ; Baca, H. V. ; Santoyo Cortés, A. Reyes, and J. Cárdenas, "Revista Mexicana de Agronegocios," *Revista Mexicana de*

Agronegocios, vol. 32, pp. 231–244, 2013, [Online]. Available:
<http://www.redalyc.org/articulo.oa?id=14125584007>

- [72] Alberto Fernández, “El Balanced Scorecard: ayudando a implantar la estrategia,” Mar. 2001.
- [73] W.-R. Marchand-Niño and E. J. Vega Ventocilla, “Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS),” *Interfases*, pp. 57–76, 2020, doi: 10.26439/interfases2020.n013.4876.
- [74] Julio César López, “Análisis de matriz DOFA. Los orígenes del modelo de análisis DOFA ,” 2004.