

Diseño y desarrollo del plan de implementación de un Sistema integrado de Gestión basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022 para fortalecer los procesos y el aseguramiento de la información en Berruit SAS

Jeniffer Paola Moreno Cely
Yurany Pineda López

Convenio Universidad Santo Tomas e Icontec
Facultad de Ingeniería Mecánica
Maestría en Calidad y Gestión Integral
Bogotá, D.C
2026

Diseño y desarrollo del plan de implementación de un Sistema integrado de Gestión basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022 para fortalecer los procesos y el aseguramiento de la información en Berruit SAS

Jeniffer Paola Moreno Cely
Yurany Pineda López

Trabajo de grado para optar título de Magister en Calidad y Gestión integral

Modalidad Consultoría

Línea de investigación: Gestión integral de calidad y seguridad de la información

Director trabajo de grado:
Andrés Ernesto Rojas Ortega

Convenio Universidad Santo Tomas e Icontec
Facultad de Ingeniería Mecánica
Maestría en Calidad y Gestión Integral
Bogotá, D.C
2026

Resumen

El presente trabajo de grado, desarrollado bajo la modalidad de consultoría, tuvo como objetivo diseñar y desarrollar el plan de implementación de un Sistema Integrado de Gestión (SIG) basado en las normas NTC-ISO 9001:2015 (Gestión de la Calidad) e ISO/IEC 27001:2022 (Seguridad de la Información) para Berruit SAS, empresa dedicada a la prestación de servicios de tecnologías de la información y ciberseguridad. El diagnóstico inicial reveló un nivel de cumplimiento del 15 % frente a ambas normas, evidenciando brechas críticas en gestión por procesos, planificación estratégica y controles de seguridad de la información. Para abordar estos retos, se adoptó la especificación técnica PAS 99:2012 apoyada en la Estructura Armonizada de ISO (cláusulas 4 a 8), estructurando la intervención en cuatro fases alineadas con el ciclo PHVA: diagnóstico y análisis de brechas, construcción del plan de trabajo, diseño del SIG e implementación. La metodología integró técnicas cualitativas como revisión documental, entrevistas semiestructuradas, análisis DOFA-PESTEL, matrices de gestión de riesgos y elaboración de la Declaración de Aplicabilidad (SoA). Como resultado, se alcanzó un cumplimiento del 97,5 % en las cláusulas operativas, el 90,3 % en los controles del Anexo A de la ISO/IEC 27001:2022 y un promedio global del SIG del 82,7 %, superando la meta del 80 %. Se generaron más de 80 documentos codificados, estableciendo las bases organizacionales, procedimentales y normativas que preparan a Berruit SAS para avanzar hacia las fases de evaluación del desempeño, auditoría interna y certificación formal durante el año 2026.

Palabras Clave: Sistema integrado de gestión, gestión de la calidad, seguridad de la información, NTC-ISO 9001:2015, ISO/IEC 27001:2022, ciclo PHVA, PAS 99:2012, Ciberseguridad, Estandarización de procesos, Gestión de riesgos.

Abstract

This graduate work, developed under a consulting modality, aimed to design and develop an implementation plan for an Integrated Management System (IMS) based on the NTC-ISO 9001:2015 (Quality Management) and ISO/IEC 27001:2022 (Information Security) standards for Berruit SAS, a company specializing in the provision of information technology and cybersecurity services. The initial diagnosis revealed a compliance level of 15% against both standards, exposing critical gaps in process management, strategic planning, and information security controls. To address these challenges, the technical specification PAS 99:2012 was adopted, supported by the ISO Harmonized Structure (clauses 4 to 8), structuring the intervention in four phases aligned with the PDCA cycle: diagnosis and gap analysis, work plan construction, IMS design and structuring, and implementation. The methodology integrated qualitative techniques such as document review, semi-structured interviews, SWOT-PESTLE analysis, risk management matrices, and the development of the Statement of Applicability (SoA). As a result, a compliance level of 97.5% was achieved in the operational clauses, 90.3% in the Annex A controls of ISO/IEC 27001:2022, and an overall IMS average of 82.7%, exceeding the established target of 80%. More than 80 coded documents were generated, establishing the organizational, procedural, and normative foundations that prepare Berruit SAS to advance toward the performance evaluation, internal audit, and formal certification phases during 2026.

Keywords: Integrated Management System, Quality Management, Information Security, NTC-ISO 9001:2015, ISO/IEC 27001:2022, PDCA Cycle, PAS 99:2012, Cybersecurity, Process standardization, Risk management.

Tabla de contenido

1.	Introducción	10
2.	Contexto de la organización.....	13
2.1.	Ubicación y Reseña histórica.....	13
2.2.	Productos y servicios prestados por la organización	14
2.3.	Contexto internacional y del sector ISO 9001 e ISO27001.....	16
2.3.1.	Evidencia académica: impacto de la certificación ISO 9001 en empresas colombianas	17
2.3.2.	Colombia en el contexto latinoamericano: liderazgo y oportunidades.....	18
2.3.3.	ISO/IEC 27001 en Colombia: marco institucional y oportunidad estratégica en el sector TI	20
2.3.4.	Relevancia sectorial de ISO/IEC 27001 y acceso a mercados internacionales	21
2.3.5.	Síntesis y justificación del proyecto	22
3.	Problema de investigación o necesidades de la organización o sector	23
3.1.	Antecedentes	23
3.2.	Planteamiento del problema.....	24
3.3.	Formulación del problema	26
4.	Justificación	27
5.	Objetivos.....	29
5.1.	Objetivo general.....	29
5.2.	Objetivos específicos	29
6.	Marco referencial.....	30
6.1.	Marco teórico	30
6.1.1.	NTC ISO 9001:2015.....	31
6.1.2.	NTC-ISO/IEC 27001:2022.....	39
6.1.3.	INTEGRACIÓN DE LA NORMA NTC/ISO 9001:2015 Y LA NTC-ISO/IEC 27001:2022	45
6.2.	Marco normativo.....	55
6.3.	Metodologías de Integración.....	49
6.3.1.	Norma Española (AENOR) UNE 66177:2015 “Guía para la integración de sistemas de gestión”	49
6.3.2.	Uso integrado de estándares de sistemas de gestion (IUMSS).....	50
7.	Fases o etapas del plan de intervención	57
7.1.	Conformación del equipo de consultoría	63
7.2.	Cronograma.....	64
7.3.	Instrumentos y técnicas para la toma de información y para la presentación de resultados	64
8.	Resultados y discusión del proyecto	66
8.1.	Diagnóstico del estado de madurez de Berruit SAS frente al cumplimiento de las normas NTC-ISO 9001:2025 e ISO/IEC 27001:2022	66
8.1.1.	Análisis de los resultados del diagnóstico	74

8.2. Diseño del plan de trabajo para cumplimiento de requisitos ISO 9001 e ISO 27001.	78
8.3. Ejecución del plan de trabajo para el sistema integrado de gestión, numerales 4 al 8 de las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022.	81
8.3.1. Numeral 4.1 – Comprensión de la organización y su contexto.	83
8.3.2. Numeral 4.2 - Comprensión de las necesidades y expectativas de las partes interesadas	88
8.3.3. Numeral 4.3 – Determinación del alcance del Sistema de Gestión Integrado .	90
8.3.4. Numeral 4.4 – Sistema de gestión y sus procesos	93
8.3.5. Numeral 5 – Liderazgo	95
Liderazgo y compromiso	95
Política	96
Roles, responsabilidades y autoridades en la organización	97
8.3.6. Numeral 6 – Planificación	99
Acciones para abordar riesgos y oportunidades	100
Evaluación de riesgos de seguridad de la información	102
Tratamiento de riesgos y Declaración de Aplicabilidad	103
Objetivos del Sistema Integrado de Gestión y planificación para lograrlos	105
Planificación de los cambios	106
8.3.7. Numeral 7 – Apoyo	108
Recursos	108
Personas (Numeral 7.1.2)	109
Infraestructura (7.1.3)	110
Recursos de seguimiento y medición (7.1.5)	111
Conocimiento organizacional (7.1.6)	113
Competencia (7.2)	114
Toma de conciencia (7.3)	115
Comunicación (7.4)	116
Información documentada – 7.5	118
8.3.8. Numeral 8 – Operación	120
8.1 Planificación y control operacional	121
8.1.1 Estructura Procedimental Operacional	121
8.1.2 Planificación de la seguridad de la información	122
8.1.3 Comunicación operacional	123
8.2 Requisitos para los Productos y servicios (ISO 9001:2015)	123
8.2.1 Comunicación con el cliente	123
8.2.2 Determinación de los requisitos para productos y servicios	124
8.2.3 Revisión de los requisitos para productos y servicios	124
8.3 Diseño y Desarrollo de los Productos y Servicios (ISO 9001:2015)	125
8.4 Control de los Procesos, Productos y Servicios Suministrados Externamente (ISO 9001:2015)	125
8.4.1 Generalidades	126
8.4.2 Tipo y Alcance del Control	126
8.4.3 Información para los Proveedores Externos	127
8.5 - Producción y Provisión del Servicio (ISO 9001:2015)	127

8.5.1 Control de la Producción y de la Provisión del Servicio.....	127
8.5.2 Identificación y Trazabilidad.....	128
8.5.3 Propiedad Perteneciente a los Clientes o Proveedores Externos.....	128
8.5.4 Preservación	129
8.5.5 Actividades Posteriores a la Entrega	129
8.5.6 Control de los Cambios	130
8.6 Liberación de los Productos y Servicios (ISO 9001:2015)	130
8.7 Control de las Salidas No Conformes (ISO 9001:2015)	131
8.2 Evaluación de los Riesgos de Seguridad de la Información (ISO/IEC 27001:2022).	132
8.2.1 Metodología de Evaluación de Riesgos	132
8.2.2 Resultados de la Evaluación de Riesgos	133
8.3 Tratamiento de los Riesgos de Seguridad de la Información (ISO/IEC 27001:2022)	134
8.3.1 Controles de Tratamiento Implementados	134
8.4 Declaración de Aplicabilidad (Statement of Applicability — SoA) (ISO/IEC 27001:2022).....	136
8.4.1 Estadísticas de la Declaración de Aplicabilidad.....	136
8.4.2 No aplicabilidad de controles	137
8.4.3 Estado de Implementación y Plan de Acción.....	137
8.5 Gestión de la Continuidad del Negocio (ISO/IEC 27001:2022).....	138
8.6 Seguridad del Talento Humano en la Operación del SGI (ISO/IEC 27001:2022)	139
8.7 Gestión de PQRSF (ISO 9001:2015 e ISO/IEC 27001:2022)	140
8.8 Síntesis: La Operación como Eje del SGI.....	140
8.3.9. Cierre de la implementación del sistema integrado de gestión	141
9. Conclusiones y Recomendaciones.....	149
9.1. Conclusiones	149
9.2. Recomendaciones	149
10. Referencias.....	153
11. Anexos	161

Listado de Tablas

Tabla 1 Principales beneficios en la implementación de un SIG.....	46
Tabla 2 Correlación requisitos normas NTC/ISO 9001:2015 y la NTC-ISO/IEC 27001:2022.....	48
Tabla 3 Integración de sistemas de gestión mediante PASS 99 – 2012.....	52
Tabla 4 Clasificación de recursos requeridos para la integración.....	53
Tabla 5 Normatividad asociada al diseño e implementación de un sistema integrado de gestión basado en las normas NTC-ISO 9001:2015 E ISO/IEC 27001:2022 en BERRUIT SAS	55
Tabla 6 Criterios de evaluación herramienta diagnóstica ISO9001 E ISO27001	67
Tabla 7 Ejemplo de aplicación herramienta diagnóstica en BERRUIT SAS, numeral 5.3	68
Tabla 8 Matriz de comunicaciones	117
Tabla 9 Creación documental anexo 2 ISO/IEC 27001:2022.....	119
Tabla 10 Distribución de riesgos por proceso y nivel de criticidad.....	133
Tabla 11 Resumen estadístico de la declaración de aplicabilidad	136
Tabla 12 Cumplimiento por capítulo de normas – clausulas 4 al 10	142
Tabla 13 Cumplimiento por categoría – anexo a ISO/EIC 27001:2022	145

Listado de Figuras

Figura 1 Consolidado certificaciones por sistemas de gestión a nivel mundial.....	17
Figura 2 Posición de Colombia en el ranking LATAM por estándar ISO (2024)	19
Figura 3 Colombia e ISO/IEC 27001: posición regional y oportunidad de crecimiento global (2024).....	20
Figura 4 Sectores industriales con certificaciones ISO/IEC 27001 a nivel mundial (2024).....	22
Figura 5 Participación sector Tecnología en economía colombiana 2019.....	27
Figura 6 Gráfica Encuesta de Inversión en Investigación y Desarrollo I+D	28
Figura 7 Historia de la NTC ISO 9001	32
Figura 8 Triada de seguridad de la información	42
Figura 9 Metodología “Handbook”.....	50
Figura 10 Diagrama implementación del SIG en Berruit S.A.S	57
Figura 11 Cronograma de trabajo	64
Figura 12 Principales instrumentos y técnicas utilizados	65
Figura 13 Consolidado de cumplimiento en ISO 9001:2015, diagnóstico inicial Berruit SAS.....	70
Figura 14 Consolidado de cumplimiento en ISO/IEC 27001:2022, diagnóstico inicial Berruit SAS	70
Figura 15 Resultado diagnóstico aplicado Berruit SAS ante la norma ISO 9001:2015 por capítulo.	71
Figura 16 Resultado diagnóstico aplicado Berruit SAS ante la norma ISO/IEC 27001:2022 por capítulo.	73
Figura 17 Nivel de madurez inicial en Berruit SAS frente norma NTC-ISO 9001:2015	75
Figura 18 Nivel de madurez inicial en Berruit SAS frente norma ISO/IEC 27001:2022	76
Figura 19 Nivel de madurez inicial en Berruit SAS frente al sistema integrado de gestión	77
Figura 20 Misión y Visión de Berruit S.A.S.....	84
Figura 21 DOFA Berruit SAS.....	86
Figura 22 Resumen del análisis PESTAL.....	87
Figura 23 Mapa de procesos Berruit SAS.....	93
Figura 24 Organigrama Berruit S.A.S	98
Figura 25 Riesgos y oportunidades de proceso.....	102
Figura 26 Nivel de cumplimiento de cláusulas 4 al 10	144

1. Introducción

El sector de las Tecnologías de la Información y las Comunicaciones (TIC) experimenta una expansión en el mercado en las últimas décadas (La República, 2024), esto debido a los últimos cambios y transformación digital y la creciente demanda de soluciones tecnológicas y de ciberseguridad. En este contexto, las empresas del sector enfrentan el reto de garantizar la calidad de sus procesos y la seguridad de la información, aspectos esenciales para su competitividad y sostenibilidad en un entorno cada vez más regulado y exigente debido a las cambiantes dinámicas de la sociedad.

Berruit SAS, es una compañía dedicada a la venta de productos y servicios tecnológicos y de ciberseguridad, la cual reconoce la necesidad de estandarizar sus procesos y fortalecer la confianza de sus clientes y socios mediante la implementación de un Sistema Integrado de Gestión (SIG) basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022. La primera establece los lineamientos para la gestión de la calidad, permitiendo la mejora continua y la satisfacción del cliente, mientras que la segunda se enfoca en la protección, integridad y disponibilidad de la seguridad de la información, garantizando la protección de los activos digitales y el cumplimiento de las regulaciones vigentes.

Por lo tanto, este trabajo de consultoría tiene como propósito diseñar e implementar un SIG que integre las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022, asegurando la alineación de los procesos de la empresa con las mejores prácticas internacionales. En este sentido, la implementación de un SIG en Berruit SAS representa una ventaja estratégica clave en un sector altamente competitivo como el de las TIC y la ciberseguridad. La integración de las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022 permitirá optimizar la eficiencia operativa, reducir costos asociados a la no calidad y minimizar riesgos que estén relacionados con la protección y seguridad de la información. Adicionalmente, fortalecerá la capacidad de la empresa para poder cumplir con las exigencias y los requisitos normativos y contractuales exigidos por clientes y organismos de regulación, lo que a su vez incrementará su credibilidad y confianza en el mercado.

De igual manera, la certificación en estos estándares no solo diferenciará a Berruit SAS de sus competidores, sino que también le abrirá nuevas oportunidades de negocio con empresas y

sectores que exigen altos niveles de calidad y seguridad en sus proveedores tecnológicos. De esta manera, la adopción del SIG se convierte en un factor determinante para consolidar su crecimiento y liderazgo en la industria.

Dicho lo anterior, este trabajo contiene en el capítulo 1 el contexto de la organización Berruit SAS, su ubicación, una reseña histórica, las funciones generales de la compañía, los productos y servicios que ofrecen, y la descripción del sector en el que se desempeñan.

Posteriormente, en el capítulo 2 se plantean las necesidades de la organización, delimitando la problemática actual que dio lugar a la formulación de la siguiente pregunta: ¿De qué manera el diseño de un Sistema de Gestión Integrado, basado en las normas ISO 9001:2015 e ISO/IEC 27001:2022, permite a Berruit SAS, estandarizar sus procesos internos, mejorar la planificación, gestión, control y seguimiento de sus actividades, garantizando la gestión operativa y la seguridad de la información, fortaleciendo la confianza de sus partes interesadas y su competitividad en el mercado? .

En el Capítulo 3 se desarrolla la justificación, detallando la relevancia estratégica y los aportes de la consultoría para la solución del problema planteado. A continuación, en el capítulo 4 se plantea el objetivo general y los objetivos específicos de este trabajo de consultoría, seguido del capítulo 5 que contiene el marco teórico y normativo que describen tanto las teorías como la normatividad y regulaciones que soportan los temas que se abordan en este trabajo.

Más adelante, en el capítulo 6 se define la metodología para realizar la consultoría en la compañía, acto seguido se desarrollan cada uno de los objetivos específicos en el capítulo 7 y por último en el capítulo 8 se plantean las conclusiones y recomendaciones para la compañía Berruit SAS.

Como conclusión del trabajo, se evidencia la pertinencia de continuar la implementación de manera integrada de las normas ISO 9001:2015 e ISO/IEC 27001:2022. De acuerdo con el alcance desarrollado en la consultoría, se logró avanzar en la implementación de los numerales 4 al 8 de ambas normas; sin embargo, se sugiere que Berruit S.A.S. continúe con la implementación de los capítulos 9 y 10, relacionados con la evaluación del desempeño y la mejora, con el fin de consolidar el Sistema Integrado de Gestión, verificar su eficacia mediante auditorías internas y revisión por la dirección, y asegurar la mejora continua del sistema en el tiempo.

2. Contexto de la organización

Berruit S.A.S es una empresa colombiana especializada en la gestión tecnológica de la información y ciberseguridad empresarial. Su enfoque principal es proporcionar soluciones tecnológicas innovadoras para optimizar la infraestructura digital de sus clientes, garantizando la protección de datos, la gestión operativa y la competitividad y permanencia en un mercado digital en constante evolución.

La empresa opera en el sector de tecnologías de la información (TI), un ámbito fundamental para el crecimiento y desarrollo de las empresas en la actualidad. La digitalización de los procesos empresariales y la creciente necesidad de seguridad informática han convertido a este sector en un pilar clave para la sostenibilidad y expansión de cualquier organización.

Berruit S.A.S se distingue por su capacidad de ofrecer un portafolio integral de servicios, incluyendo ciberseguridad, outsourcing de TI, consultoría en infraestructura tecnológica, soluciones en la nube, monitoreo de redes y desarrollo de software a la medida. Su objeto de negocio se basa en la prestación de servicios personalizados que responden a las necesidades específicas de cada cliente, fortaleciendo su transformación digital y garantizando el cumplimiento de los más altos estándares de seguridad y eficiencia.

La empresa en la actualidad viene posicionándose como un aliado estratégico para organizaciones que buscan mejorar su infraestructura tecnológica, reducir riesgos que estén relacionados a la seguridad de la información y optimizar su operatividad mediante soluciones avanzadas.

2.1. Ubicación y Reseña histórica

La organización se encuentra radicada en Bogotá, Colombia, con proyección en el mercado latinoamericano. Su infraestructura tecnológica y modelo de negocio le permiten prestar servicios de alcance nacional e internacional, con un enfoque en la transformación digital y la protección de datos para empresas de diversos sectores. (Berruit Internacional, s.f.)

Fue fundada el 25 de abril de 2014 como una empresa unipersonal que ofrecía servicios básicos de soporte técnico, mantenimiento de computadores y limpieza de equipos electrónicos.

Durante sus primeros años, la empresa se enfocó en atender necesidades puntuales de pequeñas empresas y clientes individuales.

El 24 de abril de 2017, dio un salto significativo en su evolución, consolidándose como Berruit S.A.S y ampliando su portafolio de servicios hacia la gestión avanzada de servidores Windows, redes informáticas y soluciones de ciberseguridad.

A medida que el mercado demandaba soluciones tecnológicas más robustas, expandió su enfoque hacia la consultoría IT, el cableado estructurado, el cloud computing y la automatización de procesos empresariales. Con ello, logró consolidarse como un proveedor integral de soluciones tecnológicas para empresas que buscan mejorar su infraestructura digital y garantizar la seguridad de su información.

En la actualidad, se ha convertido en un referente en el sector de TI, con una visión de convertirse en un líder global en ciberseguridad y automatización empresarial para el año 2030. Su objeto de negocio se basa en la construcción de relaciones estratégicas con sus clientes, fomentando la innovación y el desarrollo de soluciones personalizadas para fortalecer la transformación digital de las empresas.

2.2. Productos y servicios prestados por la organización

Berruit S.A.S ofrece un portafolio integral de productos y servicios tecnológicos diseñados para mejorar la seguridad, estabilidad y eficiencia operativa de sus clientes. Su enfoque principal es proporcionar soluciones tecnológicas de vanguardia que permitan a las empresas optimizar sus procesos y mitigar riesgos de un entorno digital complejo y en constante cambio.

Las principales soluciones se centran en:

- **Protección de la infraestructura tecnológica:** Implementación de soluciones de ciberseguridad avanzadas para mitigar riesgos asociados a ataques informáticos y pérdida de datos. (Berruit SAS, s.f.)

- **Optimización de procesos empresariales:** Desarrollo e implementación de tecnologías que mejoran la eficiencia operativa y facilitan la automatización de procesos.
- **Consultoría IT:** Asesoramiento especializado en infraestructura tecnológica, seguridad informática y transformación digital.
- **Monitoreo y soporte IT:** Servicios de outsourcing IT que garantizan la estabilidad y operatividad de los sistemas tecnológicos de los clientes.
- **Capacitación y formación:** Programas de capacitación en ciberseguridad y gestión tecnológica para empresas y sus equipos de trabajo.

Berruit S.A.S ofrece servicios especializados en tecnología de la información, estructurados en dos grandes categorías, servicios y productos

Se ofrecen los siguientes servicios

- **Ciberseguridad empresarial:** Implementación de sistemas de protección contra amenazas digitales, monitoreo de redes y auditorías de seguridad. (Berruit SAS, s.f.)
- **Outsourcing IT:** Servicios de externalización de tecnologías de la información, permitiendo a las empresas delegar la gestión de su infraestructura tecnológica.
- **Consultoría IT:** Diagnósticos, asesorías y estrategias personalizadas para optimizar la infraestructura de TI de las empresas.
- **Outsourcing BPO:** Servicios de tercerización para la gestión eficiente de procesos empresariales mediante soluciones tecnológicas.
- **Capacitación en ciberseguridad:** Formación especializada para empresas y equipos de TI en buenas prácticas de seguridad informática.

- **Evaluaciones de seguridad (Assessment de seguridad):** Diagnósticos de vulnerabilidades y auditorías de seguridad para fortalecer la protección de la información.
- **Diagnóstico general de tecnología:** Análisis integral de la infraestructura tecnológica de las empresas para identificar oportunidades de mejora y optimización en sus procesos.

En cuanto a productos se ofrece tanto hardware como software, y se describen a continuación (Berruit SAS, s.f.):

Software:

- Licencias de software especializado.
- Suscripciones a plataformas tecnológicas.
- Services de Platform as a Service (PaaS), Infrastructure as a Service (IaaS) y Software as a Service (SaaS).

Hardware:

- Equipos de cómputo y servidores.
- Sistemas de energía y redes de telecomunicaciones.
- Equipos de almacenamiento y procesamiento de datos.

2.3. Contexto internacional y del sector ISO 9001 e ISO27001.

El panorama mundial de las certificaciones bajo estándares ISO refleja un crecimiento sostenido que evidencia la creciente conciencia organizacional sobre calidad, seguridad y eficiencia operativa. Según el reporte *ISO Survey 2024* (Global Standards, 2025), elaborado a partir de datos del repositorio aifcertsearch.org, en 2024 se emitieron 1.474.118 certificaciones ISO 9001:2015 en 2.321.640 sitios certificados a nivel global, representando un incremento del 76 % frente a las 837.978 certificaciones de 2023. La norma ISO/IEC 27001 alcanzó 96.709

certificaciones en 179.877 sitios, con una variación interanual del 104 %, constituyéndose en el estándar de mayor crecimiento en el período analizado (Global Standards, 2025). La Figura 1 presenta el comparativo global.

Figura 1 Consolidado certificaciones por sistemas de gestión a nivel mundial.



Fuente: GlobalSTD Certification. (2025). Infografía ISO Survey 2024 [Infografía en PDF]. https://www.globalstd.com/wp-content/uploads/2025/10/Infografia-ISO-Survey-2024_ES.pdf

La Figura 1 se ilustra la variación interanual de las dos normas objeto del presente trabajo, evidenciando que la ISO/IEC 27001 duplicó su base de certificaciones en tan solo un año, fenómeno atribuible a la digitalización masiva de la economía global y al aumento sostenido de ciberataques (Global Standards, 2025). El panorama mundial de las certificaciones bajo estándares ISO refleja un crecimiento sostenido que evidencia la creciente conciencia organizacional sobre calidad, seguridad y eficiencia operativa. Según el reporte *ISO Survey 2024* (Global Standards, 2025), elaborado a partir de datos del repositorio aifcertsearch.org, en 2024 se emitieron 1.474.118 certificaciones ISO 9001:2015 en 2025).

2.3.1. Evidencia académica: impacto de la certificación ISO 9001 en empresas colombianas

Más allá de los datos estadísticos globales, la literatura académica colombiana ofrece evidencia empírica sobre el impacto concreto que genera la certificación ISO 9001 en las organizaciones del país. El estudio seminal de Benzaquen-de Las Casas y Convers-Sorza (2015), publicado en el *Journal of Globalization, Competitiveness & Governability*, analizó una muestra

de 207 empresas colombianas y encontró diferencias estadísticamente significativas en los nueve factores de gestión de calidad total (TQM) evaluados, siendo consistentemente superiores en las organizaciones con certificación ISO 9001 frente a las no certificadas. Los autores concluyen que la certificación se asocia directamente con mejores niveles de competitividad, productividad y posicionamiento en el mercado (Benzaquen-de Las Casas & Convers-Sorza, 2015), hallazgo de particular relevancia para Berruit S.A.S como empresa que compite en el exigente sector TI colombiano.

En el ámbito regional, Martínez-Rojas et al. (2018) estudiaron los factores de éxito de la certificación ISO 9001 en 71 empresas de Cúcuta y su área metropolitana, publicando sus resultados en Estudios Gerenciales. Sus hallazgos evidencian que 23 de los 24 criterios de gestión evaluados se cumplen en más del 95 % de las empresas analizadas, siendo la mejora continua el factor con mayor impacto reportado. El estudio también confirma que la certificación ISO 9001 incide positivamente en la eficiencia operativa y la sostenibilidad empresarial (Martínez-Rojas et al., 2018), dimensiones que resultan estratégicamente alineadas con los objetivos de Berruit S.A.S en cuanto a la optimización de sus procesos de servicio y la fidelización de clientes.

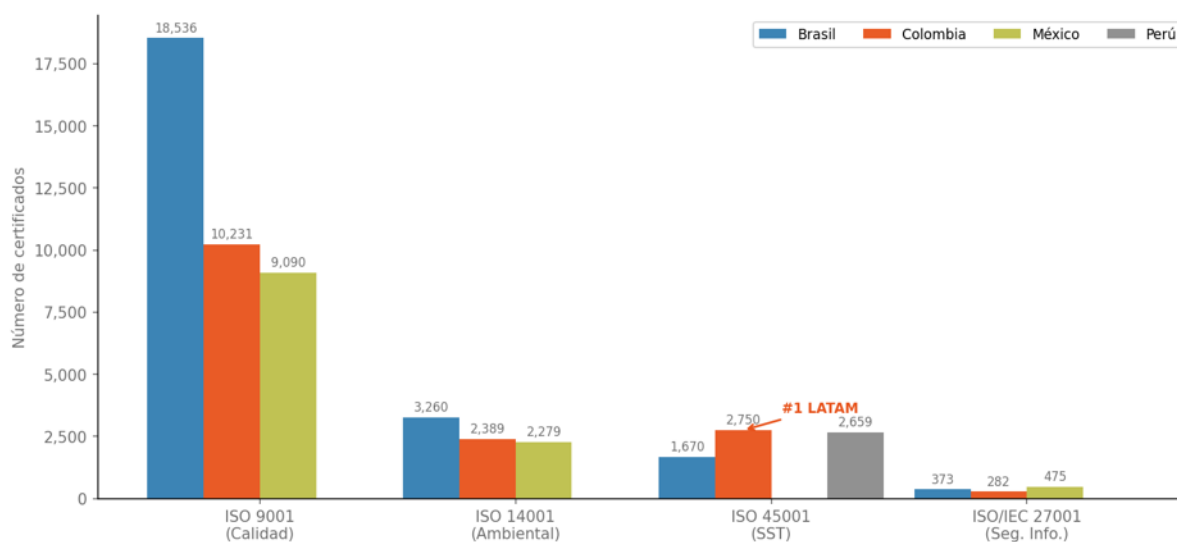
Desde una perspectiva de gestión del servicio al cliente en el contexto colombiano, Gutiérrez Gómez y Playonero Ortiz (2019), en su trabajo depositado en el repositorio de la Universidad Santiago de Cali, señalan que la implementación de la ISO 9001:2015 en empresas de servicios favorece la obtención de la certificación de calidad y permite distinguir a la organización por ofrecer un trato diferenciado a sus clientes, contribuyendo al incremento de la satisfacción y a la mejora continua del servicio (Gutiérrez Gómez & Playonero Ortiz, 2019). Este argumento cobra especial relevancia para Berruit S.A.S, cuyo modelo de negocio descansa precisamente en la prestación de servicios tecnológicos personalizados.

2.3.2. Colombia en el contexto latinoamericano: liderazgo y oportunidades

Dentro del contexto latinoamericano, Colombia presenta un comportamiento diferenciado según el estándar analizado. Según el ISO Survey 2024 (Global Standards, 2025), Colombia ocupa el primer lugar en América Latina en certificaciones ISO 45001:2018 (Seguridad y Salud en el

Trabajo) con 2.750 certificados, y el segundo lugar en ISO 14001:2015 con 2.389 certificaciones. Complementariamente, el portal G-Certi (2025), con base en el mismo ISO Survey, ubica a Colombia en el puesto 18 a nivel mundial en ISO 9001, con 10.231 certificaciones activas, lo que lo posiciona como uno de los mercados de calidad más maduros de la región. La Figura presenta la comparación del desempeño de Colombia frente a Brasil, México y Perú en los principales estándares ISO.

Figura 2 Posición de Colombia en el ranking LATAM por estándar ISO (2024)



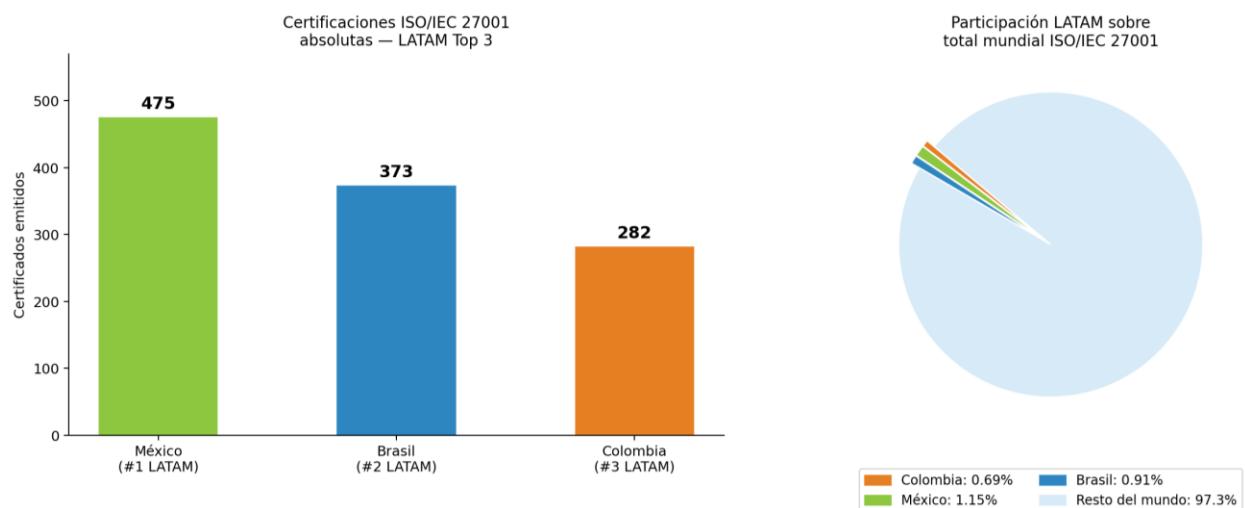
Nota: GlobalSTD Certification. (2025). Infografía ISO Survey 2024 (basado en datos de ISO.org) [Infografía en PDF]. https://www.globalstd.com/wp-content/uploads/2025/10/Infografia-ISO-Survey-2024_ES.pdf

En cuanto a la ISO 9001:2015, ICONTEC (2023) organismo nacional de normalización según el Decreto 2269 de 1993 y miembro oficial de ISO para Colombia (ISO, 2024) reporta más de 10.100 certificaciones vigentes en el país, enfatizando que los estándares ISO constituyen una herramienta estratégica para la competitividad y la internacionalización de las empresas colombianas (ICONTEC, 2023). Esta afirmación se ve respaldada por datos que señalan que más del 50 % de las empresas exportadoras colombianas certificadas mejoraron su desempeño en comercio internacional tras la implementación del sistema de gestión de calidad (ICONTEC, 2023).

2.3.3. ISO/IEC 27001 en Colombia: marco institucional y oportunidad estratégica en el sector TI

En materia de seguridad de la información, Colombia ocupa el tercer lugar de América Latina con 282 certificaciones ISO/IEC 27001 en 2024, detrás de México (475) y Brasil (373), según el ISO Survey 2024 (Global Standards, 2025). Si bien esta cifra representa el 0,29 % del total mundial de 96.709 certificaciones, la tasa de crecimiento del 104 % de esta norma configura una ventana de oportunidad significativa para el sector TI colombiano. La Figura 3 ilustra la posición relativa de Colombia en el contexto regional y la participación en el total mundial.

Figura 3 Colombia e ISO/IEC 27001: posición regional y oportunidad de crecimiento global (2024)



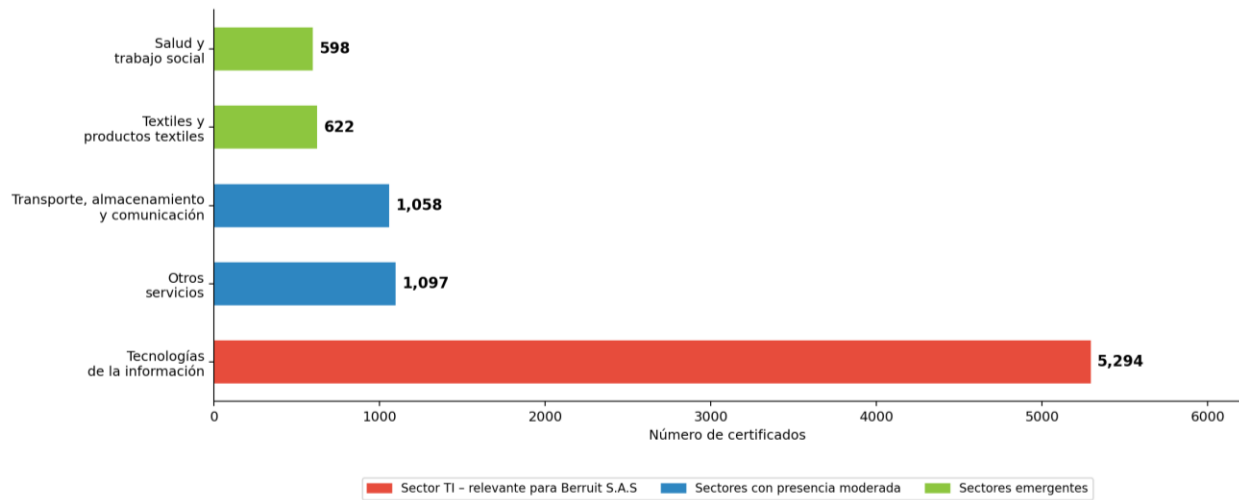
Nota: GlobalSTD Certification. (2025). Infografía ISO Survey 2024 [Infografía en PDF]. https://www.globalstd.com/wp-content/uploads/2025/10/Infografia-ISO-Survey-2024_ES.pdf

Desde el marco institucional, ICONTEC adoptó la norma NTC-ISO/IEC 27001:2013 como traducción idéntica (IDT) del estándar internacional, con participación del sector bancario y de telecomunicaciones a través del Comité Técnico 181 de Técnicas de Seguridad de la Información (ICONTEC, 2013). Esta adopción temprana fue impulsada por la necesidad de gestionar y controlar los riesgos de seguridad de la información en sectores donde la información y la tecnología son activos críticos de negocio (ICONTEC, 2013).

A nivel regulatorio, el ecosistema colombiano provee incentivos normativos adicionales para la adopción de la ISO/IEC 27001. La *Ley 1581 de 2012 (Habeas Data)* establece obligaciones de protección de datos personales que se alinean directamente con los controles del Anexo A de la norma; la regulación de la Superintendencia Financiera de Colombia (SFC) exige a las fintech y entidades del sector financiero, demostrar controles de seguridad de la información; y el sector BPO en el que Colombia se ha consolidado como hub para EE. UU. y América Latina, requiere la ISO/IEC 27001 como estándar de confianza ante clientes internacionales (G-Certi, 2025). Para Berruit S.A.S, empresa de base TI que presta servicios a clientes corporativos en sectores regulados, esta convergencia normativa y de mercado refuerza la urgencia y pertinencia estratégica de la certificación.

2.3.4. Relevancia sectorial de ISO/IEC 27001 y acceso a mercados internacionales

A escala global, el ISO Survey 2024 (Global Standards, 2025) confirma que el sector TI es el principal adoptante de la norma ISO/IEC 27001, con 4.671 certificaciones —más de cuatro veces el segundo sector (otros servicios, 1.097)—. En Colombia, el 91 % de las certificaciones ISO/IEC 27001 se concentra en el sector de tecnologías de la información y el 9 % restante en intermediación financiera (ISO.org, 2024), lo que confirma que Berruit S.A.S opera en el subsector de mayor demanda de esta norma en el país. La Figura 4 presenta la distribución sectorial global de la ISO/IEC 27001.

Figura 4 Sectores industriales con certificaciones ISO/IEC 27001 a nivel mundial (2024)

Nota: GlobalSTD Certification. (2025). Infografía ISO Survey 2024 [Infografía en PDF]. https://www.globalstd.com/wp-content/uploads/2025/10/Infografia-ISO-Survey-2024_ES.pdf

Desde la perspectiva de acceso a mercados internacionales, la certificación ISO 9001 ofrece ventajas competitivas tangibles. Los registros de ICONTEC (2023) indican que más del 50 % de las empresas exportadoras colombianas certificadas mejoraron su desempeño en comercio internacional, consolidando la norma como una herramienta estratégica de internacionalización. Asimismo, la adopción de estándares ISO facilita el cumplimiento de exigencias contractuales en licitaciones públicas y privadas, donde cada vez con mayor frecuencia se requiere la certificación como requisito demostrable, generando un efecto en cascada que impulsa la certificación de nuevas empresas proveedoras (Benzaquen-de Las Casas & Convers-Sorza, 2015; ICONTEC, 2023).

2.3.5. Síntesis y justificación del proyecto

La convergencia de evidencia estadística, académica e institucional permite identificar tres argumentos centrales que justifican el diseño e implementación del Sistema Integrado de Gestión ISO 9001:2015 e ISO/IEC 27001 en Berruit S.A.S. En primer lugar, la ISO/IEC 27001 registra el mayor crecimiento interanual entre todos los estándares ISO (104 %), con el sector TI como su principal adoptante a nivel global y en Colombia (Global Standards, 2025; G-Certi, 2025; ICONTEC, 2013). En segundo lugar, la evidencia académica colombiana demuestra que la

certificación ISO 9001 genera diferencias estadísticamente significativas en competitividad, eficiencia operativa y sostenibilidad entre empresas certificadas y no certificadas (Benzaquen-de Las Casas & Convers-Sorza, 2015; Martínez-Rojas et al., 2018). En tercer lugar, Colombia se ubica en el puesto 18 mundial en ISO 9001 y en el tercer lugar de LATAM en ISO/IEC 27001, en un ecosistema normativo —Ley Habeas Data, regulación SFC, exigencias BPO— que incentiva activamente la adopción de estándares de seguridad de la información (G-Certi, 2025; ICONTEC, 2023). Estos factores configuran un entorno de alta pertinencia para que Berruit S.A.S implemente ambas normas como palanca de competitividad, confianza y expansión en el mercado colombiano e internacional.

3. Problema de investigación o necesidades de la organización o sector

3.1. Antecedentes

Basado en las anteriores estadísticas, referencias académicas e institucionales se puede demostrar cómo la implementación de la ISO 9001 de Gestión de Calidad e ISO/IEC 27001 de Gestión de seguridad de la información pueden ayudar a una organización a la mejora operativa, tener mayor presencia en el mercado y confianza con los clientes actuales.

Respecto al mejorar la gestión operativa, ISO 9001 promueve la estandarización de los procesos, optimizando los recursos y los flujos de trabajo internos, reduce errores y reprocesos, beneficiando al cliente y la empresa. ISO/IEC 27001 define lineamientos y controles para la protección de la información, reduciendo ataques cibernéticos e interrupciones en la operación que pueden generar pérdidas económicas y reputacionales.

En términos de posicionamiento en el mercado y fortalecimiento de la confianza de los clientes, la norma ISO 9001 está orientada a la mejora continua de la calidad de los productos y servicios ofrecidos, mediante el cumplimiento de estándares internacionales y de los requisitos del cliente, lo que se refleja en mayores niveles de satisfacción. Por su parte, la norma ISO/IEC 27001 contribuye a que las organizaciones sean percibidas como entidades más seguras y confiables, al garantizar una adecuada gestión y protección de la información. Como resultado, las empresas que

implementan esta norma fortalecen su credibilidad y reputación ante clientes, proveedores y demás partes interesadas.

En el caso de Berruit SAS, la certificación ISO/IEC 27001 representa un respaldo estratégico con un impacto particularmente positivo, dado que está directamente relacionada con su producto y servicio principal. Asimismo, como organización basada en funciones y servicios tecnológicos, Berruit cuenta con una valiosa oportunidad para adoptar un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a esta norma. La ISO/IEC 27001 proporciona un marco integral para la protección de los activos de información de la organización y de sus clientes, mediante la identificación, evaluación y tratamiento de los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos. Su implementación no solo fortalece la seguridad de la información, sino que también incrementa la confianza de los clientes y aliados estratégicos, generando una ventaja competitiva en el mercado (Arias y Manrique, 2020).

3.2. Planteamiento del problema

Berruit SAS, presenta retos en la planificación, control y seguimiento de sus actividades, debido a la falta de estandarización de los procesos internos identificados en el marco del Sistema de Gestión de la Calidad y los riesgos asociados a estos procesos en el marco de seguridad de la información. Estas debilidades de la organización no solo afectan la eficiencia operativa y la confianza de los clientes, sino que también se ha identificado por la Alta Dirección una barrera para la expansión a nuevos negocios y el fortalecimiento de la competitividad en el mercado.

A esta problemática de la organización, se suma, que el sector TIC en Colombia ha experimentado un notable crecimiento, lo que también ha impulsado la creciente exposición de las empresas a diversos riesgos que pueden ser explotados a través de sus vulnerabilidades. Entre estos, los activos de información se destacan como uno de los elementos más valiosos y críticos, ya que requieren una protección adecuada que garantice los principios de disponibilidad, confidencialidad e integridad. Según la investigación de Pirani (2022), empresa global especializada en soluciones de seguridad informática, los ciberataques dirigidos a empresas aumentaron un 59 % en 2022 respecto del año anterior, siendo el ransomware como el principal tipo de ciberataque que enfrentan las organizaciones. Pirani (2022) señala que una de cada 40

empresas ha sido víctima de este tipo de ciberataque, que, en términos generales, consiste en el secuestro de información con el fin de exigir un pago para su liberación. (Pirani 2022).

El sector tecnológico en Colombia ha atravesado un año 2024 complicado, caracterizado por desafíos derivados de las dificultades económicas globales, tensiones internacionales, variaciones inflacionarias, incertidumbres legislativas y la constante amenaza de ciberataques (Montoya Al, 2024), las cifras indican que un promedio del 60% de las empresas colombianas han presentado al menos un incidente de seguridad en los últimos 12 meses, lo que subraya la necesidad urgente de mejorar la conciencia y la preparación en este ámbito. De acuerdo con un informe de la consultora PwC, el 34% de las empresas en Colombia han sido víctimas de fraude en sus plataformas digitales en los últimos dos años, lo que resalta la importancia de adoptar medidas de seguridad más robustas. (CCIT, 2024).

Sin embargo, muchas empresas todavía no cuentan con una estrategia integral de ciberseguridad. De acuerdo con un estudio, únicamente el 37% de las empresas en Colombia disponen de un control formal de respuesta a incidentes de seguridad cibernética, lo que resalta la urgencia de fomentar una mayor conciencia y preparación en este campo. (CCIT, 2024).

Este trabajo pretende abordar la problemática de Berruit a través del diseño y ejecución de un plan de implementación de un sistema de gestión integrado basado en las normas ISO9001 e ISO27001, que abarque el diagnóstico del estado actual de la organización a través de la aplicación de una herramienta de diagnóstico integrada, estructurar un plan para el cumplimiento de los requisitos integrados y la ejecución del plan desde el requisito de análisis del contexto organizacional hasta el control operacional. De esta forma, aportar a Berruit a la estandarización de los procesos internos, la mejora de la planificación, gestión, control operacional, el seguimiento de sus actividades, la eficiencia operativa y la administración de los riesgos de seguridad de la información. Con el propósito que la organización se encamine a dar un paso estratégico a la construcción de relaciones de confianza con los clientes actuales y fortalecer sus capacidades para la competitividad, permanencia y expansión en el mercado

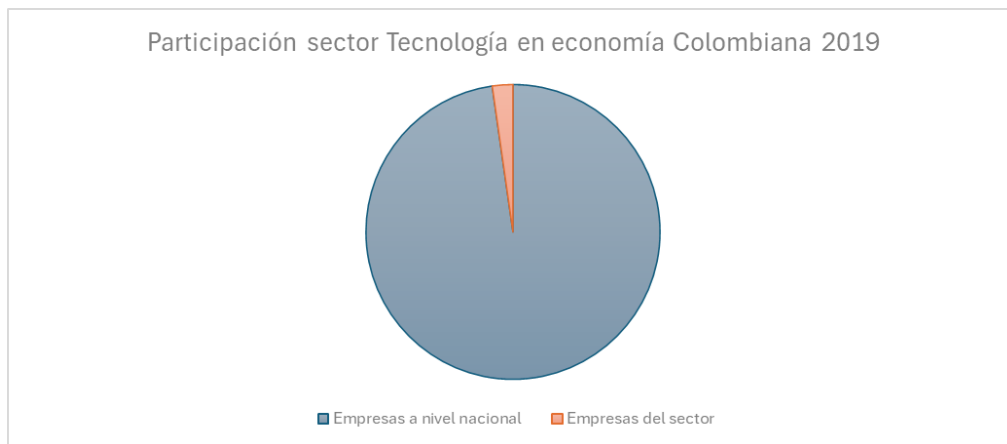
3.3. Formulación del problema

¿Cómo el diseño y desarrollo de un plan de implementación de un sistema de gestión integrado basado en las normas ISO 9001 e ISO/IEC 27001 puede contribuir a la estandarización de los procesos internos, la gestión de riesgos de seguridad de la información y el fortalecimiento de la competitividad y confiabilidad de Berruit SAS en el sector TI?.

4. Justificación

En los últimos años, la tecnología en Colombia ha experimentado un notable crecimiento, al punto de convertirse en un sector clave tanto para el producto interno bruto (PIB) como para el mercado laboral del país (Datacrédito Experian, 2024). Según el Directorio Estadístico de Empresas 2019-2022 del DANE, en 2021, de las 5.704.308 empresas registradas en Colombia, tanto de naturaleza natural como jurídica, 131.877 estuvieron dedicadas a actividades de información y comunicaciones, lo que representa un 2,3 % (CCIT, 2022), según la figura 5.

Figura 5 Participación sector Tecnología en economía colombiana 2019



Nota: Elaboración propia con base en datos DANE (2021)

Según la Federación de Software y TI (Fedesoft), desde 2010, las empresas del sector han experimentado un crecimiento continuo, acelerado por la pandemia. La industria tecnológica de Colombia aumentó su valor 7.3 veces, generando más de 150.000 empleos y alcanzando un 2.94% del PIB, un porcentaje que se ha mantenido en 2021 y 2022.

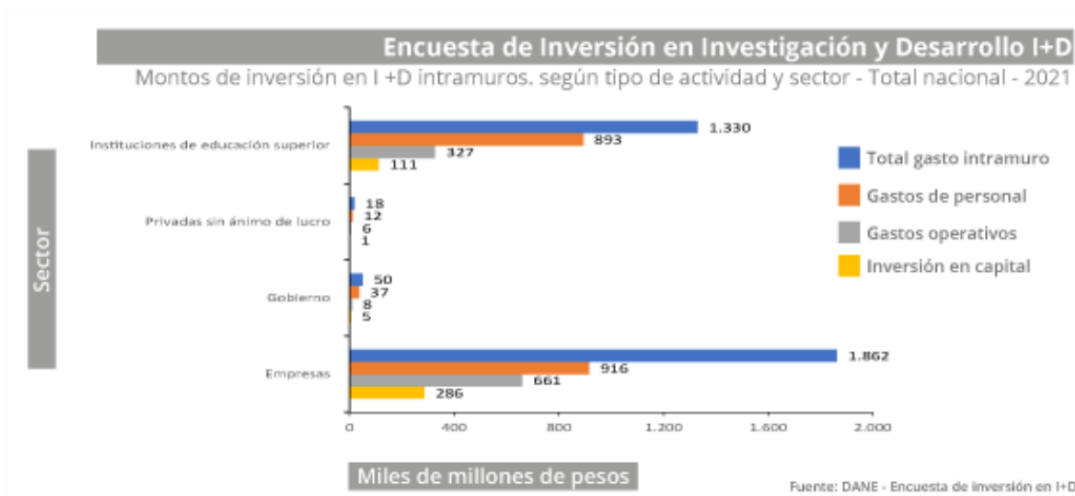
Este avance ha permitido que Colombia se consolide como el cuarto mercado tecnológico más grande de Latinoamérica, solo por detrás de Brasil, México y Chile (Datacrédito Experian, 2024).

A pesar de la problemática mencionada, el sector ha demostrado resiliencia y continuo crecimiento dando paso a la innovación y desarrollando soluciones disruptivas. (Montoya Al,

2024), aumentando las inversiones en soluciones para proteger activos y datos, se proyecta un crecimiento significativo en el mercado latinoamericano de ciberseguridad. (CCIT, 2024).

En 2021, el DANE realizó una encuesta a empresas de diversos sectores económicos para medir el porcentaje de inversión en investigación y desarrollo (I+D). Los resultados mostraron que la inversión total en los sectores analizados alcanzó los \$3,3 billones. Los sectores que realizaron mayor inversión fueron las empresas, con \$1,9 billones y las instituciones de educación superior, con \$1,3 billones. Estos dos sectores representaron el 57,1% y el 40,8% del total, respectivamente (DANE, 2021), ver figura 6.

Figura 6 Gráfica Encuesta de Inversión en Investigación y Desarrollo I+D



Nota: Información tomada de DANE (2021)

De acuerdo con un estudio realizado por la compañía Mordor Intelligence, se proyecta que este mercado alcanzará los US\$ 8,92 mil millones en 2024, con una estimación de llegar a US\$ 12,48 mil millones en 2029. Esto representa un crecimiento a una tasa anual compuesta del 6,95% durante el período de 2024 a 2029, lo que refleja el aumento en la demanda de servicios y productos de seguridad cibernética en la región.

Lo anterior constituye una valiosa oportunidad de crecimiento y desarrollo para BERRUIT. Por esta razón, se busca contribuir al fortalecimiento y preparación interna de la compañía, con el fin de que cuente con las herramientas, procesos y capacidades necesarias para alcanzar el crecimiento esperado.

5. Objetivos

5.1. Objetivo general

Diseñar y desarrollar un plan de implementación para un Sistema de Gestión Integrado basado en ISO 9001:2015 e ISO/IEC 27001:2022 para Berruit SAS, abarcando desde el análisis del contexto organizacional hasta el control operacional correspondiente al numeral 8 de las normas; que permita la estandarización de los procesos internos, la gestión adecuada de los riesgos de seguridad de la información, con el propósito de fortalecer la confiabilidad con los clientes y competitividad en el sector TI.

5.2. Objetivos específicos

- Diagnosticar el cumplimiento de los requisitos de las normas ISO 9001:2015 e ISO/IEC 27001:2022 con el fin de establecer el nivel de cumplimiento de Berruit SAS.
- Establecer el plan de trabajo identificando los procesos clave y sus interacciones para cumplir los requisitos del Sistema de Gestión Integral ISO 9001 e ISO/IEC 27001.
- Desarrollar el plan de implementación del Sistema Integrado de Gestión basado en las normas ISO 9001:2015 e ISO/IEC 27001:2022, desde el análisis del contexto organizacional hasta el control operacional, con el propósito de alcanzar un nivel de cumplimiento superior al 80 % de los requisitos aplicables, fortaleciendo la confianza de los clientes y la competitividad de Berruit S.A.S. en el sector de tecnologías de la información.

6. Marco referencial

El presente capítulo desarrolla el marco referencial que soporta teórica y normativamente este trabajo consultoría. En ese sentido, se incluyen antecedentes relevantes que permiten contextualizar el diseño e implementación del SGI, junto con los fundamentos teóricos clave para comprender su enfoque y alcance. Así mismo, se abordan la normatividad y estándares aplicables, con el fin de establecer una base sólida para el desarrollo del trabajo de consultoría. En consecuencia, este marco no solo facilita la comprensión del problema de investigación, sino que también orienta la aplicación de metodologías y el análisis de resultados, garantizando un enfoque estructurado y fundamentado.

6.1. Marco teórico

Algunas empresas han decidido implementar la norma ISO 9001:2015 como respuesta a las dificultades para alcanzar sus objetivos de crecimiento, lo que ha impactado negativamente en sus ventas y en la calidad de sus productos y servicios. Por otro lado, muchas organizaciones han adoptado un Sistema de Gestión de la Calidad (SGC) no solo como una herramienta para superar estos desafíos, sino también como una estrategia para agregar valor a sus procesos y promover una cultura de mejora continua que impulse su competitividad. Estas empresas reconocen que fortalecer la cultura organizacional y desarrollar las habilidades de sus colaboradores puede potenciar sus productos y servicios. Además, al involucrar a la alta gerencia en el diseño e implementación del SGC, se motiva a otras áreas de la organización, promoviendo un entorno de trabajo colaborativo y consolidando a la empresa como un equipo sólido.

Con el avance de la tecnología, la protección de la información se ha convertido en una prioridad esencial. En este sentido, la implementación de la norma ISO/IEC 27001 resulta fundamental para proteger eficazmente la información crítica de la organización, adoptar un enfoque proactivo hacia la seguridad de los datos y demostrar que las empresas que cumplen con estos estándares internacionales son más confiables (Fiore et al.,2022).

La adopción de las normas NTC ISO 9001 e ISO/IEC 27001 no solo garantiza la eficiencia y confiabilidad en los procesos organizacionales, sino que también alinea a la organización con sus objetivos estratégicos, facilitando la toma de decisiones y mejorando su posicionamiento en el

mercado. En este contexto, se plantea la asesoría a BERRUIT SAS para diseñar e implementar estas normas, contribuyendo así a su crecimiento y fortaleciendo la confianza con sus clientes.

6.1.1. NTC ISO 9001:2015

La norma internacional NTC ISO 9001:2015 especifica los requisitos para implementar un Sistema de Gestión de la Calidad (SGC), y está basada en la norma NTC ISO 9000:2015, la cual describe los conceptos y los principios fundamentales de la gestión de la calidad que son aplicables a organizaciones de cualquier sector o tamaño (ICONTEC, 2015). El SGC se centra en garantizar que los productos y servicios cumplan completamente con los requisitos del cliente y con las normativas legales aplicables, promoviendo así la mejora continua y la satisfacción del cliente.

Uno de los enfoques clave de la NTC ISO 9001:2015 es el enfoque basado en procesos, que ayuda a las organizaciones planificar y gestionar sus procesos de manera eficiente, asegurando que las interacciones entre ellos estén alineadas para lograr los resultados deseados. Este enfoque se apoya en el Ciclo de Deming (PHVA), que establece las fases de Planificar, Hacer, Verificar y Actuar. Al aplicar este ciclo, las organizaciones logran que sus procesos cuenten con los recursos adecuados, se gestionen eficazmente y se identifiquen oportunidades de mejora de manera constante (ICONTEC, 2015). El ciclo PHVA fomenta una cultura de mejora continua, donde los ajustes y optimizaciones se realizan de forma proactiva, mejorando el rendimiento general del SGC.

Además, la norma introduce el pensamiento basado en el riesgo, un enfoque que ayuda a las organizaciones a identificar los factores que podrían desviar los procesos y el sistema de gestión de calidad de los resultados planificados. Este enfoque tiene como objetivo no solo prevenir posibles problemas, sino también implementar controles preventivos que minimicen los efectos negativos (ICONTEC, 2015). Al mismo tiempo, permite maximizar las oportunidades que puedan surgir, optimizando el uso de los recursos y aumentando la resiliencia de la organización.

El SGC no solo busca mejorar la calidad de los productos y servicios, sino también aumentar la eficiencia operativa, reducir costos y garantizar que los procesos se ajusten a los cambios en el contexto empresarial. Mediante la aplicación del pensamiento basado en el riesgo,

las organizaciones pueden abordar de manera anticipada posibles amenazas y oportunidades, fortaleciendo la capacidad de respuesta frente a un mercado en constante evolución.

El Sistema de Gestión de la Calidad basado en la NTC ISO 9001:2015 proporciona un marco sólido para que las organizaciones mejoren continuamente, gestionen sus procesos de manera efectiva y tomen decisiones informadas basadas en análisis de riesgo y datos objetivos. Esto no solo garantiza la satisfacción del cliente, sino que también contribuye al éxito sostenido de la organización a largo plazo.

Antecedentes

En el año 1987 la norma británica BS 5750 fue el modelo para la primera edición de la NTC ISO 9001, desde entonces la norma ha pasado por varios cambios significativos, en el cual se destaca mayor facilidad de uso e implementación. La NTC ISO 9001:2015 determina los requisitos generales para el sistema de gestión en el cual no se especifica para un sector en particular, sino que aplica para todos (Kohl, 2020).

La NTC ISO 9001:2015 ha pasado por cambios desde el año 1987 desde su primera publicación hasta la fecha como se evidencia en la figura 7:

Figura 7 Historia de la NTC ISO 9001



Nota. La figura muestra la historia de la norma NTC ISO 9001:2015. Fuente: elaboración propia con base en Kohl (2020)

Fundamentos teóricos sobre la gestión de la calidad

En el desarrollo de este trabajo, es fundamental abordar qué significa la calidad y su importancia en organizaciones que buscan una mejora continua y la satisfacción del cliente mediante productos y servicios que ofrezcan valor percibido y beneficios tangibles. La calidad, según la NTC - ISO 9000, se define como “una organización orientada a la calidad promueve una cultura que da como resultado comportamientos, actitudes y procesos para proporcionar valor mediante el cumplimiento de las necesidades y expectativas de los clientes y otras partes interesadas pertinentes” (ICONTEC, 2015).

Impacto de la gestión de la calidad en diversas dimensiones.

De acuerdo con Carro & González (2020), algunas de las dimensiones en las que la norma ISO 9001 tiene impacto en una organización son las siguientes:

- **Costos y participación en el mercado:** Mejorar la calidad se traduce en mayor participación en el mercado y reducción de costos al disminuir las fallas, los reprocesos y las devoluciones por productos defectuosos.
- **Prestigio de la organización:** La calidad impacta la reputación de una empresa mediante la percepción que los clientes tienen de sus productos y el desempeño del personal. Las relaciones con proveedores y las prácticas internas también influyen en esta percepción.
- **Responsabilidad del producto:** Las organizaciones que producen productos o servicios defectuosos pueden ser responsables de daños o lesiones causados, lo cual implica costos legales y acuerdos que pueden afectar la imagen de la compañía, además de inversiones adicionales en publicidad para restaurar la confianza del cliente.
- **Implicaciones internacionales:** La calidad tiene un alcance global, tanto a nivel empresarial como nacional, y está sujeta a expectativas y necesidades de calidad y precio que son reconocidas en el mercado global.

Adicionalmente, para Bakhtiar (2023), la implementación de la NTC ISO 9001:2015 incrementa la confianza y satisfacción del cliente mediante un sistema de calidad organizado, documentado y gestionado. Esto impulsa el rendimiento de los empleados y promueve un entorno laboral positivo. Sin embargo, la implementación también enfrenta obstáculos, como la falta de personal calificado, una cultura organizacional deficiente, falta de interés de la alta dirección, resistencia al cambio y recursos limitados en aspectos como financieros, de personal o infraestructura. Estos factores pueden disminuir la efectividad del sistema de calidad, afectando la relación con el cliente.

Superar estos obstáculos requiere de una cultura organizacional sólida y de un equipo de trabajo competente. Es fundamental contar con infraestructura adecuada y condiciones físicas favorables, como buena iluminación, áreas de descanso y temperatura regulada, que promuevan la productividad. Además, aspectos como la motivación y la empatía son cada vez más importantes para mejorar el rendimiento (Hernández et.al., 2022).

Finalmente, el éxito o el fracaso de la gestión de calidad en una organización puede depender de su cultura organizacional. Esta cultura, reflejada en las actitudes, comportamientos, valores y creencias de líderes y trabajadores, puede potenciar o limitar las capacidades de los colaboradores. Para lograr una ventaja competitiva sostenible, las empresas deben evitar una cultura restrictiva y, en cambio, desarrollar una cultura creativa y flexible que impulse la innovación y la adaptabilidad (Hernández et.al., 2022).

El vínculo entre liderazgo y la calidad

El liderazgo en la gestión de calidad se convierte en una filosofía de dirección integral que transforma la forma de pensar y actuar de los miembros de una organización (Pupo et.al., 2021). Para alcanzar los objetivos de calidad, los líderes deben establecer un propósito y proporcionar orientación estratégica, además de crear un ambiente interno que fomente el compromiso de los trabajadores con los objetivos organizacionales (Pupo et.al., 2021).

De acuerdo con Ramírez et.al., (2019) y Moreno et al., (2023), se presentan cuatro estilos de liderazgo que pueden influir de diferentes maneras en la cultura de calidad de una organización:

- Autoritario: Este estilo se basa en el autoritarismo, recurriendo a la coacción y la recompensa para guiar a los empleados. El líder toma todas las decisiones y asigna las tareas sin involucrar al equipo, limitando su participación. Este enfoque permite una organización estricta, pero tiende a inhibir la autonomía y la colaboración del grupo.
- Autocrático: En este modelo, el líder centraliza la autoridad y toma decisiones de manera unilateral, con métodos de trabajo impuestos y poca participación de los empleados. Aunque este estilo puede ser efectivo en situaciones que requieren control estricto, también puede limitar la iniciativa y el compromiso del equipo.
- Democrático: Aquí, el líder promueve la participación del grupo de trabajo en la toma de decisiones, incentivando un ambiente de colaboración y confianza. La opinión de cada miembro se toma en cuenta y el grupo discute los planes antes de su implementación. Este estilo es efectivo para construir una cultura de trabajo inclusiva y comprometida, mejorando la moral y el sentido de pertenencia.
- Laissez-faire: Este estilo es de mínima intervención, donde el líder adopta un rol pasivo y otorga libertad total para que cada miembro del equipo tome decisiones sin apenas dirección. El líder interviene solo en situaciones extremas. Aunque fomenta la independencia, puede dar lugar a una falta de cohesión y dirección si no se controla adecuadamente.

Según Ramírez et.al., (2019), en la actualidad los liderazgos transaccionales y transformacionales emergen como apoyo para dinamizar la gestión del cambio. El liderazgo transaccional considera al líder como una pieza fundamental para el éxito del cambio organizacional, su responsabilidad abarca la planificación y dirección del cambio, lo cual incluye la estructuración de procesos con el objetivo de reducir la incertidumbre, mantener la estabilidad y asegurar el logro de los objetivos establecidos; este estilo de liderazgo es especialmente adecuado cuando se requiere garantizar resultados detallados y el cambio puede ser planificado y ejecutado de manera gradual, no obstante, es importante estar preparado para manejar imprevistos, manteniendo el control sobre las situaciones cotidianas que puedan surgir. El liderazgo transformacional necesita que el líder tenga características que le permitan enfrentar situaciones desafiantes e inspirar a su grupo el abordamiento de los problemas de maneras nuevas y creativas.

Este tipo de líder estimula a su equipo a cuestionar tanto sus propias creencias y valores como los del líder, en especial cuando las soluciones no son las idóneas para resolver los problemas actuales.

Principios de gestión de la calidad

Es fundamental destacar los principios de gestión de la calidad descritos en la Norma NTC - ISO 9000, entre los cuales se encuentra:

- El enfoque al cliente tiene como objetivo satisfacer sus requisitos y, en lo posible, superar sus expectativas (ICONTEC, 2015). Para garantizar el éxito sostenido, es fundamental que las empresas atraigan y mantengan la confianza tanto de los clientes como de otras partes interesadas, cumpliendo con sus necesidades y expectativas, las cuales cambian con el tiempo. Además, deben asegurarse de que los productos y servicios que ofrecen aporten valor a sus clientes, lo que fortalece la reputación de la empresa, incrementa las ganancias y amplía su participación en el mercado. Sin embargo, para que una empresa perdure en el tiempo, también es esencial prestar atención a sus clientes internos, es decir, a los empleados. La cultura organizacional desempeña un papel fundamental en este aspecto, ya que promover el bienestar de los colaboradores contribuye directamente a la solidez y al éxito a largo plazo de la organización (Kohl, 2020).
- El **liderazgo** es fundamental para el éxito de una organización. Según la norma NTC - ISO 9000:2015 define, “Los líderes establecieron la unidad de propósito y la dirección, y crean las condiciones necesarias para que las personas se comprometan con el logro de los objetivos de calidad de la organización” (ICONTEC, 2015). Esto permite a las empresas aumentar su eficacia y eficiencia al cumplir dichos objetivos. Además, el liderazgo facilita la coordinación de los procesos, mejora la comunicación entre los distintos niveles y funciones, y contribuye al desarrollo y fortalecimiento de la capacidad tanto de la empresa como de su personal para entregar los resultados deseados. Los líderes también garantizan la disponibilidad de recursos financieros, humanos y de otro tipo necesarios para alcanzar los objetivos establecidos. El líder tiene la responsabilidad de planificar, implementar y controlar el cumplimiento de las políticas, estrategias y actividades

relacionadas con la calidad. La alta dirección, por su parte, debe adoptar una filosofía y política orientada a la generación de productos y servicios de calidad, lo que hace indispensable el seguimiento, la medición, el análisis y la evaluación de estos. Por ello, es esencial formar tanto a los altos directivos como al personal que está en contacto con los clientes, tanto internos como externos (Pupo et.al., 2021).

- El **compromiso de las personas** es clave para aumentar la capacidad de la organización de generar y proporcionar valor. Se busca que los empleados sean competentes, empoderados y comprometidos, y que sean respetados e involucrados activamente en todos los niveles de la organización (ICONTEC, 2015). Para lograr esto, es fundamental reconocer sus esfuerzos, proporcionarles el conocimiento necesario y mejorar sus competencias, lo que facilita su compromiso con los objetivos de calidad de la empresa. Además, es esencial hacerles conscientes de la importancia del sistema de gestión de calidad y cómo este impacta en su área (Kohl, 2020). Estimular su iniciativa y creatividad, brindándoles confianza y aumentando su satisfacción, fomentando su colaboración en toda la organización. Esto, a su vez, facilita un diálogo abierto, permitiendo que se compartan conocimientos y experiencias de manera efectiva.
- En cuanto al **enfoque a procesos**, la norma NTC - ISO 9000:2015 establece que “se alcanzan resultados coherentes y previsibles de manera más eficaz y eficiente cuando las actividades se comprenden y gestionan como procesos interrelacionados que funcionan como un sistema coherente” (ICONTEC, 2015). Esto implica la necesidad de identificar los procesos relevantes para la calidad y sus interacciones, comprendiendo que el sistema genera resultados consistentes y previsibles. Esto permite a la organización optimizar el desempeño del sistema, focalizando los esfuerzos en procesos clave, teniendo en cuenta sus entradas, salidas y oportunidades de mejora. Al gestionar los procesos de manera eficiente, se logra un uso óptimo de los recursos y una disminución de las barreras interdisciplinarias. De este modo, la organización genera confianza entre las partes interesadas, asegurando coherencia, eficacia y eficiencia, y garantizando que todos comprendan los procesos y sus interacciones.

- La **Mejora** es un principio fundamental en la gestión de la calidad y representa el enfoque continuo que las organizaciones deben adoptar para alcanzar el éxito a largo plazo. La mejora en la calidad no solo es clave para mantener y elevar los niveles actuales de desempeño, sino que también permite a las organizaciones adaptarse, reaccionar y anticiparse a cambios en sus condiciones internas y externas (ICONTEC, 2015). Para impulsar este proceso de mejora continua, es esencial fomentar un pensamiento basado en el riesgo, lo cual no solo ayuda a prevenir problemas, sino que también permite identificar y crear nuevas oportunidades. En este contexto, el personal es un recurso vital: su implicación y desarrollo son fundamentales para implementar procesos de mejora efectivos, ya que el rendimiento, el servicio y la calidad de los productos son criterios cruciales para evaluar tanto la capacidad de la organización como la satisfacción del cliente. Adoptar un enfoque de investigación proactiva y promover el uso del análisis de causa raíz permite a la organización identificar problemas desde su origen, aplicando acciones preventivas y correctivas efectivas (Kohl, 2020). Este ciclo de detección, prevención y corrección no solo fortalece la calidad, sino que también consolida una cultura de mejora continua en todos los niveles de la organización.
- **La toma de decisiones basada en la evidencia** se centra en el análisis y evaluación de datos objetivos para fundamentar decisiones con un enfoque lógico y estructurado, lo que incrementa la probabilidad de alcanzar los resultados deseados. Aunque el análisis de datos proporciona una base sólida, es importante reconocer que la interpretación de la información puede implicar cierto grado de subjetividad, lo cual exige cuidado en la evaluación de los datos (Kohl, 2020). Para una toma de decisiones eficaz, es necesario recopilar datos de diversas fuentes relevantes, tales como el control de procesos, encuestas de satisfacción y calificación por parte de los clientes, quejas y reclamos, resultados de auditorías y cualquier otra fuente pertinente (Kohl, 2020). Es fundamental validar los métodos de medición empleados y, cuando sea posible, comparar los resultados con otros estándares para garantizar que los datos utilizados sean concluyentes, precisos y útiles. Al asegurar que la información es confiable y efectiva, las organizaciones pueden tomar decisiones informadas que permiten controlar los impactos de sus acciones y

responder de manera proactiva a los desafíos (Kohl, 2020). Con esta metodología, los resultados demuestran decisiones más eficientes y un mejor rendimiento en todos los procesos.

- Para la **gestión de las relaciones** la norma NTC - ISO 9000, lo define “para el éxito sostenido, las organizaciones gestionan sus relaciones con las partes interesadas pertinentes, tales como los proveedores” (ICONTEC, 2015). Este principio toma relevancia en el SGC ya que comprende la importancia en sus relaciones con sus proveedores y socios que crean un impacto en el desempeño de la organización, manteniendo un éxito sostenido, generando criterios y métodos de evaluación de las relaciones comerciales (ICONTEC, 2015), comprendiendo los beneficios mutuos y la interdependencia de las relaciones que se establezcan (Kohl, 2020), lo que impacta en la cadena de suministro y a su vez proporciona un flujo estable de productos y servicios (Kohl, 2020). Los hace ser exhaustivos en la elección de nuestros proveedores, teniendo evaluaciones de desempeño, calidad de los productos y servicio y el respaldo postventa, generando una ganancia para ambas compañías, nos hace mantenernos en el tiempo y tener credibilidad y confianza con nuestro cliente final.

6.1.2. NTC-ISO/IEC 27001:2022

Considerando el objetivo de este trabajo, otra norma de interés para implementar en la organización Berruit SAS es la NTC-ISO/IEC 27001:2022, relacionada con el Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma permite una integración con el Sistema de Gestión de Calidad, lo que puede hacer que la gestión organizacional sea más eficiente y efectiva. Además, su implementación resulta especialmente relevante, dado que la misión de Berruit SAS se centra en la ciberseguridad, la protección de datos y otras necesidades tecnológicas definidas dentro del alcance de la organización.

En ese sentido, la seguridad de la información se asocia generalmente a la gestión de tecnologías de la información y las comunicaciones, cuyo objetivo es mantener los riesgos controlados respecto a la información organizacional y de los dispositivos tecnológicos, los cuales permiten su recepción, tratamiento, acceso, intercambio, almacenamiento, transformación y

adecuada presentación. De igual manera, la ISO/IEC 27000 define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información (Valencia, 2021).

La NTC-ISO/IEC 27001 de 2022 sobre el Sistema de gestión de seguridad de la información, proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de seguridad de la información. Las organizaciones pueden implementar este sistema en línea con sus necesidades y objetivos, los requisitos de seguridad que deban cumplir, sus procesos y estructura de la organización (ISO, 2022).

Es importante la implementación de un sistema de seguridad de la información porque preserva la confidencialidad, la integridad y la disponibilidad de la información para gestionar adecuadamente los riesgos de información de las organizaciones, la cual puede ser integrada con otros sistemas como el de gestión de calidad (ISO, 2022).

Así mismo, Whitman y Mattord (2012) señalan que una organización exitosa debe implementar múltiples capas de seguridad para proteger sus operaciones. Entre estas, la seguridad de la información desempeña un papel fundamental, ya que busca garantizar la confidencialidad, integridad y disponibilidad de los activos de información, tanto los que se encuentran almacenados como aquellos que están en proceso de transmisión o tratamiento. Para lograrlo, es necesario establecer políticas y controles adecuados, así como promover procesos de educación, capacitación y concientización del personal, apoyados por el uso de tecnologías que contribuyan a la protección efectiva de la información.

Principios fundamentales de la seguridad de la información

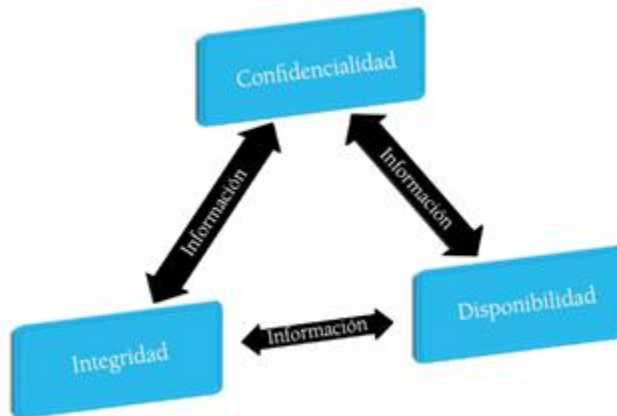
La seguridad de la información se sustenta en tres principios fundamentales: confidencialidad, integridad y disponibilidad. Es esencial revisar cada uno de estos para lograr una comprensión más completa de esta norma.

- El principio de confidencialidad busca asegurar que el acceso a la información esté restringido exclusivamente al personal autorizado. Para su cumplimiento, las organizaciones deben implementar controles adecuados en la gestión y tratamiento

de los datos. En este sentido, Whitman y Mattord (2012) señalan que la información preserva su confidencialidad cuando se encuentra protegida contra la divulgación a individuos o sistemas no autorizados; por ende, cualquier acceso o visualización por parte de terceros sin los privilegios requeridos constituye una vulneración directa a este principio.

- En relación con el principio de integridad, las organizaciones deben garantizar que la información no sea alterada, modificada, destruida o perdida, ya sea por errores accidentales, acciones maliciosas o fallos en los sistemas. Este principio exige que la información conserve su exactitud, consistencia y estado original desde su creación y durante todo su ciclo de vida. Por ello, resulta fundamental implementar controles de seguridad que permitan prevenir modificaciones no autorizadas y proteger los activos de información frente a posibles amenazas. La afectación de este principio puede generar consecuencias significativas para la organización, impactando la confiabilidad de los datos y la toma de decisiones. Al respecto, Whitman y Mattord (2012) señalan que la información posee integridad cuando se encuentra completa y libre de corrupción. En consecuencia, la integridad se ve comprometida cuando la información es expuesta a situaciones que alteran su condición auténtica, ya sea durante su almacenamiento, procesamiento o transmisión.
- Respecto al principio de disponibilidad, es necesario garantizar que la información esté accesible para las personas autorizadas por la organización y que puedan acceder a ella cuando lo requieran.

Conforme a lo antes mencionado, Valencia (2021) señala que la seguridad de la información se asocia a la confidencialidad (C), integridad (I) y disponibilidad (D), de acuerdo con la comunidad académica y profesional, siendo estos los objetivos a los que debe apuntar cualquier sistema de gestión de seguridad de la información, ver figura 8.

Figura 8 Triada de seguridad de la información

Nota. Adaptado de Triada de seguridad de la información (p. 38), por Valencia (2021), Repositorio Institucional UNAL.

En consecuencia, De la Cruz et al. (2023) menciona que la seguridad de la información es la protección de la confidencialidad, integridad y disponibilidad de la información, y que esta sea accesible solo a las personas autorizadas, sea exacta sin sufrir modificaciones no deseadas por la organización y que esté disponible cuando lo requieran.

Por otro lado, es fundamental considerar la Ley Estatutaria 1581 de 2012, mediante la cual se establecen las disposiciones generales para la protección de datos personales en Colombia. El objeto de esta ley consiste en:

Desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Ley 1581 de 2012, art. 1).

Asimismo, la Ley 1581 de 2012 establece que sus disposiciones "serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada" (Ley 1581 de 2012, art. 2).

De igual manera, esta norma contempla los principios que orientan el tratamiento de datos personales, entre los que se encuentran los principios de legalidad, finalidad, libertad, veracidad o

calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad (Ley 1581 de 2012, art. 4). Estos principios constituyen un marco de referencia fundamental para la gestión de la información de clientes, proveedores y demás partes interesadas dentro de las organizaciones.

Riesgos de la seguridad de la información

Las organizaciones están expuestas a diversas amenazas que pueden comprometer la seguridad de la información, por lo que resulta fundamental identificarlas, analizarlas y gestionarlas adecuadamente para minimizar su impacto sobre las operaciones y el cumplimiento de los objetivos organizacionales. En este sentido, Whitman y Mattord (2012) definen la gestión de riesgos como el proceso mediante el cual se identifican los factores que pueden afectar los activos de información y la infraestructura tecnológica de una organización, con el propósito de implementar medidas de control que reduzcan su exposición a niveles aceptables.

Asimismo, los autores señalan que, en aquellas organizaciones cuya operación depende significativamente de las tecnologías de la información, la seguridad de la información y la gestión de riesgos deben formar parte integral del proceso de toma de decisiones empresariales. Esto implica evaluar el equilibrio entre los costos asociados a la implementación de controles de seguridad y los beneficios derivados de contar con sistemas seguros, confiables y disponibles.

En consecuencia, la gestión de riesgos constituye un proceso continuo orientado a la identificación, análisis, evaluación y tratamiento de eventos potenciales que puedan afectar la confidencialidad, integridad y disponibilidad de la información. De esta manera, las organizaciones fortalecen su capacidad de respuesta ante incidentes y contribuyen a la continuidad y estabilidad de sus operaciones

En la gestión de la seguridad de la información y teniendo en cuenta que la información es vulnerable a riesgos, es necesario abordar el concepto de **ciberseguridad**, la ISO/IEC 27032 (como se citó en Valencia, 2021) define la ciberseguridad como:

La norma ISO/IEC 27032 (2012) define la ciberseguridad como la «preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio», entendiendo este último como el «entorno resultante de la interacción de personas, software e internet, a través

de dispositivos tecnológicos y redes conectadas a él que no existen en ninguna forma física» (p. 2).

Dicho lo anterior, la ciberseguridad aborda una parte específica de la gestión de la seguridad de la información, por lo tanto, se enfoca en la protección de las amenazas de información que se encuentran únicamente en el espacio virtual.

Beneficios de la implementación de la NTC-ISO/IEC 27001 de 2022

La implementación de la NTC-ISO/IEC 27001 de 2022 brinda varios beneficios a las organizaciones ya sea del sector público o privado, en ese sentido, Kirvan (2023) menciona que los marcos de seguridad suministran un punto de partida para establecer procesos, políticas y actividades técnico administrativas para la gestión de la seguridad de la información, y un marco común es la norma NTC-ISO/IEC 27001 de 2022, e indica que la implementación de esta norma es útil si la organización necesita demostrar sus capacidades sobre seguridad de la información. En la norma en mención, se señalan los requisitos para implementar un sistema de gestión de la seguridad de la información (SGSI) y los controles respectivos.

Dicho lo anterior, al implementar la NTC-ISO/IEC 27001 de 2022 las organizaciones contarán con un Sistema de Gestión de Seguridad de la Información que proteja la información de la exposición o divulgación a personas o sistemas no autorizados, previniendo la pérdida de la integridad de esta. Las personas podrán tener acceso a la información de acuerdo con los criterios que defina cada organización, por tanto, se contará con información disponible.

Asimismo, con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), la organización podrá identificar y gestionar los riesgos asociados a la seguridad de la información, contribuyendo así a la prevención de amenazas y la mitigación de su impacto en los productos y servicios. Este sistema también permite optimizar los recursos al mejorar la eficiencia de los procesos internos, reducir los incidentes de seguridad y facilitar una toma de decisiones más informada y oportuna.

De igual manera, el Sistema de Gestión de Seguridad de la Información facilita el cumplimiento de la normatividad vigente, incluyendo en Colombia las disposiciones de la Ley

Estatutaria 1581 de 2012 sobre protección de datos personales. Además, su implementación fortalece la confianza y la reputación de la organización frente a clientes y proveedores. La obtención de una certificación en esta norma permite a las organizaciones destacar a nivel nacional e internacional en su campo de competencia, abriendo mejores oportunidades de negocio. Esto es particularmente relevante para las empresas de ciberseguridad, ya que demuestra su compromiso con la seguridad.

6.1.3. INTEGRACIÓN DE LA NORMA NTC/ISO 9001:2015 Y LA NTC-ISO/IEC 27001:2022

Según el tipo de producto o servicio que ofrecerán, las empresas seleccionan uno o varios sistemas de gestión que se ajustan a sus necesidades, con el fin de mejorar la experiencia del cliente y fortalecer sus procesos internos.

Al considerar la intención de las organizaciones en obtener las certificaciones en sistemas de gestión, las empresas se enfrentan a diversas dudas e inquietudes que pueden afectar su proceso de toma de decisiones. Esta decisión es crucial, ya que influirá en la inversión de tiempo, dinero, personal y recursos necesarios para alcanzar el objetivo. La implementación de este proyecto implicará un cambio en la cultura organizacional y también traerá consigo una mayor competitividad al obtener las certificaciones, la empresa mejorará su posicionamiento, credibilidad e imagen corporativa en el mercado.

Lo más importante de saber es que si una compañía ya tiene implementado un sistema de gestión como la NTC ISO 9001:2015 en calidad y desea certificarse en otra, o sencillamente es su objetivo diseñar e implementar dos normas para la obtención de sus certificaciones, lo mejor será llevar a cabo la integración de los sistemas, ya que esto representará menos impacto e inversión para todos los procesos de la organización.

Mantener un sistema de gestión certificado de manera independiente resulta en realizar actividades de manera duplicada, dificultad para cumplir los objetivos, desgaste del personal en cumplimiento de actividades, incremento de costos, fracasos internos, baja eficiencia y por ende menos productividad.

A esta conclusión llegaron varios autores en distinta literatura consultada, sobre los diferentes beneficios que conlleva la integración.

Tabla 1 Principales beneficios en la implementación de un SIG

Gestión	Costos	Trabajadores
Impacto en la sostenibilidad organizacional	Reducción de costos de gestión	Mejora la coordinación de los equipos
Aumento en la capacidad para tomar decisiones estratégicas	Disminución de costos de auditorías y certificación	Mejora la motivación del personal y el trabajo en equipo
Disminución en la duplicidad de funciones	Optimización de costos de certificación	Agilidad en la comunicación interna y externa
Facilidad de adaptación a estándares globales	Reducción de papeleo	
Mayor eficiencia		
Claridad en las responsabilidades		
Eficiencia en el enfoque basado en procesos		
Integración de requisitos, auditorías integradas		
Alineación entre objetivos, procesos y recursos		

Nota. Información tomada del artículo “Metodología para la integración de sistemas de gestión: revisión de literatura”, 2023.

Compatibilidad entre la NTC/ISO 9001 y la NTC-ISO/IEC 27001:2022

Adicionalmente, consciente de las complejidades operativas para integrar diversos esquemas de gestión, la ISO/IEC introdujo en 2012 la Estructura de Alto Nivel (*High Level Structure - HLS*) a través del Anexo SL de sus Directivas. Este marco estableció requisitos, términos y una arquitectura común de diez capítulos para simplificar la alineación normativa. Posteriormente, en mayo de 2021, la norma fue actualizada para oficializar el concepto como **Estructura Armonizada** (*Harmonized Structure - HS*), optimizando el texto base y facilitando el cumplimiento simultáneo de estándares como la ISO 9001:2015 y la ISO/IEC 27001:2022.

A continuación, se muestran los diversos capítulos que componen esa estructura armonizada y que se encuentran en cualquier norma ISO:

- Numeral 1: Alcance: Alcance de la norma a implementar
- Numeral 2: Referencias normativas: En esta se explica la especificación de la norma a implementar y se definen los objetivos
- Numeral 3: Términos y definiciones: Indica las definiciones generales y cualquier otro termino específico de la norma a implementar
- Numeral 4: Contexto de la organización: Comprensión de los asuntos internos y externos, las necesidades y expectativas de las partes interesadas relevantes.
- Numeral 5: Liderazgo: Responsabilidad y compromiso de la alta dirección, políticas, funciones organizacionales, roles, responsabilidades y autoridades.
- Numeral 6: Planificación: medidas para gestionar riesgos y oportunidades, objetivos de calidad y planes para lograrlos. La gestión de riesgos desde cada uno de los enfoques de la ISO estaría enfocada una hacia la calidad del producto o servicio, mientras que por el otro lado se revisan los riesgos durante la identificación, análisis y reducción de los riesgos respecto a la confidencialidad, integridad y disponibilidad de la información en las organizaciones.
- Numeral 7: Apoyo: recursos necesarios, competencia, concientizar, comunicación e información documentada
- Numeral 8: Operaciones: planificación operativa y gobernanza
- Numeral 9: Evaluación del desempeño: seguimiento, medición, análisis y evaluación, auditoría interna, revisión por la dirección
- Numeral 10: Mejora: Tanto NTC ISO 9001 como NTC-ISO/IEC 27001 promueven la mejora continua como un principio central, en NTC ISO 9001, la mejora continua asegura la satisfacción del cliente y optimización de procesos mediante auditorías y revisiones periódicas. En NTC-ISO/IEC 27001, implica una constante adaptación a nuevos riesgos de seguridad. No conformidad, acción correctiva y mejora continua.

Por lo anterior y en razón a que el propósito es poder asesorar la empresa BERRUIT SAS, se ha decidido dar inicio al diseño e implementación de las normas NTC ISO 9001:2015 e NTC-ISO/IEC 27001:2022 dentro de la compañía.

En la tabla 2 se representa la correlación de los requisitos de las normas para facilitar la integración:

Tabla 2 Correlación requisitos normas NTC/ISO 9001:2015 y la NTC-ISO/IEC 27001:2022

Aspecto	ISO 9001:2015 (Numeral)	ISO 9001:2015	ISO/IEC 27001:2022 2 (Numeral)	ISO/IEC 27001:2022
Contexto	4	Enfoque en partes interesadas y procesos del negocio	4	Enfoque en requisitos de seguridad y legalidad.
Política y objetivos	5.2, 6.2	Política de calidad y objetivos de calidad	5.2, 6.2	Política de seguridad de la información y objetivos de seguridad
Liderazgo y compromiso	5.1	Compromiso del liderazgo con el sistema de gestión de calidad	5.1	Compromiso del liderazgo con la seguridad de la información
Enfoque basado en el riesgo	6.1	Identificación de riesgos que afectan la calidad del producto o servicio	6.1.2	Identificación de riesgos que afectan la seguridad de la información
Competencias, formación y toma de conciencia	7.2, 7.3	Competencias relacionadas con la calidad	7.2, 7.3	Competencias relacionadas con la seguridad de la información
Gestión de documentos y registros	7.5	Control de documentos y registros que garantizan la calidad	7.5	Control de documentos y registros relacionados con la seguridad de la información
Operación	8	Control de la producción y prestación del servicio.	8	Valoración y tratamiento de riesgos de seguridad.
Gestión de proveedores	8.4	Evaluación de proveedores en base a la calidad del producto/servicio	8.1	Evaluación de proveedores en base a la seguridad de la información
Auditorías internas	9.2	Auditorías internas del sistema de gestión de calidad	9.2	Auditorías internas del sistema de gestión de seguridad de la información

Control de no conformidades y acciones correctivas	10.2	Gestión de no conformidades que afectan la calidad	10.1	Gestión de no conformidades que afectan la seguridad de la información
Mejora continua	10.3	Mejora de productos y servicios	10.2	Mejora de controles y respuestas ante riesgos de seguridad

Fuente: Elaboración propia con base en la información de las normas NTC/ISO 9001 y la NTC-ISO/IEC 27001:2022

6.1.4. Metodologías de Integración

Con el fin de ofrecer la integración de los sistemas, se ha realizado una investigación de las diferentes metodologías existentes que pueden utilizarse para realizar un exitoso proceso de integración y escoger la adecuada para aplicación dentro de la compañía Berruit SAS, optimizando los procesos y mejorando la eficacia actual de la empresa.

Varias entidades de certificación de carácter nacional han realizado propuestas metodológicas de aplicación de normas, que es preciso conocer en el momento de realizar un proyecto de integración (Cabrera et al. 2015), a continuación, se muestran las más comunes:

6.1.5. Norma Española (AENOR) UNE 66177:2005 “Guía para la integración de sistemas de gestión”

La aplicación de UNE 66177:2005, permite disponer de una serie de herramientas, métodos, ejemplos y notas, dirigida especialmente a desarrollar, implantar y evaluar el proceso de integración de los sistemas de gestión de la calidad, gestión ambiental y gestión de la seguridad y salud en el trabajo, no pretende eliminar reemplazar las normas sino ayudar a las organizaciones a abordar la implementación integrada de dichos sistemas, con el objetivo de desarrollar una visión compartida de la organización y, en consecuencia, a mejorar la eficacia y rentabilidad del negocio (AENOR, 2005).

Introduce el principio de la gestión por procesos como base para la integración:

- Las características del producto o servicio y la satisfacción de los clientes.
- Los aspectos medioambientales que se generan.
- Los riesgos laborales a los que están expuestos los trabajadores.

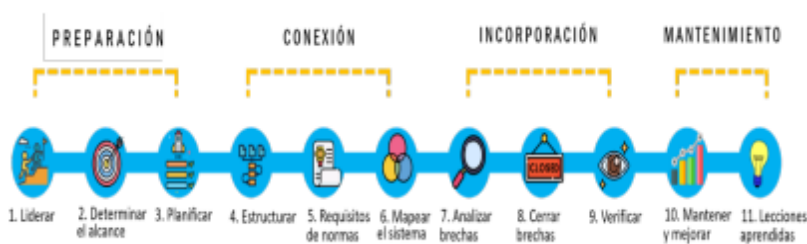
La guía se basa en el ciclo PDCA, presente en todos los estándares de sistemas de gestión, y presenta las siguientes fases para la integración (Fernández et al. 2024):

- Análisis del contexto
- Selección del método de integración
- Elaboración del plan de integración
- Apoyo de la alta dirección
- Implantación del plan de integración
- Revisión y mejora del sistema integrado de gestión

6.1.6. Uso integrado de estándares de sistemas de gestión (IUMSS)

También conocido como “Handbook”, esta guía fue publicada por primera vez en el año 2008 por la ISO y posteriormente, en el año 2018 tuvo su primera actualización. El manual Handbook o manual IUMSS, la figura No. 9 evidencia que está organizado por capítulos, los dos primeros, hacen referencia a generalidades y requisitos de los sistemas de gestión; mientras el tercero, presenta la guía como tal distribuida en cuatro etapas: Preparar, conectar, incorporar y mantener (Moreno et al., 2021).

Figura 9 Metodología “Handbook”



Nota. Información tomada del artículo Integración de Sistemas mediante Metodología de “Uso Integrado de Estándares de Gestión”, Fernández et al. (2024)

La metodología Handbook ISO es una herramienta robusta orientada a la disminución del exceso de redundancias y al cierre de brechas entre los requisitos de las normas ISO integradas y los procesos de una organización; sin embargo, en la actualidad es poco conocida (Moreno et al, 2021).

6.1.7. PAS 99:2012 de BSI (British Standards Institution)

PAS 99 es una Especificación elaborada por British Standards Institution (Institución Británica de Normalización – BSI). Esta norma ha sido principalmente pensada para ser utilizada por aquellas organizaciones que disponen o están implementando los requisitos de varias normas del sistema de gestión. La primera versión de PAS 99 fue publicada en 2006 y posteriormente fue actualizada en 2012 para alinearse con la Estructura de Alto Nivel (High Level Structure, HLS) establecida en el Anexo SL de ISO, la cual proporciona una estructura común para las normas de sistemas de gestión. Esta alineación facilita la integración de diversos estándares y promueve una gestión más eficiente de los procesos organizacionales.

Las características generales de PAS 99 son las siguientes:

- Es una especificación de requisitos para sistemas integrados de gestión. Por lo tanto, es auditable si una organización cumple dichos requisitos y, por lo tanto, certificable.
- Considera siete requisitos comunes para los sistemas de gestión identificados en el Anexo SL publicado por la ISO, dicha estructura es la siguiente:
 - Contexto de la organización.
 - Liderazgo.
 - Planificación.
 - Soporte.
 - Operación.
 - Evaluación del desempeño.
 - Mejora.
- Incluye el modelo PDCA utilizado en la mayoría de las normas de sistemas de gestión.
- Ayuda a que organizaciones con más de un sistema de gestión, se puedan enfocar de modo que sus operaciones de forma más eficaz (Mirallas, 2018)

Con base en lo expuesto, la metodología seleccionada para la presente propuesta de integración es PAS 99:2012, debido a que proporciona un marco de referencia para la integración

de múltiples sistemas de gestión dentro de una misma organización. Esta especificación fue actualizada para alinearse con la Estructura de Alto Nivel definida en el Anexo SL de ISO, conocida actualmente como la estructura armonizada de los sistemas de gestión, lo que facilita la integración de requisitos comunes entre normas como ISO 9001:2015 e ISO/IEC 27001:2022. Asimismo, su enfoque basado en el ciclo PHVA (Planificar, Hacer, Verificar y Actuar) permite identificar, estandarizar y gestionar procesos de manera integrada, contribuyendo a una implementación más eficiente, coherente y orientada a la mejora continua.

Tabla 3 Integración de Sistemas de Gestión Mediante PASS 99 – 2012

CICLO PDCA	ESTRUCTURA PASS 99	ESTRUCTURA ARMONIZADA ISO
Planear	Contexto	Capítulo 4
	Liderazgo	Capítulo 5
	Planificación	Capítulo 6
	Soporte	Capítulo 7
Hacer	Operación	Capítulo 8
Verificar	Evaluación del desempeño	Capítulo 9
Actuar	Mejora	Capítulo 10

Nota. Información tomada de Integración de Sistemas de Gestión Mediante PASS 99 – 2012. (s.f.)

Retos y consideraciones de la implementación

La integración de las normas NTC ISO 9001 (calidad) e NTC-ISO/IEC 27001 (seguridad de la información) presenta varios retos para la empresa, dependiendo de su tamaño, el compromiso de la gerencia, la cultura organizacional hacia el cambio y los recursos disponibles. A continuación, se describen algunos de los principales desafíos y consideraciones que deben abordarse de manera planificada para asegurar el éxito de la integración:

- Compromiso de la Alta Dirección

El éxito en la implementación de un Sistema de Gestión Integrado no depende exclusivamente de la asignación de recursos económicos y técnicos, sino del liderazgo genuino ejercido por la alta dirección (Karapetrovic & Willborn, 1998). De acuerdo con el numeral 5 de las normas ISO 9001:2015 e ISO/IEC 27001:2022, la dirección debe asumir la responsabilidad de planificar, supervisar y evaluar la eficacia de las directrices estratégicas del sistema. Asimismo,

Whitman y Mattord (2018) enfatizan que el involucramiento activo de la gerencia actúa como un catalizador ejemplarizante, promoviendo la transformación de la cultura organizacional hacia la seguridad de la información y la mejora continua.

- Resistencia al Cambio Cultural

Uno de los principales desafíos estratégicos radica en comunicar efectivamente a los colaboradores los objetivos de la integración normativa, evitando que el proceso sea percibido como una sobrecarga operativa o una duplicidad de funciones. De acuerdo con el numeral 7.3 (Toma de conciencia) de las normas ISO 9001:2015 e ISO/IEC 27001:2022, la organización debe asegurar que el personal comprenda la importancia de su contribución a la eficacia del sistema. En este contexto, el liderazgo de la alta dirección y de los jefes de área resulta determinante para modelar la cultura organizacional y consolidar un compromiso transversal con el sistema de gestión integrado.

- Recursos Disponibles

Antes de iniciar la fase de implementación, la organización debe verificar la disponibilidad y suficiencia de los recursos necesarios para el establecimiento, mantenimiento y mejora del sistema integrado, en cumplimiento del numeral 7.1 de los estándares ISO.

En la Tabla 4 se consolidan las tipologías de recursos requeridos para sostener la estructura del sistema de gestión integrado.

Tabla 4 Clasificación de recursos requeridos para la integración

Recursos humanos:	Personal con tiempo y dedicación para el diseño y mantenimiento del sistema.
Recursos tecnológicos	Herramientas para capacitaciones, reuniones y documentación que soporte la integración.
Recursos económicos	Inversión en infraestructura, consultoría y personal directo, además de los costos asociados a las certificaciones y auditorías requeridas

Nota. Elaboración propia, información basada en las exigencias del numeral 7.1 de las normas ISO

- Formación y Entrenamiento

Para garantizar la sostenibilidad del sistema y evitar vulnerabilidades operativas o brechas de seguridad, es indispensable establecer mecanismos eficaces de transferencia del conocimiento (ISO/IEC, 2022). La alta dirección debe garantizar programas de capacitación continua que permitan al personal desarrollar las competencias necesarias (numeral 7.2 de las normas ISO), comprender el impacto de sus actividades en el desempeño global y aplicar con rigor los procedimientos operativos y de seguridad establecidos.

- Gestión Documental

La definición previa de los mecanismos para la identificación, almacenamiento, protección y disposición de la información documentada representa un factor crítico de éxito, según lo reglamenta el numeral 7.5 de los estándares internacionales integrados. La adopción de herramientas tecnológicas para la gestión documental optimiza los flujos de trabajo, reduce la carga operativa, previene el uso de versiones obsoletas y asegura la trazabilidad necesaria durante los procesos de auditoría.

- Enfoque en la Mejora Continua

El compromiso con la mejora continua (numeral 10 de ISO 9001 e ISO/IEC 27001) impide que la organización limite su actuación al cumplimiento de requisitos mínimos o estáticos. El sistema integrado debe concebirse como un marco dinámico capaz de adaptarse proactivamente a las transformaciones del contexto interno y externo, garantizando la resiliencia operativa, la satisfacción del cliente y la protección de los activos de información a largo plazo.

Para concluir, implementar un sistema de gestión requiere una planificación cuidadosa y una gestión eficiente de los recursos. Si se abordan adecuadamente los principios, retos y aspectos fundamentales de las normas ISO 9001:2015 e ISO/IEC 27001:2022, la empresa podrá lograr una integración exitosa que fortalezca su posición competitiva y optimice sus procesos internos. Esta integración permitirá, además, mantener y mejorar continuamente el sistema, aportando un valor real y sostenible a la organización.

6.2. Marco normativo

Este marco normativo representado en la tabla 3, reúne las principales regulaciones y estándares que respaldan el diseño e implementación de un Sistema Integrado de Gestión (SIG) basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022 en la compañía Berruit SAS. A lo largo de este capítulo, se presenta el contexto legal y normativo que sustenta su aplicación en la compañía, garantizando el cumplimiento de los requisitos establecidos y reforzando la confianza de clientes y socios al demostrar un compromiso sólido con la calidad y la seguridad de la información.

Tabla 5 Normatividad asociada al Diseño e implementación de un Sistema integrado de Gestión basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022 en Berruit SAS

NORMA	DESCRIPCIÓN	FECHA DE RATIFICACIÓN
NTC-ISO 9001:2015	Sistemas de gestión de la calidad. Requisitos.	23/09/2015
IEC-ISO/IEC 27001:2022	Requisitos de la seguridad de la información, la ciberseguridad y la protección. Sistemas de gestión de seguridad de la información.	09/11/2022
Ley 1581 de 2012 Reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y el Decreto 1081 de 2015.	Por la cual se dictan disposiciones generales para la protección de datos personales.	Publicada en el Diario Oficial 48587 de octubre 18 de 2012
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.	Publicada en el Diario Oficial 47.223 de enero 5 de 2009.
Ley 527 de 1999 Desarrollado por el Decreto 4487 de 2009 - Reglamentado parcialmente por el Decreto 1747 de 2000.	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones	Publicado en el Diario Oficial No, 43.673, 21 de agosto de 1999
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones ?TIC?, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones	Publicado en el Diario Oficial 47426 de julio 30 de 2009.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.	Publicado en el Diario Oficial 48622 de noviembre 22 de 2012.
Decreto 338 de 2022	Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015,	08/03/2022

	Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones	
CONPES 3854	Política Nacional de Seguridad Digital	11/04/2016
CONPES 4144	Política Nacional de Inteligencia Artificial	14/02/2025

Nota: Elaboración propia a partir de ISO 9001:2015, ISO/IEC 27001:2022, Ley 1581 de 2012, Ley 1273 de 2009, Ley 527 de 1999, Ley 1341 de 2009, Decreto 2364 de 2012, Decreto 338 de 2022, CONPES 3854 de 2016 y CONPES 4144 de 2025.

7. Fases o etapas del plan de intervención

El plan de intervención para el diseño e implementación del Sistema Integrado de Gestión (SIG) en Berruit SAS se estructuró en cuatro fases secuenciales y articuladas, alineadas con el ciclo PHVA (Planear–Hacer–Verificar–Actuar) y con los requisitos establecidos en la NTC-ISO 9001:2015 y la ISO/IEC 27001:2022, tal como se evidencia en la figura No. 10.

Cada fase contempla un propósito definido, actividades específicas, productos entregables y conclusión sobre el ejercicio realizado.

Figura 10 Diagrama implementación del SIG en Berruit S.A.S



Nota. Fuente: Elaboración propia.

Fase 1. Diagnóstico organizacional y análisis de brechas

- Propósito**

Determinar el estado actual de Berruit SAS frente a los requisitos normativos de calidad y seguridad de la información, identificando fortalezas, debilidades y brechas de cumplimiento.

- Descripción metodológica**

Se realiza una revisión documental, entrevistas semiestructuradas con la dirección general y la dirección administrativa, personas encargadas del proceso de integración de las normas al interior de la compañía, análisis de las actividades realizadas, ya que no cuenta con los procesos

estructurados. Posteriormente, se diseña y se aplica una matriz de evaluación comparativa frente a los numerales aplicables de ambas normas.

- **Actividades planeadas**

- Reunión de apertura con la alta dirección
- Revisión documental preliminar
- Entrevistas semiestructuradas, observación directa de actividades operativas
- Identificación preliminar de procesos existentes (no formalizados)
- Identificación inicial de riesgos organizacionales y de información
- Evaluación del nivel de cumplimiento normativo.
- Elaboración de matriz de brechas.

- **Producto entregable**

Informe de diagnóstico y matriz de análisis de brechas.

- **Relación con objetivos específicos**

Desarrollar la herramienta de diagnóstico y analizar la situación actual para la construcción de la línea base del Sistema integrado de gestión.

- **Fase del ciclo PHVA**

Diagnóstico

Fase 2. Construcción plan de trabajo

- **Propósito**

Diseñar el plan estructurado de intervención para la implementación del Sistema Integrado de Gestión en Berruit SAS, estableciendo actividades, responsables, recursos, tiempos y entregables necesarios para el desarrollo progresivo del proyecto.

- **Descripción metodológica**

Con base en los resultados obtenidos en la fase de diagnóstico, se procede a estructurar el plan de trabajo que orienta el diseño e implementación del Sistema Integrado de Gestión.

Esta fase tiene un carácter estratégico y de planificación, permitiendo traducir las brechas identificadas en acciones concretas organizadas en fases secuenciales. Se establece una programación detallada que garantiza coherencia metodológica, viabilidad operativa y alineación con los objetivos del trabajo de grado.

El plan de trabajo se diseña bajo el enfoque de PHVA y la estructura armonizada, incorporando criterios de priorización, asignación de responsabilidades y definición de productos verificables.

- **Actividades planeadas**

- Revisión y clasificación de brechas identificadas.
- Priorización de necesidades de intervención.
- Definición de alcance del proyecto SIG
- Determinación de procesos incluidos.

- **Estructuración de fases de intervención por numerales y PHVA**

- Organización de actividades por etapas.
- Secuenciación lógica del proceso de implementación.
- Identificación de productos esperados por actividad.

- **Asignación de responsables y roles**

- Identificación de responsables internos.
- Definición de participación de la alta dirección.

- **Estimación de tiempos y cronograma**

- Elaboración del cronograma general del proyecto.

- **Identificación de recursos necesarios**

- Recursos humanos.
- Recursos tecnológicos.
- Recursos documentales y administrativos.
- Recursos económicos

- **Definición de criterios de seguimiento y control**

- Establecimiento de indicadores de avance del proyecto.

- **Producto entregable**

Plan de trabajo estructurado del Sistema Integrado de Gestión, representado en un cronograma del proyecto de consultoría

- **Relación con objetivos específicos**

Diseñar el plan de trabajo identificando los procesos clave y sus interacciones para cumplir los requisitos del sistema de gestión integrado.

- **Fase del ciclo PHVA**

Planificación

Fase 3 Diseño y estructuración del Sistema Integrado de Gestión

- **Propósito**

Diseñar la estructura documental del sistema integrado de gestión que da cumplimiento a los requisitos de las normas, asegurando su integración y la alineación con la organización.

Descripción metodológica

Una vez definido el plan de trabajo, se procede a realizar el diseño del sistema integrado de gestión bajo el enfoque de la estructura armonizada (HLS), integrando los numerales y contribuyendo a evitar duplicidad de la documentación.

Se adopta el enfoque de gestión por procesos y gestión del riesgo como ejes transversales en la implementación.

- **Actividades desarrolladas**

- Diseño del mapa de procesos (estratégicos, misionales y de apoyo).
- Caracterización de procesos y definición de interacciones.
- Definición del alcance del SIG documentado.
- Formulación de la política integrada (calidad y seguridad de la información).
- Definición de objetivos del SIG y sus indicadores.
- Identificación y análisis de riesgos (calidad y seguridad de la información).
- Elaboración de la matriz de riesgos y plan de tratamiento.
- Diseño de procedimientos obligatorios y operativos.
- Elaboración de formatos, registros y controles documentales.
- Definición de controles de seguridad de la información aplicables al contexto organizacional.
- Definición de indicadores de desempeño.

- **Producto entregable**

- Mapa de procesos.
- Política integrada.
- Objetivos e indicadores del SIG.
- Matriz de riesgos y plan de tratamiento.
- Procedimientos y formatos del sistema y del cumplimiento Anexo de la ISO/IEC 27001:2022

- **Relación con objetivos específicos**

- Ejecutar el plan de intervención integrado desde el análisis del contexto organizacional hasta el control operacional.

- **Fase del ciclo PHVA**

Hacer.

Fase 4. Implementación del Sistema integrado de gestión

- **Propósito**

Poner en marcha el sistema integrado de gestión diseñado, asegurando su apropiación y su aplicabilidad dentro de la operación de Berruit S.A.S.

- **Descripción metodológica**

En esta fase se realiza la socialización, capacitación e implementación progresiva de los procedimientos, controles y herramientas diseñadas.

La implementación se desarrolla paralelamente al diseño de los documentos y controles, debido a que los mismos responsables participan en la construcción del diseño, permitiendo su implementación oportuna y conforme a lo establecido en el cronograma del plan de trabajo.

- **Actividades desarrolladas**

- Socialización del SIG a la alta dirección y colaboradores.
 - Implementación de procedimientos y formatos diseñados.
 - Aplicación del control documental.
 - Puesta en marcha de los controles de seguridad de la información.
 - Ejecución del plan de trabajo

- Generación de registros del sistema.

- **Producto entregable**

- Sistema implementado en operación.
- Registros de aplicación de procedimientos.
- Evidencias de socialización.

- **Relación con objetivos específicos**

Implementar el Sistema Integrado de Gestión en los procesos estratégicos, misionales y de apoyo de la organización.

- **Fase del ciclo PHVA**

Hacer.

7.1. Conformación del equipo de consultoría

El equipo de consultoría encargado del diseño e implementación del Sistema Integrado de Gestión en Berruit SAS esta conformado por dos profesionales con competencias complementarias en gestión organizacional, calidad y seguridad de la información. El diseño e implementación del Sistema Integrado de Gestión en Berruit SAS se desarrolla mediante un esquema de intervención colaborativa, conformado por una consultora líder externa y el equipo directivo interno de la organización y la gerencia general.

La conformación del equipo permite garantizar un enfoque técnico integral, asegurando el abordaje estratégico, documental y operativo requerido para la implementación del sistema conforme a la NTC-ISO 9001:2015 y la ISO/IEC 27001:2022.

7.2. Cronograma

A continuación, en la figura No. 11 se presenta el plan de trabajo, de acuerdo con las etapas y actividades planteadas en el numeral 6.1, especificando las fechas, responsables, recursos, entregables y los riesgos en caso de no ejecutar cada etapa. *(Ver anexo B)*

Figura 11 Cronograma de trabajo

ALCANCE	ALCANCE DEL TRABAJO DE GRADO																													
ETAPA PRIVA	PLANEAR											HACER																		
TIEMPO	MES 1		MES 2		MES 3		MES 4		MES 5		MES 6		MES 7		MES 8		MES 9		MES 10		MES 11									
TRUCTURA DE ALTO NIVEL	Clausa 4	Clausa 4	Clausa 4	Clausa 4	Matriz de riesgos	Matriz de riesgos	Matriz de riesgos	Clausa 5	Clausa 5	Clausa 6	Clausa 7	Clausa 7	Clausa 8	Clausa 8	Clausa 8	Clausa 8	Clausa 8	Anexo A	Anexo A	Anexo A	Anexo A	Anexo A								
	Contexto	Planificación y Proceso		Claro contexto y Proceso	Función	Función	Función	Liderazgo Plan 1	Liderazgo Plan 1	Liderazgo Plan 2	Objetivos y Indicadores	Compentencias y recursos	Documentación y comunicación	Operación ISO 9001	Operación ISO 9001	Operación ISO 27001	Operación ISO 27001	Control organizacional y balance	Control organizacional y balance	Control organizacional y balance	Control organizacional y balance	Control organizacional y balance								
OBJETIVO	Comprender el entorno estratégico.		Completar elementos base del SGI.		Dejar todo completado en el manual 4.		Consolidación y normalización de todos los riesgos.		Validación y definición de todos los riesgos.		Controlar el plan de tratamiento y control de riesgos.		Institucionalizar el liderazgo del SGI.		Formular roles, responsabilidades y comunicaciones.		Alinear el SGI al enfoque de desempeño.		Crear la base de soporte humano.		Implementar la infraestructura documental.		Corregir operativamente los 7 procesos.		Asegurar la operación TI de seguridad.		Implementar A.5 y A.6.		Finalizar controles esenciales.	
ACTIVIDADES																														

Nota. Fuente: Elaboración propia

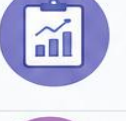
7.3. Instrumentos y técnicas para la toma de información y para la presentación de resultados

Para el desarrollo del presente trabajo de grado, orientado al diseño e implementación de un Sistema Integrado de Gestión basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022 en Berruit SAS, se emplea diferentes instrumentos y técnicas de recolección, análisis y presentación de información, los cuales permiten obtener datos relevantes sobre el estado actual de la organización, identificar brechas frente a los requisitos normativos y estructurar las acciones necesarias para la implementación del sistema.

Debido a que el proyecto corresponde a un proceso de intervención organizacional aplicado, se utilizan principalmente técnicas cualitativas y herramientas de análisis.

A continuación, en la figura 12 se describen los principales instrumentos y técnicas utilizados:

Figura 12 Principales instrumentos y técnicas utilizados

INSTRUMENTO / TÉCNICA	DESCRIPCIÓN	PROPÓSITO / APORTES
 Revisión documental	Revisión de la documentación en la organización, incluyendo documentos administrativos, información estratégica, registros operativos y documentos relacionados con la gestión organizacional. Esta revisión permitió identificar el estado inicial de los procesos, los elementos estratégicos de la empresa y la información disponible para la construcción del Sistema Integrado de Gestión.	 Conocer el estado inicial de los procesos y los elementos estratégicos de la organización, identificando la información disponible para la construcción del sistema.
 Entrevistas semiestructuradas	Se aplicaron entrevistas semiestructuradas a jefes de proceso y miembros de la alta dirección para recopilar información sobre el funcionamiento de los procesos, responsabilidades, flujos de información y controles. Permitieron orientar la conversación con preguntas guía y profundizar en aspectos relevantes. La información obtenida fue insumo para la identificación de procesos, caracterización de actividades, análisis del contexto organizacional e identificación de riesgos.	 Recopilar información clave sobre los procesos, roles, controles y riesgos para la estructuración del sistema de gestión.
 Observación directa	Se realizó observación directa de algunas actividades operativas y administrativas de la organización, lo que permitió comprender la dinámica real de los procesos y contrastar la información obtenida mediante las entrevistas y la revisión documental.	 Comprender la dinámica real de los procesos y validar la información recolectada por otros medios.
 Herramientas de análisis organizacional	Se emplearon herramientas estratégicas como el análisis PESTAL, la matriz DOFA y la identificación de factores internos y externos, las cuales permitieron comprender el entorno de la organización y establecer los elementos estratégicos necesarios para la estructuración del Sistema Integrado de Gestión.	 Analizar el contexto interno y externo de la organización y definir elementos estratégicos para el sistema.
 Herramientas de gestión de procesos	Para la estructuración del sistema bajo el enfoque de gestión por procesos se utilizaron instrumentos como el mapa de procesos, las caracterizaciones de procesos y el análisis de interacciones entre procesos, lo que permitió definir la estructura organizacional del sistema de gestión.	 Definir la estructura del sistema de gestión y comprender la interacción entre los procesos de la organización.
 Matriz de análisis de brechas	Se diseñó y aplicó una matriz de evaluación comparativa con base en los requisitos establecidos en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022, con el fin de identificar el nivel de cumplimiento de la organización frente a dichos estándares. Esta herramienta permitió determinar las brechas existentes y establecer la línea base para la implementación del Sistema Integrado de Gestión.	 Identificar el nivel de cumplimiento frente a las normas y establecer las brechas y la línea base para la implementación.
 Matriz de gestión de riesgos	Para la identificación, análisis y tratamiento de riesgos se empleó una matriz de riesgos integrada, mediante la cual se evaluaron los riesgos asociados a los procesos organizacionales y a la seguridad de la información, considerando criterios de probabilidad e impacto, así como la definición de controles y planes de tratamiento.	 Evaluar y gestionar los riesgos de los procesos y de la seguridad de la información, definiendo controles y planes de tratamiento.
 Instrumentos de seguimiento y evaluación	Durante las fases de verificación y mejora del sistema se utilizaron instrumentos como indicadores de gestión y registros de seguimiento, los cuales permitieron evaluar el desempeño del sistema frente a los instrumentos creados por parte de la consultoría y validar su eficacia a través de la utilidad para la operación de los procesos.	 Evaluar el desempeño del sistema y validar la eficacia de los instrumentos implementados en la operación.
 Instrumentos para la presentación de resultados	Para la presentación de los resultados obtenidos se utilizaron diferentes instrumentos gráficos y documentales, tales como matrices de análisis, diagramas de procesos, tablas comparativas, cronogramas de implementación, los cuales facilitaron la interpretación de la información y la consolidación de los resultados del proyecto.	 Facilitar la interpretación, comunicación y consolidación de los resultados del proyecto mediante herramientas visuales y documentales.
 Resultado global: La aplicación de estos instrumentos y técnicas permitió recopilar información confiable, analizar el contexto y los procesos, identificar riesgos y brechas, y establecer las bases para la implementación, seguimiento y mejora continua del Sistema Integrado de Gestión.		

Nota. Fuente: Elaboración propia.

8. Resultados y discusión del proyecto

En este capítulo se presentan los resultados obtenidos durante el desarrollo de la consultoría para Berruit SAS respecto al diseño e implementación del Sistema Integrado de Gestión basado en las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022. Los resultados se presentan de manera estructurada conforme fueron establecidos los objetivos de este trabajo, permitiendo visualizar el proceso de intervención empresarial desarrollado y los avances alcanzados en cada una de las fases definidas para el cumplimiento de la consultoría.

Cada fase describe las actividades realizadas, los instrumentos que se utilizaron y los productos generados, permitiendo con esto comprender como fue el desarrollo de la implementación del sistema integrado de gestión dentro de Berruit SAS. Igualmente se presentan tablas, matrices, figuras u otros para permitir al lector la comprensión y evidenciar el proceso metodológico aplicado.

Por otra parte, los resultados obtenidos se analizan a la luz de los conceptos desarrollados en el marco teórico y conceptual, especialmente aquellos relacionados con la gestión por procesos, la gestión de riesgos y la integración de los requisitos establecidos en las normas ISO 9001:2015 e ISO/IEC 27001:2022.

Finalmente, este capítulo presenta los resultados derivados del desarrollo de la consultoría y evidencia su contribución al fortalecimiento organizacional de Berruit S.A.S., mediante la mejora de sus procesos internos, el fortalecimiento de la gestión de la seguridad de la información y el avance en el cumplimiento de los requisitos asociados al Sistema Integrado de Gestión.

8.1. Diagnóstico del estado inicial de Berruit SAS frente al cumplimiento de las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022

Con el propósito de determinar el nivel de cumplimiento de Berruit S.A.S. frente a los requisitos de las normas NTC ISO 9001:2015 e ISO/IEC 27001:2022, se aplica un instrumento de autodiagnóstico diseñado por el Centro Nacional de Memoria Histórica (2024, p. 15). Este

instrumento sirve como base para evaluar el estado actual de la organización y establecer una línea base para el diseño e implementación del Sistema Integrado de Gestión.

La evaluación se lleva a cabo mediante la revisión documental, la realización de entrevistas semiestructuradas con la alta dirección y los líderes de proceso, así como la verificación de las prácticas organizacionales existentes. A partir de la aplicación del instrumento, se obtiene una valoración porcentual del grado de cumplimiento de cada una de las cláusulas evaluadas, lo que permite identificar fortalezas, oportunidades de mejora y brechas frente a los requisitos de ambas normas.

El instrumento permite analizar el cumplimiento de los requisitos asociados a las cláusulas 4 a 10 de la estructura armonizada de los sistemas de gestión, así como los controles establecidos en el Anexo A de la norma ISO/IEC 27001:2022. Adicionalmente, la herramienta fue adaptada para incorporar la evaluación y calificación independiente de los requisitos de cada norma, facilitando la identificación de brechas y la formulación del plan de trabajo desarrollado durante la consultoría.

La tabla No. 6 representa los criterios de evaluación y un porcentaje de ponderación clasificado de la siguiente manera:

Tabla 6 Criterios de evaluación herramienta diagnóstica ISO9001 e ISO27001

VARIABLE DE CUMPLIMIENTO	NO APLICA	COMPLETO	PARCIAL	NINGUNO
VALOR ASIGNADO	Fuera de cálculo	1	0,5	0

Fuente: Elaboración propia

Una vez terminada la calificación del nivel de cumplimiento de cada numeral de la norma, se calcula el ponderado sumando el resultado de cada uno de los requisitos de ese numeral y dividiéndolo en el número de preguntas, para identificar un total de cumplimiento, tal como se identifica a continuación:

Tabla 7 Ejemplo de aplicación herramienta diagnóstica en Berruit SAS, numeral 5.3

5 LIDERAZGO (ISO 9001:2015)	5 LIDERAZGO (ISO 27001:2022)	ISO 9001:2015				ISO 27001:2022			
		N/A	COMPLETO	PARCIAL	NINGUNO	N/A	COMPLETO	PARCIAL	NINGUNO
5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN	5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN			14%				13%	
¿La alta dirección tiene asignada la responsabilidad y autoridad para:	La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen.			X				X	
a) Asegurarse de que el SGC es conforme con los requisitos de estas Norma Internacional;	La alta dirección debe asignar la responsabilidad y autoridad para: a) asegurarse de que el sistema de gestión de la seguridad de la información sea conforme con los requisitos de esta Norma;				X				X
b) Asegurarse de que los procesos están generando y proporcionando las salidas previstas;	b) informar a la alta dirección sobre el desempeño del sistema de gestión de la seguridad de la información.				X				X
c) Informar, en particular, a la alta dirección sobre el desempeño del sistema de gestión integrado, incluyendo el desempeño ambiental y sobre las oportunidades de mejora;	NOTA La alta dirección también puede asignar responsabilidades y autoridades para informar sobre el desempeño del sistema de gestión de la seguridad de la información dentro de la organización.				X				X
d) Asegurarse de que se promueve el enfoque al cliente en toda la organización;				X					
e) Asegurarse de que la integridad del SGC se mantiene cuando se planifican e implementan cambios en el SGC?					X				
¿La alta dirección se asegura que las responsabilidades y autoridades para los roles pertinentes se documenten, asignen, se comuniquen, se entiendan y se mantengan como información documentada en toda la organización?					X				
		0	0	2	5	0	0	1	3

Fuente: Elaboración propia.

En el ejemplo anterior de la tabla No. 7, para el cumplimiento de la ISO 9001:2015 frente al numeral 5.3, se identifica que, de un total de 7 requisitos, dos (2) requisitos se clasificaron como "parcial" y cinco (5) como "ninguno". De acuerdo con los criterios de la Tabla No. 6, esto resultó en una calificación total de uno (1) para dicha pregunta (0,5 + 0,5). Por su parte, el cumplimiento de la ISO 27001:2022, se identifica que, de los 4 requisitos aplicables, únicamente uno (1) marca como "parcial" mientras que tres (3) se clasifican en "ninguno" obteniendo una calificación final de (0,5).

Posteriormente, para obtener el porcentaje de cumplimiento, se dividió esta calificación entre el número total de requisitos de cada numeral y se multiplicó por 100. Los resultados por numeral son los siguientes:

- ISO 9001:2015 (Numeral 5.3): Con 7 requisitos, el cumplimiento es del **14%**

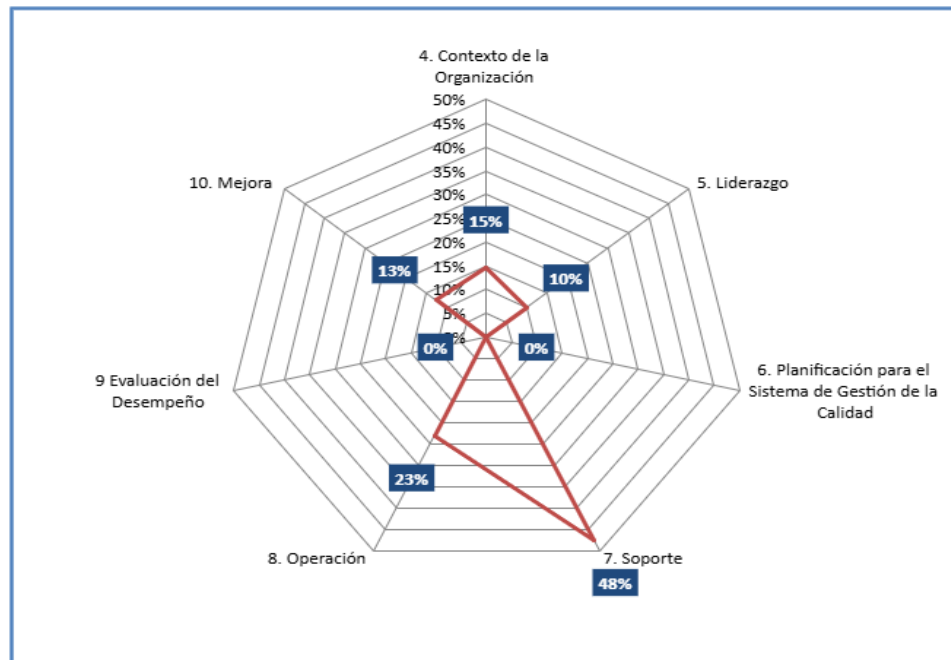
$$((1/7) * 100)$$

- ISO/IEC 27001:2022 (Numeral 5.3): Con 4 requisitos, el cumplimiento es del **12,5%** aproximándolo al **13%**.

$$((0,5/4) * 100)$$

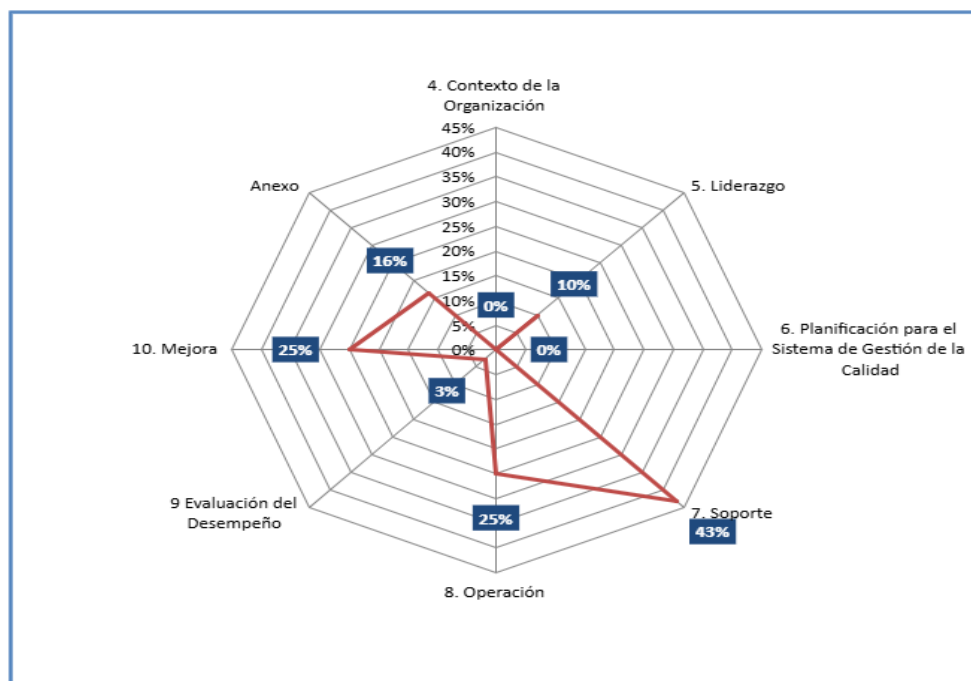
La sumatoria de cada resultado evidencia el nivel de implementación que tiene la compañía frente a cada requisito de la norma, ver figuras 13 y 14.

Figura 13 Consolidado de cumplimiento en ISO 9001:2015, diagnóstico inicial Berruit SAS



Fuente: Resultado aplicación herramienta diagnóstica del Centro de memoria Histórica.

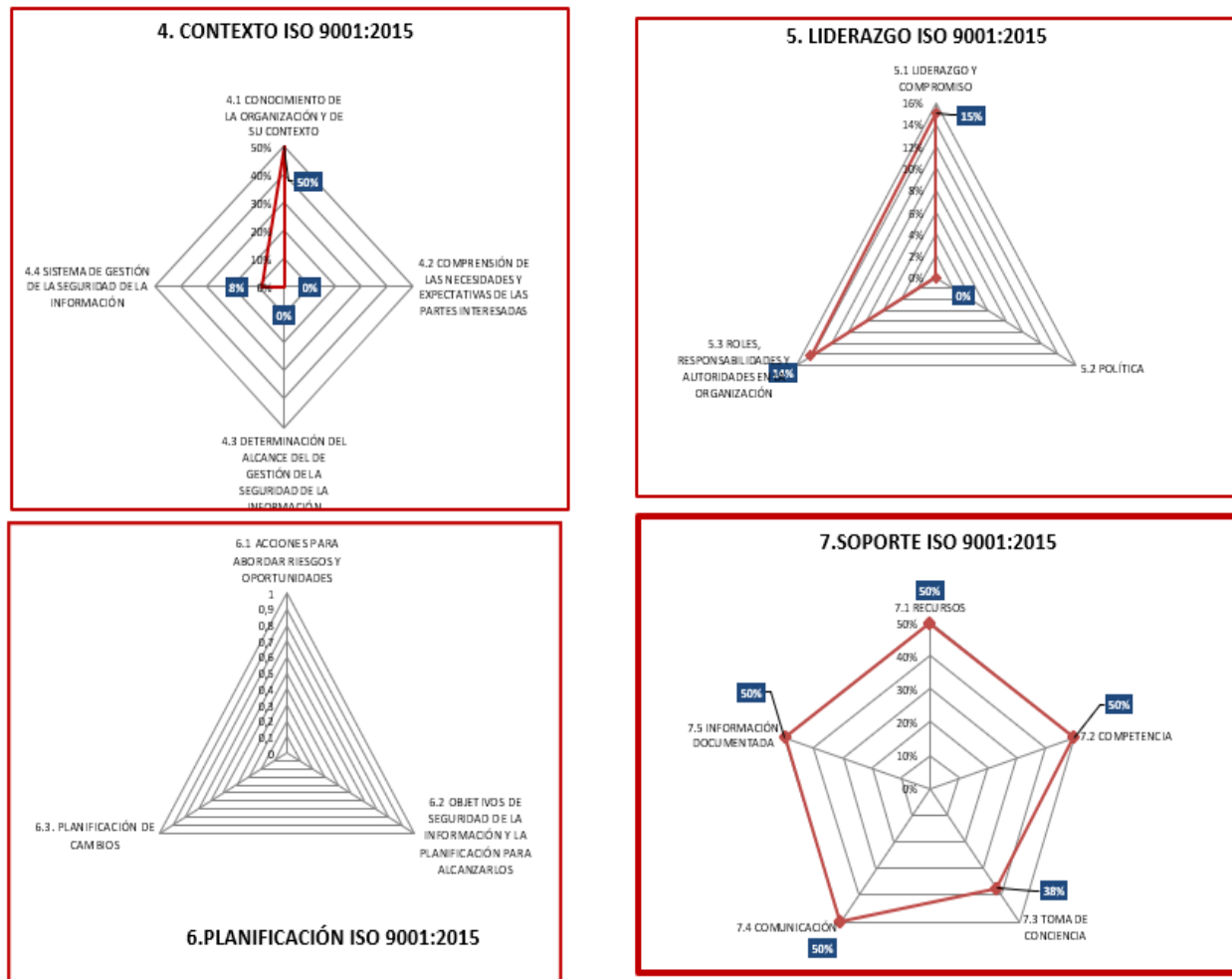
Figura 14 Consolidado de cumplimiento en ISO/IEC 27001:2022, diagnóstico inicial Berruit SAS



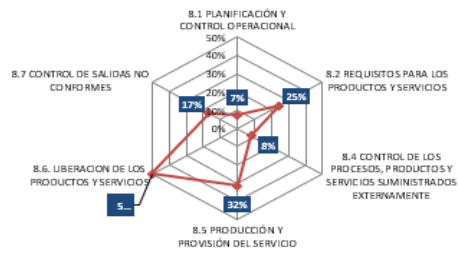
Fuente: Resultado aplicación herramienta diagnóstica del Centro de memoria Histórica.

Estos resultados indican que, aunque la organización contaba con algunas prácticas administrativas y operativas relacionadas principalmente con el soporte organizacional, no existía un sistema de gestión formalmente estructurado ni documentado que permitiera garantizar el cumplimiento de los requisitos normativos. Las figuras 16 y 17 presentan en detalle por numeral el nivel de cumplimiento identificado para cada uno de los numerales evaluados.

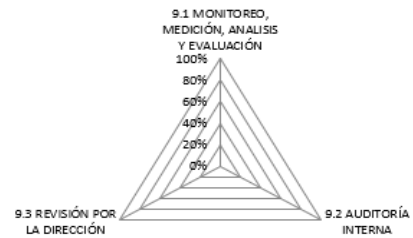
Figura 15 Resultado diagnóstico aplicado Berruit SAS ante la norma ISO 9001:2015 por capítulo.



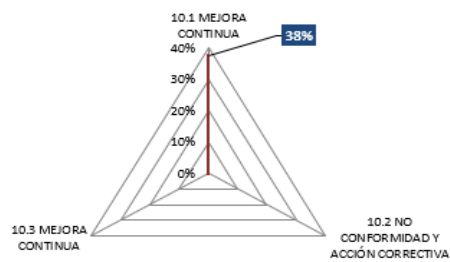
8. OPERACIÓN ISO 9001:2015



9 EVALUACIÓN DEL DESEMPEÑO ISO 9001:2015

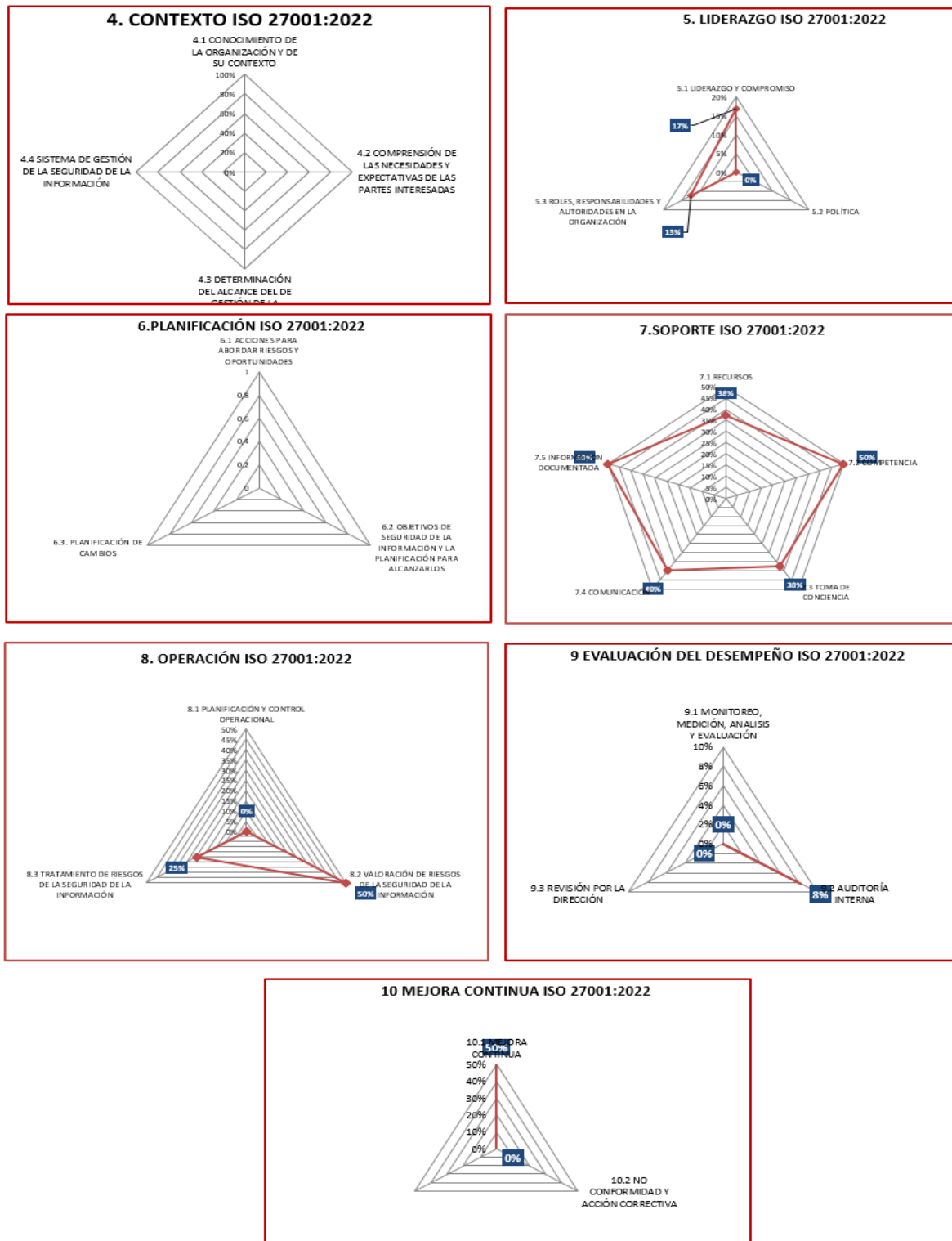


10 MEJORA CONTINUA ISO 9001:2015



Fuente: Elaboración propia.

Figura 16 Resultado diagnóstico aplicado Berruit SAS ante la norma ISO/IEC 27001:2022 por capítulo.



Fuente: Elaboración propia.

A continuación, se amplía los resultados del diagnóstico.

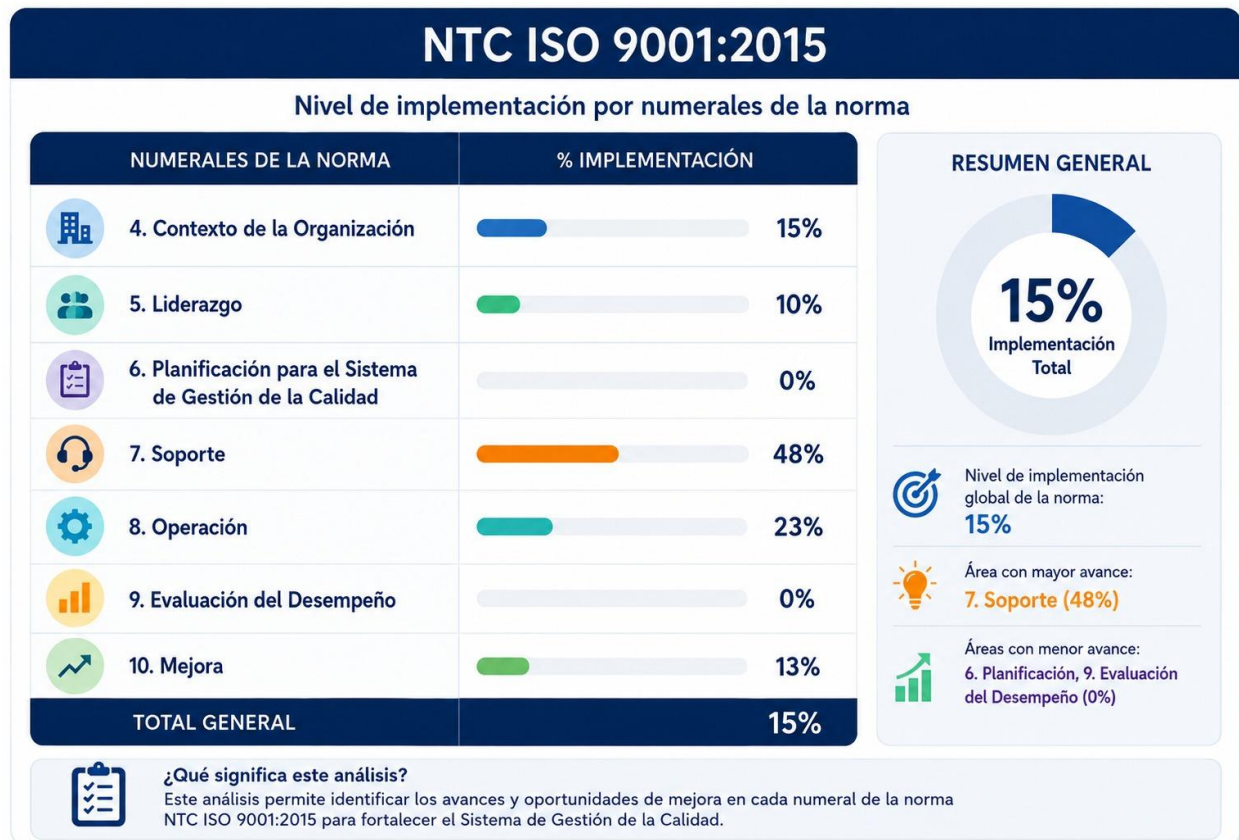
8.1.1. Análisis de los resultados del diagnóstico

Los resultados obtenidos a partir de la aplicación del instrumento de autodiagnóstico permitieron identificar el nivel inicial de madurez de la organización frente a los requisitos establecidos en las normas presentaba un nivel de implementación de 15% para la norma NTC-ISO 9001:2015, un 15% para la norma ISO/IEC 27001:2022 incluyendo el anexo A, para un total de nivel de madurez del 15% del sistema integrado de gestión. Ver herramienta diagnóstica aplicada a los requisitos de normas y el anexo A del presente trabajo (Anexo A Instrumento Autodiagnóstico SGC Y SGSI INICIAL 2024).

Respecto a los resultados frente a la norma de calidad se visualiza que en la cláusula 7 de Soporte es la que evidencia un mayor nivel de cumplimiento con un total de 48%, seguido del numeral 8 con un total de 23%, ya que contaba con asignación de recursos, manejo de la seguridad de la información claramente por ser su core del negocio, con algunos controles operacionales. Se evidenció que no cumplía con una estructura frente a un sistema de gestión y el direccionamiento hacia una política de calidad.

El numeral 5 de Liderazgo, por su parte evidenció un nivel de madurez bajo, con un cumplimiento del 10%, aunque se identificó claramente la asignación, responsabilidad y autoridad de la alta dirección y cargos directivos en la organización, no se observó una orientación hacia la gestión y compromiso con la gestión de la calidad, así como la asignación de los roles y responsabilidades frente al sistema de gestión.

En cuanto a los numerales 6 de Planificación y 9 Seguimiento al desempeño, su nivel de cumplimiento fue prácticamente nulo, siendo las brechas identificadas en la consultoría con mayor participación. Esta situación demuestra que la organización no presenta una organización de sus procesos, ni la planificación de sus objetivos de la calidad, tampoco se evidenció una gestión estructurada de la operación, el seguimiento de indicadores, auditorías internas o revisión por la dirección.

Figura 17 Nivel de madurez inicial en Berruit SAS frente norma NTC-ISO 9001:2015

Fuente: Elaboración propia

Respecto a los resultados del nivel de madurez de la empresa frente a la norma ISO/IEC 27001:2022 se evidenció que su implementación es igual frente a la de calidad, ya que arrojó un total de 15% de cumplimiento general, este resultado es atribuido a las buenas prácticas de control y gestión de la seguridad de la información por ser su expertise en el mercado tecnológico, usaban controles básicos de control de la información, uso de varias herramienta tecnológicas y algunos controles informales frente a la operación o servicio ofrecido a los clientes.

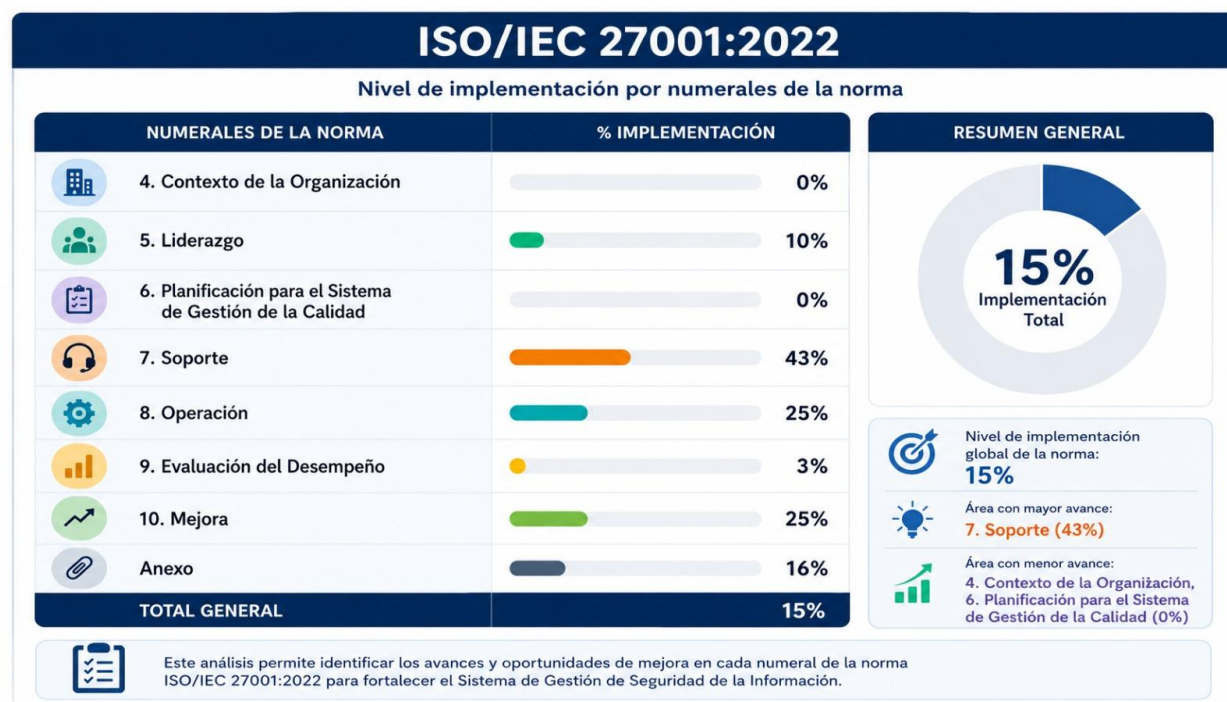
Los resultados muestran que en la cláusula 7 de Soporte alcanzó un nivel de madurez del 43% por la razón indicada anteriormente frente a las buenas prácticas de gestión de la seguridad de la información, manejo de herramientas tecnológicas de control y protección de datos, estas mismas condiciones se ven reflejadas en la cláusula 8 (operación) que arrojó un nivel de cumplimiento de 25%.

Por otro lado, y muy similar a lo reflejado con la NTC-ISO 9001:2015, las cláusulas 6 de Planificación, 9 de Seguimiento al desempeño y 10 de mejora, el nivel de madurez es muy bajo, identificando unas brechas significativas para el proceso de consultoría.

En relación con el cumplimiento del Anexo A de la ISO/IEC 27001:2022, se identificó un nivel de madurez de 16%, lo cual evidencia que la mayoría de los controles documentales, físicos, tecnológicos y humanos, no se encontraban documentados dentro de la organización.

El numeral 5 por su parte evidenció un nivel de madurez bajo con un cumplimiento del 10%, aunque se tenía muy bien definida la alta dirección y cargos directivos en la organización, no se tenía definido una orientación hacia la gestión y compromiso con la gestión de la seguridad de la información, así como la asignación de los roles y responsabilidades frente al sistema de gestión.

Figura 18 Nivel de madurez inicial en Berruit SAS frente norma ISO/IEC 27001:2022

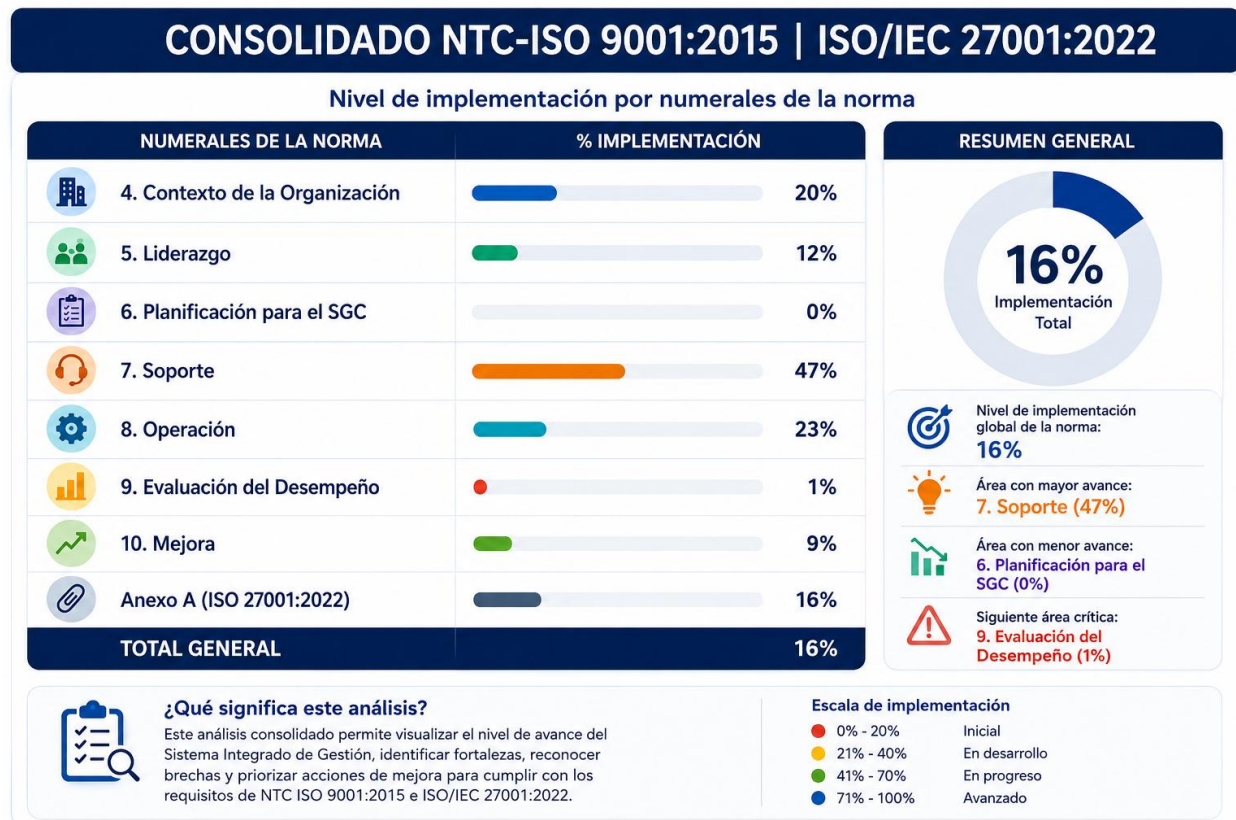


Fuente: Elaboración propia

En conclusión, consolidado del ejercicio diagnóstico para la compañía, se declara que estaba en etapa inicial de madurez en la gestión organizacional caracterizada por el uso de buenas prácticas operativas y administrativas, pero sin la determinación de una estructura

formal, clara y oportuna de gestión bajo procesos, el enfoque a la gestión de riesgos y la mejora continua del sistema.

Figura 19 Nivel de madurez inicial en Berruit SAS frente al sistema integrado de gestión



Fuente: Elaboración propia

Dentro de las principales brechas identificadas se encuentran:

- Identificación de partes interesadas de la organización.
- Diseño y gestión de análisis estratégico, tales como DOFA y PESTEL.
- Identificación general de los procesos organizacionales, formalizando el alcance dentro del sistema de gestión.
- Actualización del plan estratégico, modelo CANVA.
- Diseño del mecanismo para el manejo de información documentada.
- Seguimiento o evaluación de eficacia de los controles y prácticas organizacionales que han sido recientemente implementados.
- Documentación y caracterización de los procesos organizacionales.

- Definición formal de políticas del sistema de gestión.
- Implementación estructurada de la gestión de riesgos.
- Definición de roles y responsabilidades dentro del sistema de gestión.
- Establecimiento de indicadores y mecanismos de seguimiento.
- Implementación de controles específicos asociados a seguridad de la información.
- Implementación de auditorías internas.
- Desarrollo de mecanismos de mejora continua.

En este escenario se concluye la necesidad de realizar el diseño e implementación de un sistema integrado de gestión para estructurar y cumplir los lineamientos de las normas ISO de calidad y seguridad de la información vigentes.

8.2. Diseño del plan de trabajo para cumplimiento de requisitos ISO 9001 e ISO 27001.

Este capítulo responde al objetivo específico de Diseñar el plan de trabajo, para cumplir este objetivo, se contempló una duración aproximada de seis meses, periodo durante el cual se desarrollaron las actividades de diagnóstico, diseño y estructuración del Sistema Integrado de Gestión.

Este plan fue presentado y aprobado por la Alta Dirección de Berruit SAS al inicio del proyecto, garantizando la disponibilidad de los recursos requeridos y el compromiso de los responsables de cada proceso. Este respaldo resultó fundamental para la identificación efectiva de los procesos clave y la comprensión de sus interacciones, facilitando el acceso a la información organizacional y la toma oportuna de decisiones durante el desarrollo de la consultoría.

Así mismo, la organización dispuso los recursos tecnológicos necesarios para el desarrollo de reuniones, almacenamiento de información y construcción documental del sistema, facilitando la interacción entre procesos y la consolidación de la información requerida

Para la ejecución del plan de trabajo se consideraron recursos humanos conformados por el equipo consultor, la alta dirección de Berruit SAS, la dirección administrativa y los líderes de

proceso, quienes participaron activamente en las sesiones de levantamiento de información, validación documental y revisión de avances.

Para el diseño del plan de trabajo se incorporó la identificación, caracterización y articulación de los procesos organizacionales, lo cual se logró mediante:

- La construcción del mapa de procesos, que integra siete procesos estratégicos, misionales y de apoyo.
- La caracterización de cada proceso, definiendo entradas, actividades, salidas, responsables e indicadores.
- La identificación de las interacciones entre procesos, evidenciando cómo los resultados de un proceso se convierten en insumos de otros, bajo un enfoque sistémico.

Este ejercicio permitió garantizar que el Sistema Integrado de Gestión se estructurara no como un conjunto aislado de procedimientos, sino como un sistema dinámico.

El plan fue estructurado bajo el ciclo PHVA, permitiendo organizar las actividades de manera lógica y secuencial para asegurar el cumplimiento de los requisitos de las normas NTC-ISO 9001 e ISO/IEC 27001.

Fase Planear. En esta fase se establecieron las bases del sistema, incluyendo:

- Comprensión del contexto organizacional mediante análisis estratégico (PESTAL y DOFA).
- Identificación de partes interesadas y sus necesidades.
- Definición del alcance del sistema.
- Caracterización de los procesos clave y sus interacciones.

- Identificación, análisis y valoración de riesgos asociados a los procesos.
- Como resultado, se consolidó una estructura inicial del SIG alineada con los numerales 4, 5 y 6 de las normas, asegurando la coherencia entre contexto, procesos y riesgos.

Fase Hacer: Esta fase permitió materializar el diseño del sistema mediante:

- Formalización del liderazgo y compromiso organizacional.
- Definición de roles y responsabilidades asociadas a cada proceso.
- Implementación de controles operacionales.
- Desarrollo de procedimientos documentados.
- Implementación de controles de seguridad de la información.

En esta etapa, las interacciones entre procesos se operacionalizaron, evidenciando flujos de información, responsabilidades compartidas y puntos de control en la ejecución.

Fase Verificar: El plan contempló la evaluación del desempeño del sistema a través de:

- Seguimiento de indicadores de los procesos.
- Evaluación de la satisfacción del cliente.
- Auditorías internas por procesos y por requisitos normativos.
- Revisión por la dirección.

Estas actividades permiten validar la eficiencia de las interacciones entre procesos y la capacidad del sistema para generar resultados.

Fase Actuar: Finalmente, se estableció la fase de mejora continua, orientada a:

- Implementación de acciones correctivas.

- Tratamiento de no conformidades.
- Ajustes en los procesos y sus interacciones.

Esto garantiza que el sistema evolucione y se adapte a los cambios organizacionales y del entorno.

En conclusión, el diseño del plan de trabajo permitió cumplir plenamente con el objetivo específico planteado al estructurar un Sistema de Gestión Integrado basado en procesos, identificando sus interacciones clave en alineación con los requisitos de las normas ISO 9001:2015 e ISO/IEC 27001:2022. Es preciso aclarar que el alcance evaluable de este proyecto comprende el diseño e implementación documental correspondiente a los numerales 4 al 8 de la Estructura Armonizada. Por su parte, la planificación de los numerales 9 (Evaluación del desempeño) y 10 (Mejora) —incluida en el Anexo B Plan de implementación Berruit SAS— se presenta como una hoja de ruta proyectada para la continuidad operativa de la organización, por lo cual no forma parte de la evaluación del cumplimiento del presente objetivo. Este enfoque garantiza un sistema funcional y orientado a resultados, sentando las bases para la posterior evaluación y mejora continua.

8.3. Ejecución del plan de trabajo para el sistema integrado de gestión, numerales 4 al 8 de las normas NTC-ISO 9001:2015 e ISO/IEC 27001:2022.

Dando inicio a la consultoría, se ejecutó el plan de trabajo desarrollado en el numeral 8,2, con el propósito que Berruit continúe el camino de la implementación del Sistema de Gestión Integral ISO 9001 e ISO/IEC 27001. El abordaje se realizó a través de la aplicación por numerales de la norma con un tiempo de 11 meses, empezando en junio de 2025 y finalizando en mayo de 2026, de esta forma cumpliendo el cronograma establecido en este documento.

Durante la ejecución del proyecto se presentaron algunos retos asociados principalmente a la disponibilidad de tiempo de los líderes de proceso, debido a las actividades operativas propias de la organización y a los compromisos comerciales derivados de la prestación de servicios de

ciberseguridad. Esta situación generó ajustes menores en la programación inicial, especialmente en las actividades relacionadas con la validación documental y la recopilación de evidencias para la implementación de los controles de seguridad de la información.

Como resultado del seguimiento periódico al cronograma, se realizaron ajustes puntuales en la secuencia de algunas actividades sin afectar el cumplimiento de los objetivos establecidos. Entre los cambios más relevantes se encontró la necesidad de fortalecer la fase de análisis de riesgos y ampliar las sesiones de trabajo destinadas a la construcción de la Declaración de Aplicabilidad y la definición de controles asociados al Anexo A de la ISO/IEC 27001:2022, debido a la importancia estratégica de estos elementos para la organización.

Una de las principales lecciones aprendidas durante el desarrollo de la consultoría fue identificar que la implementación de un Sistema de Gestión de Seguridad de la Información resulta más eficiente cuando se desarrolla de manera integrada con un Sistema de Gestión de Calidad. La estructura por procesos, los mecanismos de control documental y el enfoque de mejora continua proporcionados por la ISO 9001:2015 facilitaron significativamente la construcción de los requisitos de la ISO/IEC 27001:2022, permitiendo una integración más organizada y alineada con los objetivos estratégicos de la organización.

Frente al alcance formulado para la consultoría de este trabajo de grado, se cumplió al 100 % con el desarrollo de los numerales 4 al 8 y el Anexo A de la norma ISO/IEC 27001:2022 a nivel documental y de diseño metodológico. Sin embargo, en lo que respecta al proyecto total de integración normativa en Berruit S.A.S., este avance abarca un 75 % de la hoja de ruta, quedando un 25 % pendiente correspondiente a los numerales 9 y 10. Estos últimos quedan proyectados en fase de planeación para que la empresa le dé continuidad al sistema mediante hitos estratégicos como la auditoría interna combinada, la revisión por la dirección y la demostración efectiva de los ciclos de mejora. Ver Anexo B.

En cuanto a la apropiación por parte de Berruit S.A.S., el SGI consolida un 82.7 % de cumplimiento global en el cuerpo de las normas y un 90.3 % en el marco de controles del Anexo A (destacando un 100 % en la categoría de Personas A.6, 90.9 % en Físico A.7, 85.2 % en Tecnológico A.8 y 85.1 % en Organizacional A.5). La brecha para alcanzar el 100 % de implementación institucional reside en actividades operativas a cargo de la empresa: el

fortalecimiento puntual del Capítulo 5 (Liderazgo, 87.5 %) y la puesta en marcha de los Capítulos 9 (Evaluación del desempeño, 25.0 %) y 10 (Mejora, 66.7 %), escenarios que requieren el desarrollo formal de la auditoría interna y la revisión por la dirección. Ver Anexo D.

A continuación, se describe la aplicación del plan de implementación en cada uno de los numerales integrados.

8.3.1. Numeral 4.1 – Comprensión de la organización y su contexto.

Dando inicio con el numeral 4.1, que indica la necesidad de la empresa en conocer su contexto interno y externo, identificando los factores que pueden afectar su capacidad para lograr los resultados previstos del sistema de gestión, los integrantes de la consultoría participaron en los dos espacios de reunión general de toda la compañía para el seguimiento y control de la operación mensual, en los cuales se realizaron los ejercicios de actualización y percepción de gerencia y líderes de procesos frente a elementos básicos del direccionamiento estratégico tales como la misión, visión (ver figura 22) y el modelo preliminar tipo Canva que describía de manera general los servicios ofrecidos. Resultado de esta reunión, se hizo necesario llevar a cabo la actualización de estos, porque se evidenciaron limitaciones en cuanto a su nivel de alineación estratégica y análisis. Se revisaron y redefinieron asegurando su coherencia con la realidad actual de la organización, su proyección futura y su enfoque hacia la calidad del servicio y la seguridad de la información. Este ejercicio permitió establecer una base sólida para el levantamiento del contexto organizacional, la toma de decisiones y la orientación de los objetivos organizacionales.

Figura 20 Misión y Visión de Berruit S.A.S.

Adicionalmente, se llevó a cabo la formulación del propósito de la empresa y se definieron los valores corporativos, información clave para poder consolidar la cultura y de esta manera iniciar la sensibilización del talento humano con los principios del sistema de gestión. Esta información contribuye significativamente a la generación de valor y al compromiso de todos frente al cumplimiento de los requisitos de estas normas internacionales.

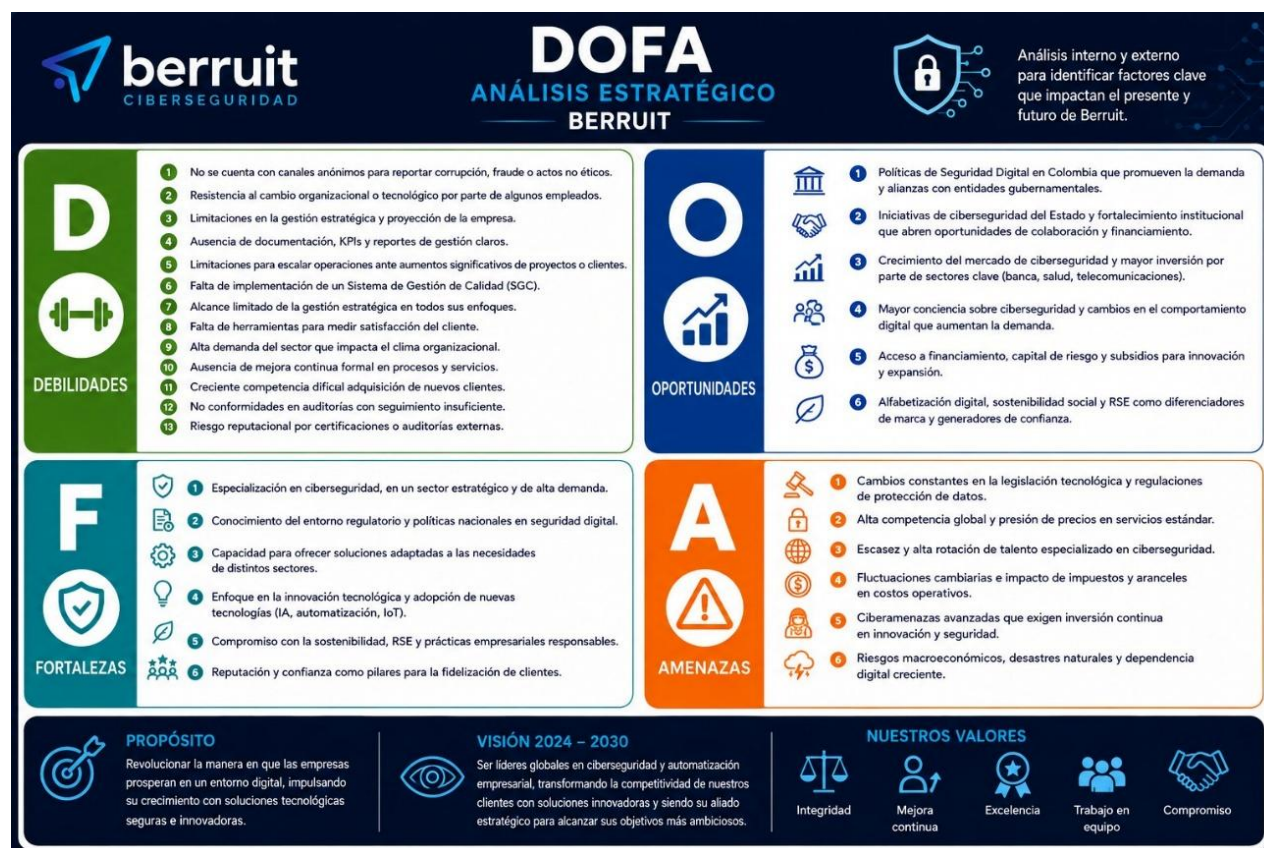
También se procedió a definir el alcance del sistema integrado de gestión, el cual se detalla en el numeral 8.3.3 de este trabajo, de esta forma se delimitaron los servicios y los productos que Berruit S.A.S ofrece, definiendo claramente los procesos, las ubicaciones donde presta sus servicios y productos y sus partes interesadas involucradas. Este alcance fue estructurado teniendo en cuenta los requisitos que las normas de calidad y de seguridad de la información, garantizando así su aplicabilidad y la pertinencia dentro del contexto de la organización.

En cuanto al análisis del contexto, se decidió dar uso de herramientas estratégicas ya estandarizadas, con las cuales se pueda permitir una comprensión integral de los factores internos y externos que incidan en la operación de Berruit SAS, es así como para todo el ámbito interno se utilizó la matriz DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas - Ver figura 21), mediante la cual se identificaron aspectos clave como que la empresa cuenta con habilidades internas, especialmente en lo relacionado con la experiencia técnica, la especialización en los servicios ofrecidos de ciberseguridad y la orientación al cliente, aspectos que representan ventajas relevantes en el entorno dinámico al que pertenece. Estas fortalezas identificadas junto con las

oportunidades externas encontradas en el ejercicio, tales como, el crecimiento del mercado tecnológico y la seguridad informática, el apoyo normativo del país y la transformación digital de las organizaciones, concluyen un buen escenario para que Berruit SAS pueda consolidarse y expandirse. Sin embargo, el análisis también pone en manifiesto la necesidad de fortalecer elementos estructurales clave, como la formalización de procesos, la medición del desempeño y la alineación estratégica, los cuales son fundamentales para garantizar la sostenibilidad y escalabilidad del negocio.

En cuanto a las debilidades, el ejercicio realizado demostró una limitada estandarización de procesos, ausencia de herramientas robustas de seguimiento y control y la resistencia al cambio, situaciones que se agravan junto a las amenazas externas como la rápida evolución tecnológica, el incremento de riesgos en ciberseguridad, la alta competitividad del sector y los cambios regulatorios en materia TICs. En este contexto, el ejercicio DOFA permitió comprender de manera integral la situación actual de la organización, siendo esto un insumo estratégico para la planificación de la implementación del Sistema Integrado de Gestión bajo las normas ISO 9001 e ISO/IEC 27001.

Figura 21 DOFA Berruit SAS



Fuente: Elaboración propia

Por otro lado, para el análisis del entorno externo, se utilizó la metodología PESTAL (ver figura 22), donde se evidencia un entorno macroeconómico dinámico y con un alto potencial de crecimiento para el sector de la ciberseguridad. En el ámbito político-legal y social, el endurecimiento normativo y la mayor conciencia colectiva frente a las amenazas digitales incrementan la demanda de servicios, aunque imponen el reto de responder con rapidez regulatoria y atender a clientes cada vez más exigentes. En las dimensiones económica y tecnológica, la posibilidad de acceder a fuentes de financiamiento e innovar continuamente se contrapone a riesgos como la volatilidad cambiaria, la carga tributaria en importaciones y la constante evolución de los ciberataques. Finalmente, el componente ambiental proyecta una oportunidad de diferenciación competitiva mediante el uso eficiente de la energía y la gestión responsable de residuos informáticos.

Figura 22 Resumen del análisis PESTAL

Fuente: Elaboración propia.

En conclusión, el análisis PESTAL permitió complementar y robustecer los hallazgos obtenidos en la matriz DOFA, proporcionando una visión más amplia y estructurada del contexto externo de la organización.

El cumplimiento del numeral 4.1 “Comprensión de la organización y su contexto” no se asocia de manera directa con un control específico del Anexo A de la ISO/IEC 27001, dado que este último corresponde a un conjunto de controles de seguridad de la información de carácter operativo y técnico. Sin embargo, su implementación constituye un elemento fundamental para la adecuada selección, diseño e implementación de dichos controles.

8.3.2. Numeral 4.2 - Comprensión de las necesidades y expectativas de las partes interesadas

El cumplimiento del numeral 4.2, indica que es necesario identificar cuáles son las partes interesadas pertinentes de la organización, luego, conocer cuales sus necesidades y expectativas, y posteriormente evaluar cuales de ellas se convierten en requisitos legales aplicables que Berruit SAS deberá trabajar por cumplir o satisfacer.

Dando inicio con la identificación y clasificación de las partes interesadas, estas fueron segmentadas en dos grandes grupos: internas y externas. Respecto a las internas se lograron clasificar los propietarios o accionistas, los empleados, el comité paritario de seguridad y salud en el trabajo (COPASST) y la brigada de emergencias. En cuanto a las partes interesadas externas se identificaron como actores clave para la operación y continuidad de Berruit SAS, los clientes, proveedores y contratistas, el estado y/o entidades regulatorias nacionales e internacionales, la competencia y la comunidad.

A continuación, se realizó un análisis de esas necesidades y expectativas de cada una de estas partes interesadas, estableciendo una relación directa entre los requerimientos y la operación de Berruit. En cuanto a los accionistas su principal necesidad es la rentabilidad del negocio, la mejora en la optimización de los recursos, el desarrollo de la innovación, mientras que sus expectativas se centran en la transparencia, el crecimiento del negocio y su continuidad. Respecto a la parte interesada de empleados, se compilaron sus necesidades en contar constantemente con su seguridad social vigente, el desarrollo y crecimiento profesional, la estabilidad laboral y el cumplimiento de todos los acuerdos laborales con Berruit SAS, estas necesidades se complementan con las expectativas que van dirigidas a tener condiciones laborales adecuadas, capacitación y una comunicación asertiva y efectiva a nivel general.

En cuanto a los actores como el COPASST y la brigada de emergencias, cuyos requerimientos están enfocados al cumplimiento normativo tal como la prevención de riesgos, disponibilidad de recursos y entrenamiento para la atención de emergencias. Estas necesidades se alinean con sus expectativas relacionadas con la generación de ambientes seguros y la mejora continua en la gestión de riesgos laborales.

Iniciando la evaluación del contexto externo, se comienza con los clientes, los cuales representan una de las partes interesadas más relevantes, donde sus necesidades se encuentran enfocadas a la calidad del servicio, al cumplimiento de todos los requisitos normativos y los resultados confiables. En cuanto a sus expectativas, se determinan que van asociadas a mantener una comunicación efectiva, la prestación de los servicios de manera oportuna, disponibilidad inmediata, soporte técnico adecuado y una asesoría especializada, esto va asociado a la fidelización y la satisfacción. En cuanto a la parte interesada de los proveedores y contratistas se encuentra que sus necesidades están dirigidas a tener relaciones comerciales claras, pagos oportunos y procesos transparentes, por otro lado, sus expectativas están relacionadas con mantener una estabilidad en la relación comercial y que sean transparentes y equitativos los procesos de selección.

Siguiendo con la parte interesada del estado y/o entidades regulatorias y autoridades nacionales o internacionales, siendo este grupo una parte crítica por su impacto en cada decisión y regulación aprobada en el marco de la seguridad de la información en Colombia, sus necesidades están centradas en el cumplimiento de normativas legales, tales como la protección de datos personales y estándares internacionales como ISO/IEC 27001, así como la alineación con disposiciones laborales, fiscales y ambientales. En consecuencia, sus expectativas se relacionan con la transparencia, la trazabilidad de la información y la adecuada gestión de incidentes de seguridad.

Finalmente, se consideraron otras partes interesadas como la competencia y la comunidad, cuyas necesidades y expectativas se centran en las condiciones equitativas de mercado, responsabilidad social, cumplimiento normativo y contribución al desarrollo económico. Este análisis permitió identificar requisitos cruciales en materia de reputación y sostenibilidad del negocio.

Como parte del ejercicio realizado se dejaron evidencias objetivas, donde se incorporaron informes financieros, encuestas de aceptación del servicio a satisfacción, registros de capacitación, entrevistas con líderes de procesos, contratos, informes del área comercial, entre otros. Asimismo, se llevó a cabo un análisis del impacto ambiental asociado a cada parte interesada, lo cual fortalecerá la integración del enfoque ambiental dentro del sistema de gestión cuando Berruit SAS así lo decida, lo anterior permite que la compañía de inicio al desarrollo de buenas prácticas organizacionales y demostrar compromiso frente a la sostenibilidad.

En conclusión, se logró identificar, analizar y documentar de manera estructurada las partes interesadas pertinentes, así como sus necesidades y expectativas, estableciendo mecanismos para su seguimiento y cumplimiento. Este ejercicio no solo da cumplimiento al numeral 4.2 de las normas ISO 9001:2015 e ISO/IEC 27001:2022, sino que también se convierte en un insumo fundamental para la planificación estratégica, la gestión de riesgos y la mejora continua del sistema de gestión.

Finalmente, en relación con la ISO/IEC 27001:2022, si bien este numeral no se vincula directamente con controles específicos del Anexo A, sí tiene una relación indirecta relevante, ya que la identificación de partes interesadas y sus requisitos influye en la determinación de necesidades de seguridad de la información, así como en la definición de controles aplicables, especialmente aquellos relacionados con cumplimiento legal, gestión de relaciones con clientes, terceros y protección de la información.

8.3.3. Numeral 4.3 – Determinación del alcance del Sistema de Gestión Integrado

En el marco del cumplimiento del requisito 4.3, relacionado con la necesidad de determinar y definir el alcance del sistema, considerando los límites y la aplicabilidad del mismo en función del contexto organizacional, las partes interesadas y los productos y servicios ofrecidos por la empresa, y con base en el resultado del análisis desarrollado en los numerales 4.1 y 4.2, relacionados con la comprensión del contexto organizacional y las necesidades y expectativas de las partes interesadas, se procedió a estructurar el alcance del SGI de Berruit S.A.S., asegurando su coherencia con la naturaleza del negocio y su direccionamiento estratégico. En este sentido, el alcance definido contempla la implementación y cumplimiento de los requisitos establecidos por

las normas ISO 9001:2015, enfocada en la gestión de la calidad, e ISO/IEC 27001:2022, orientada a la gestión de la seguridad de la información, tal como se detalla a continuación:

El Sistema de Gestión Integrado (SGI) de BERRUIT, abarca la implementación y el cumplimiento de los requisitos establecidos por las normas ISO 9001:2015 (Gestión de la Calidad) y ISO/IEC 27001:2022 (Seguridad de la Información), dentro de la comercialización y distribución de productos tecnológicos, incluyendo hardware, software y servicios especializados tales como consultoría IT, ciberseguridad, outsourcing IT, outsourcing BPO, redes e infraestructura tecnológica, operando a nivel nacional desde la ciudad de Bogotá, Colombia. El SGI aplica a los procesos estratégicos (Gerencia, sistema de gestión integral), misionales (comercial, soporte técnico externo) y de apoyo (compras, recursos humanos, soporte técnico interno), asegurando la satisfacción del cliente, la mejora continua y la protección de la información.

Servicios tercerizados: Los servicios cloud son provistos por terceros bajo acuerdos contractuales que garantizan el cumplimiento de los requisitos aplicables.

Exclusiones:

ISO 9001:2015 - 8.3 Diseño y Desarrollo de los productos y Servicios: Se excluyen las actividades de diseño y desarrollo y programación, ya que no hacen parte de las actividades de la compañía.

ISO 9001:2015 - 7.1.5.2 Recursos de seguimiento y medición (trazabilidad de las mediciones): La organización no emplea equipos de medición sujetos a calibración o trazabilidad metrológica (instrumentos físicos de medición). Las herramientas de monitoreo de TI normalmente no requieren calibración metrológica, pero sí validación funcional y control de configuración.

ISO 27001:2022 - A.7.1 a A7.4 y A8.25 a A8.31: Instalaciones físicas, dado que no forman parte del modelo de negocio de la compañía.

Este alcance considera todos los procesos y activos relacionados con la gestión de la calidad y la seguridad de la información en las operaciones definidas. Sistema de Gestión Integrado abarca todas las actividades relacionadas con la comercialización y distribución de productos tecnológicos, tales como hardware y software, así como la prestación de servicios especializados como consultoría en tecnologías de la información, ciberseguridad, outsourcing IT, outsourcing BPO, redes e infraestructura tecnológica. Estas actividades se desarrollan a nivel nacional, teniendo como sede principal de operación la ciudad de Bogotá, Colombia.

Asimismo, el alcance del SGI incluye la totalidad de los procesos organizacionales, los cuales fueron clasificados en procesos estratégicos, misionales y de apoyo. Dentro de los procesos estratégicos se encuentra la gerencia y la gestión del sistema integrado; los procesos misionales comprenden la gestión comercial y el soporte técnico externo; mientras que los procesos de apoyo incluyen áreas como compras, gestión de talento humano y soporte técnico interno.

En relación con la provisión de servicios tercerizados, se identificó que algunos servicios, particularmente aquellos asociados a soluciones en la nube (cloud), son suministrados por proveedores externos. En este sentido, la organización ha establecido acuerdos contractuales que aseguran el cumplimiento de los requisitos aplicables en términos de calidad y seguridad de la información, garantizando así el control sobre los servicios externalizados conforme a lo exigido por ambas normas.

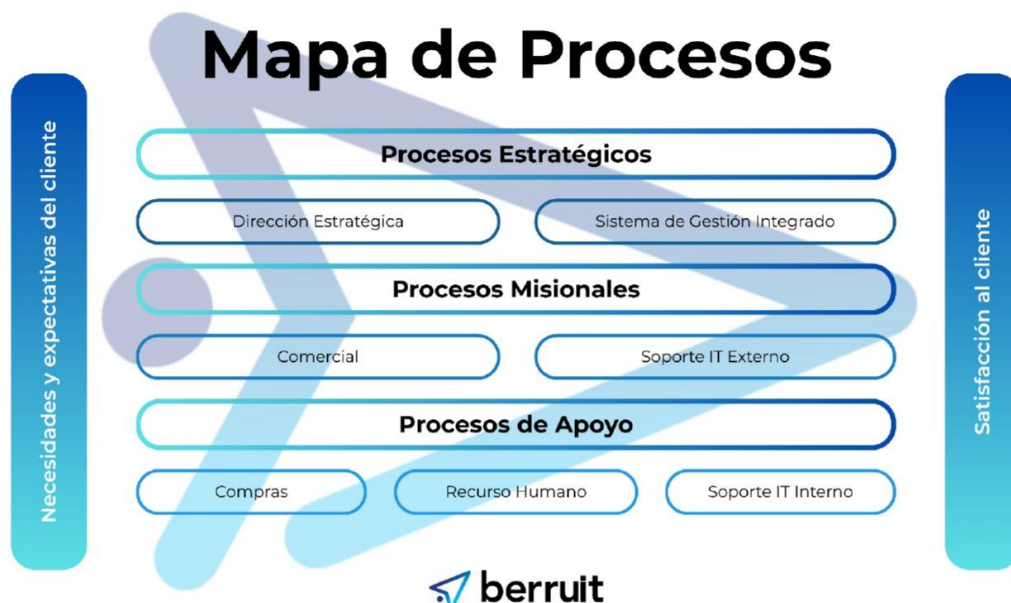
Por otra parte, se definió la no aplicabilidad justificada dentro del alcance del sistema. En el caso de la norma ISO 9001:2015, no aplica el numeral 8.3 relacionado con el diseño y desarrollo de productos y servicios, debido a que la organización no realiza actividades de este tipo, limitándose a la comercialización e implementación de soluciones tecnológicas, utilizando la infraestructura del cliente, optimizando la topografía tecnológica actual y proponiendo alternativas eficientes, rentables y seguras. En cuanto a la norma ISO/IEC 27001:2022, se ha considerado la no aplicabilidad de los controles correspondientes a instalaciones físicas (A.7.1 a A.7.4 y A.8.25 a A.8.31), dado que estos no hacen parte del modelo operativo de la organización, el cual no contempla infraestructura física sino 100% trabajo híbrido o uso de instalaciones del cliente. Esta decisión se encuentra debidamente justificada en la Declaración de Aplicabilidad (SoA), ver Anexo C.

En conclusión, la organización logró establecer un alcance claro, coherente y debidamente documentado del Sistema Integrado de Gestión, cumpliendo con los lineamientos del numeral 4.3 de las normas ISO 9001:2015 e ISO/IEC 27001:2022. Este alcance permite delimitar de manera precisa la aplicación del sistema, facilitando su implementación, evaluación y mejora continua.

8.3.4. Numeral 4.4 – Sistema de gestión y sus procesos

Una vez definido el contexto organizacional (numeral 4.1), las partes interesadas (numeral 4.2) y el alcance del Sistema Integrado de Gestión (numeral 4.3), se procedió a abordar el numeral 4.4, el cual establece la necesidad de que la organización determine, implemente, mantenga y mejore continuamente un sistema de gestión basado en procesos, incluyendo las interacciones entre los mismos. En este sentido, Berruit S.A.S. diseñó e implementó su Sistema Integrado de Gestión bajo un enfoque basado en procesos, estructurando un mapa de procesos (Ver figura 25), que permite visualizar de manera integral la operación de la organización, así como la interacción y articulación entre sus diferentes componentes. Este mapa de procesos se convierte en una herramienta clave para la gestión organizacional, al facilitar la comprensión del flujo de actividades, la generación de valor y el cumplimiento de los objetivos estratégicos.

Figura 23 Mapa de procesos Berruit SAS



Fuente: Elaboración propia.

De acuerdo con la estructura definida, los procesos fueron clasificados en tres grandes categorías: estratégicos, misionales y de apoyo. En primer lugar, los procesos estratégicos comprenden la dirección y orientación de la organización, incluyendo la gerencia y la gestión del Sistema Integrado, desde donde se establecen lineamientos, políticas, objetivos y mecanismos de seguimiento para garantizar la mejora continua y el cumplimiento de los requisitos normativos.

En segundo lugar, los procesos misionales corresponden al núcleo del negocio y están directamente relacionados con la generación de valor para el cliente. En este grupo se incluyen el proceso comercial y el soporte técnico externo, los cuales permiten la prestación de los servicios de tecnología, ciberseguridad, outsourcing y demás soluciones ofrecidas por la organización. Estos procesos se caracterizan por su interacción directa con el cliente, siendo determinantes para la satisfacción de sus necesidades y expectativas.

Por último, los procesos de apoyo incluyen aquellas actividades que, si bien no generan valor de manera directa, son fundamentales para el adecuado funcionamiento de la organización. Dentro de estos se encuentran procesos como compras, gestión de talento humano y soporte técnico interno, los cuales garantizan la disponibilidad de recursos, competencias y condiciones necesarias para la operación eficiente de los procesos misionales.

Adicionalmente, para cada uno de los procesos definidos, se establecieron sus respectivas entradas, salidas, responsables, recursos, indicadores de desempeño y criterios de control, lo cual permite asegurar su adecuada gestión y seguimiento. Asimismo, se identificaron los riesgos y oportunidades asociados a cada proceso, en coherencia con el enfoque basado en riesgos promovido por las normas ISO 9001:2015 e ISO/IEC 27001:2022.

El mapa de procesos también permitió evidenciar la interacción entre los diferentes procesos, destacando cómo los procesos estratégicos orientan la operación, los misionales generan valor y los de apoyo facilitan la ejecución de las actividades. Esta interacción asegura la coherencia del sistema y fortalece la trazabilidad de la información, aspecto clave en la gestión de la calidad y la seguridad de la información.

En cuanto a la gestión de la seguridad de la información, el enfoque por procesos permitió integrar controles y medidas de protección a lo largo de toda la operación, garantizando la confidencialidad, integridad y disponibilidad de la información en cada una de las actividades desarrolladas. De igual forma, se establecieron mecanismos de seguimiento, medición y mejora continua que permiten evaluar la eficacia del sistema y promover su evolución en el tiempo.

En conclusión, la organización logró establecer, implementar y mantener un Sistema Integrado de Gestión basado en procesos, cumpliendo con los requisitos del numeral 4.4 de las normas ISO 9001:2015 e ISO/IEC 27001:2022. Este enfoque no solo facilita la gestión eficiente de las actividades organizacionales, sino que también fortalece la capacidad de la empresa para adaptarse a los cambios del entorno, gestionar riesgos y asegurar la satisfacción de las partes interesadas.

Finalmente, en relación con la ISO/IEC 27001:2022, este numeral guarda una relación indirecta pero fundamental con el Anexo A, en la medida en que la definición de procesos permite identificar puntos de control donde se deben implementar medidas de seguridad de la información, tales como controles de acceso, gestión de activos, gestión de incidentes y relaciones con proveedores, asegurando así la adecuada protección de la información en toda la organización.

8.3.5. Numeral 5 – Liderazgo

El capítulo 5 correspondiente a liderazgo se abordó como un eje fundamental para garantizar la adecuada implementación, mantenimiento y mejora continua del sistema. Este capítulo resalta el rol de la alta dirección en la definición del direccionamiento estratégico, la asignación de roles y responsabilidades y la promoción de una cultura organizacional orientada al nuevo sistema integrado de gestión frente a la calidad y la seguridad de la información.

Liderazgo y compromiso

La alta dirección de Berruit S.A.S. asumió un rol activo y visible en la implementación del Sistema Integrado de Gestión, evidenciando su compromiso mediante la participación en la definición del contexto organizacional, la política y objetivos, la aprobación del alcance, la asignación de recursos y el seguimiento a los avances del diseño e implementación del sistema.

Este compromiso se materializó en la integración del SIG dentro de los procesos estratégicos de la organización, asegurando que los objetivos del sistema estén alineados con la dirección estratégica del negocio.

Asimismo, la gerencia promovió el pensamiento basado en procesos y en riesgos, se fortaleció la cultura organizacional mediante los espacios autorizados para la sensibilización al personal en temas de calidad y seguridad de la información. Su participación activa contribuyó a la fomentar en el personal la responsabilidad individual desde su cargo frente al cumplimiento de los requisitos del sistema y el éxito del ejercicio de consultoría.

Política

Como parte del liderazgo estratégico, la organización estableció y documentó su política integrada, donde se incluyen lineamientos relacionados con la calidad del servicio y la protección de la información, la cual quedó formalizada con el documento (Código: D-DE-06) que funge como la declaración de principios de Berruit S.A.S. Esta política fue diseñada de manera coherente con el propósito organizacional, el contexto identificado y las necesidades de las partes interesadas, garantizando su pertinencia y suficiencia, abordando simultáneamente lo siguiente:

- La satisfacción de las partes interesadas y el cumplimiento de requisitos y estándares de calidad.
- El compromiso con la seguridad de los activos de información y la gestión de riesgos tecnológicos.
- El cumplimiento del marco legal colombiano vigente.
- El compromiso con la mejora continua

La divulgación de esta política se realiza de manera transversal, asegurando que, desde el nivel estratégico hasta el operativo, cada colaborador comprenda su impacto en el cumplimiento de los objetivos y propósito de la compañía, así como la aplicación en el desarrollo de las actividades diarias.

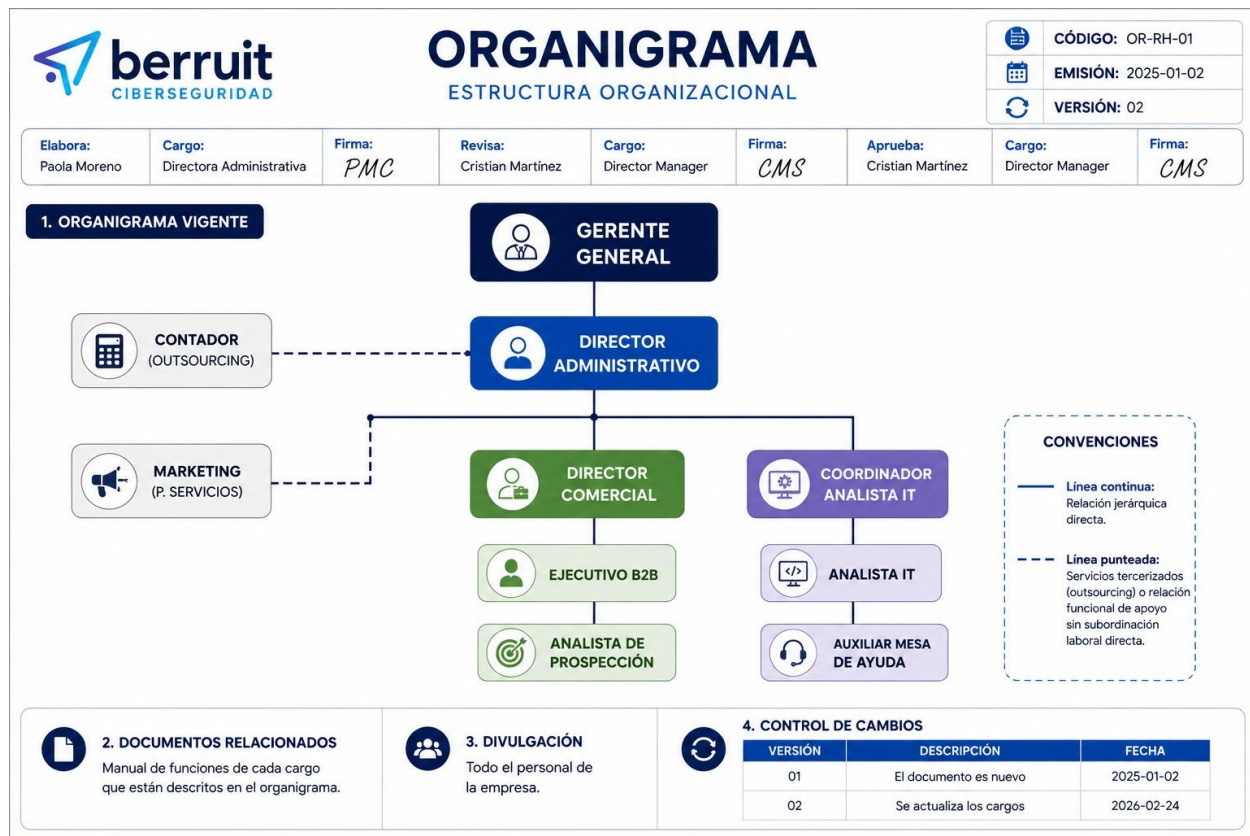
Roles, responsabilidades y autoridades en la organización

En cumplimiento de este requisito, Berruit S.A.S. actualizó los roles, responsabilidades y autoridades existentes con el fin de incorporar todos los requisitos de las normas ISO 9001:2015 e ISO/IEC 27001:2022 dentro del Sistema Integrado de Gestión, asegurando que cada colaborador comprenda su posición en el sistema, así como su función y contribución al logro de los objetivos organizacionales en materia de la calidad y la seguridad de la información.

Como evidencia de ello, se actualizó el organigrama (ver figura 24), los manuales de funciones y perfiles de cargo por cada proceso existente, en ellos se establecen de manera detallada las responsabilidades, competencias y requisitos de cada rol dentro de la organización, divulgando la asignación adecuada de responsabilidades, especialmente en lo relacionado con la protección de los activos de información y el cumplimiento de los controles del SGI.

Algunos ejemplos de manuales definidos y que demuestran un impacto en los requisitos de las normas a implementar, es el proceso de gestión de talento humano, donde se definieron roles específicos para la selección de personal (ver manuales de funciones M-RH-01 al M-RH-08), incluyendo la participación de la alta dirección, recursos humanos y líderes de área, garantizando la idoneidad del talento humano vinculado a la organización. Esto resulta clave para asegurar que el personal cuente con las competencias necesarias para desempeñar sus funciones y contribuir al cumplimiento del sistema de gestión.

Figura 24 Organigrama Berruit S.A.S



Fuente: Elaboración propia.

Por otro lado, en el proceso comercial se establecieron responsabilidades claras para cada uno de los actores involucrados, desde la prospección hasta el seguimiento postventa, asegurando la trazabilidad de las actividades y el enfoque hacia la satisfacción del cliente. Este aspecto se complementa con la implementación de mecanismos de medición, tales como indicadores de desempeño y encuestas de satisfacción, que permiten evaluar la percepción del cliente y generar acciones de mejora.

Adicionalmente, la organización fortaleció el enfoque hacia el cliente mediante la implementación de procedimientos que permiten gestionar la relación comercial, evaluar la satisfacción y dar seguimiento a las necesidades identificadas. Este enfoque es clave para garantizar la calidad del servicio y la mejora continua, en alineación con los requisitos de la norma ISO 9001.

8.3.6. Numeral 6 – Planificación

Una vez definidas las bases estratégicas y estructurales del Sistema Integrado de Gestión mediante el contexto organizacional, la identificación de necesidades de las partes interesadas, la definición del alcance y el enfoque basado en procesos con la construcción del mapa de procesos, se procedió al desarrollo del capítulo 6 correspondiente a la planificación. Este capítulo representa los mecanismos necesarios para identificar, evaluar y tratar los riesgos y oportunidades que pueden afectar el cumplimiento de los objetivos definidos, la calidad del servicio y la seguridad de la información. De igual manera, suministra las bases para la definición de objetivos estratégicos, la formulación de planes de acción y la gestión controlada de todos los cambios que se presenten en la organización y afecte el desempeño del sistema.

Para Berruit S.A.S., la planificación se desarrolló bajo un enfoque preventivo y basado en riesgos, abarcando la operación, la prestación del servicio tecnológico, la seguridad de la información, la continuidad del negocio y el cumplimiento normativo y contractual identificado. Se desarrollaron metodologías, matrices y procedimientos documentados para identificar las amenazas, vulnerabilidades, y oportunidades de mejora en los procesos.

Para dar inicio, se implementó una metodología de evaluación de riesgos basada en la valoración de probabilidad y consecuencia, utilizando escalas de medición que permitieran determinar el nivel de criticidad de los riesgos para priorizar su intervención. Esta metodología orientó la toma de decisiones para determinar la aceptabilidad de los riesgos, permitiendo definir cuáles requerían acciones inmediatas de tratamiento y cuáles podían ser aceptados temporalmente bajo seguimiento y monitoreo. Este enfoque permitió priorizar recursos y enfocar esfuerzos sobre aquellos riesgos con mayor impacto potencial para la organización.

Asimismo, la planificación contempló la definición de objetivos integrados del Sistema de Gestión, alineados con las políticas organizacionales definidas y el direccionamiento estratégico de la empresa. Estos objetivos fueron definidos con indicadores, metas, responsables y mecanismos para el seguimiento, permitiendo evaluar el desempeño del sistema.

De igual forma, se formalizó la gestión de cambios mediante el desarrollo de un procedimiento documentado que permiten controlar las modificaciones organizacionales,

tecnológicas, operativas y documentales que puedan afectar el desempeño del Sistema Integrado de Gestión, en especial en Berruit SAS donde la evolución tecnológica y los riesgos a nivel de ciberseguridad es contante, con el fin de garantizar la adaptación, control y planificación de estos cambios.

Acciones para abordar riesgos y oportunidades

En cumplimiento de los requisitos establecidos en el numeral 6.1 se tuvo en cuenta el contexto organizacional previamente identificado, así como las necesidades y expectativas de las partes interesadas, con esto se realizaron matrices de identificación y valoración de riesgos aplicables a los procesos estratégicos, misionales y de apoyo de la organización (MT-SGI-02). Dichas matrices permitieron identificar eventos que pudieran afectar el cumplimiento de objetivos estratégicos, operacionales, legales, tecnológicos y de seguridad de la información. La metodología implementada se basó en la evaluación de dos variables fundamentales: probabilidad y consecuencia.

En cuanto a la probabilidad, se estableció una escala de valoración de cinco niveles, que va desde “No probable” hasta “Muy probable”, permitiendo determinar la frecuencia estimada de ocurrencia de un evento o situación de riesgo. Por su parte, la consecuencia fue valorada mediante una escala de cinco niveles, desde “Muy bajo” hasta “Alta”, considerando el impacto que un evento puede generar sobre el cumplimiento de requisitos, los objetivos estratégicos, la satisfacción del cliente y la continuidad de las operaciones.

La combinación de estas variables permitió determinar el nivel de criticidad de cada riesgo identificado y establecer prioridades de intervención. A partir de esta valoración, se definieron controles existentes, responsables, recursos requeridos y acciones de tratamiento orientadas a reducir el impacto o la probabilidad de ocurrencia de los riesgos identificados.

En el caso específico de la ISO/IEC 27001:2022, la gestión de riesgos adquirió un enfoque especializado orientado a la protección de los activos de información, considerando amenazas relacionadas con pérdida de confidencialidad, integridad y disponibilidad de la información. Para ello, se evaluaron riesgos asociados a accesos no autorizados, fallas tecnológicas, vulnerabilidades

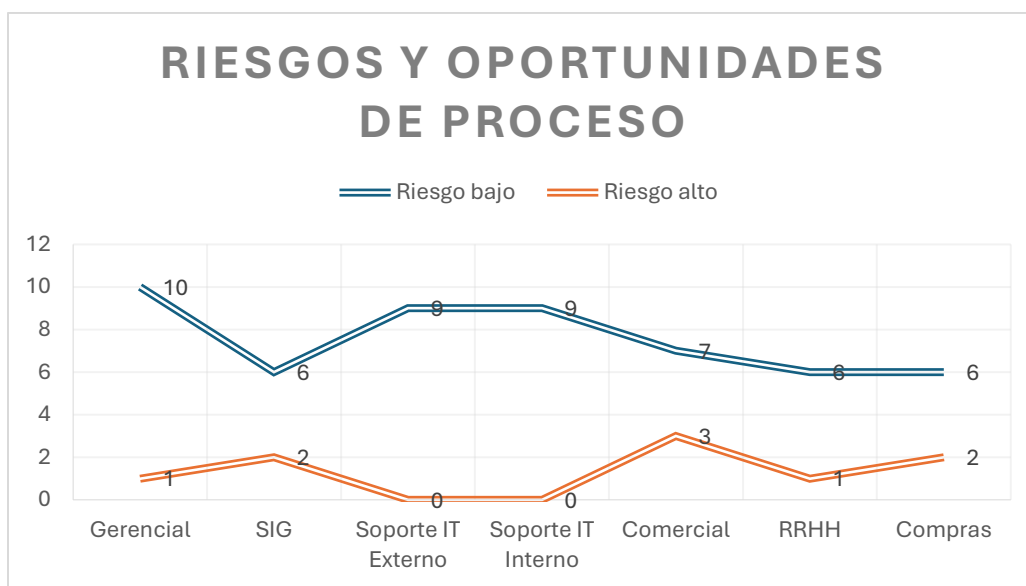
operacionales, errores humanos y amenazas cibernéticas, entre otros aspectos críticos para la operación de Berruit S.A.S.

En la figura 25, se evidencia la evaluación realizada donde la mayor parte de los riesgos de la organización se encuentran controlados en un nivel Bajo, destacando el proceso *Gerencial* (10 eventos) y los procesos de *Soporte IT* (9 eventos cada uno), estos últimos con un desempeño óptimo de cero riesgos críticos.

Sin embargo, para efectos del diseño del Sistema de Gestión, el foco de intervención se concentra en los 7 riesgos altos distribuidos en tres procesos clave:

- **Comercial (3 Riesgos Altos):** Concentra la mayor vulnerabilidad debido a bases de datos desactualizadas en la prospección, debilidades operativas en la negociación/cierre de ventas que afectan la rentabilidad, y fallas de control en la manipulación de ofertas. Asimismo, presenta un riesgo crítico de cumplimiento legal ante la posible vulneración de datos personales (Ley 1581 de 2012).
- **Sistema de Gestión Integrado - SIG (2 Riesgos Altos):** Asociados a la ausencia o datos incompletos en el seguimiento de indicadores —lo que impide medir objetivamente el desempeño del sistema— y a la falta de un plan formalizado de auditorías internas, interrumpiendo el ciclo de mejora continua.
- **Compras (2 Riesgos Altos):** Evidencia fallas en la etapa precontractual por falta de análisis técnicos y financieros antes de la aprobación de compras, y una deficiente gestión de incidentes con proveedores, lo que impide documentar reclamos y capitalizar lecciones aprendidas.

Este diagnóstico fundamenta la priorización de los planes de acción y controles operacionales propuestos en los capítulos posteriores de esta consultoría.

Figura 25 Riesgos y oportunidades de proceso

Fuente: Elaboración propia.

Evaluación de riesgos de seguridad de la información

En cumplimiento del numeral 6.1.2 de la norma ISO/IEC 27001:2022, Berruit S.A.S. se identificaron los activos de información asociados a los procesos definidos dentro del alcance del Sistema Integrado de Gestión. Este ejercicio permitió reconocer los recursos críticos para la operación, incluyendo información digital, infraestructura tecnológica, software, servicios en la nube, documentación organizacional y recursos humanos con acceso a información sensible.

Posteriormente, se realizó la valoración de riesgos basado en la metodología mencionada en el numeral 7.3.6.1 de este trabajo, como resultado de esta evaluación, se identificaron riesgos asociados a diferentes escenarios de amenaza, tales como accesos no autorizados, pérdida de información, fallas tecnológicas, falta de acceso o funcionalidad de servicios, errores humanos, ciberataques y deficiencias en la gestión de proveedores tecnológicos.

En conclusión, la organización logró implementar una metodología estructurada y documentada para la evaluación de riesgos de seguridad de la información, cumpliendo con los requisitos establecidos en el numeral 6.1.2 de la ISO/IEC 27001:2022. Este proceso permitió fortalecer la capacidad de la organización para anticiparse a amenazas, proteger sus activos de información y garantizar la continuidad y confiabilidad de sus servicios tecnológicos.

Tratamiento de riesgos y Declaración de Aplicabilidad

Una vez finalizada la evaluación de riesgos de seguridad de la información, se procedió a estructurar el proceso de tratamiento de riesgos mediante el uso de la Matriz de Riesgos y Oportunidades Integrada (MT-SGI-02), en conformidad con el numeral 6.1.3 de la norma ISO/IEC 27001:2022. Esta matriz define las acciones orientadas a mitigar, transferir, aceptar o evitar los riesgos identificados en el Sistema de Gestión de Seguridad de la Información (SGSI).

Para los escenarios donde el riesgo residual se determinó alto o crítico, se establecieron controles organizacionales, tecnológicos y operacionales en la matriz MT-SGI-02. Entre estas medidas se destacan el fortalecimiento de la Política de Seguridad de la Información (PO-STE-01), el control de accesos basado en privilegios mínimos (P-STE-02 y G-STE-01), esquemas de respaldo y recuperación de datos (P-STE-04), el monitoreo de proveedores tecnológicos, programas de concientización al personal y el despliegue de procedimientos documentados para reducir la probabilidad e impacto de incidentes.

De forma complementaria, algunos riesgos residuales menores fueron aceptados formalmente al encontrarse dentro del nivel de tolerancia fijado por la dirección, o bien cuando el costo del control superaba la pérdida potencial. Asimismo, se fijaron mecanismos de transferencia de riesgo mediante acuerdos de nivel de servicio (SLA) y cláusulas de confidencialidad en contratos con proveedores de infraestructura en la nube y soporte especializado.

Como elemento articulador del tratamiento, se desarrolló la Declaración de Aplicabilidad (SOA-SGI-01), documento maestro que formaliza y justifica la selección de los controles de seguridad para Berruit S.A.S., garantizando la trazabilidad entre las amenazas identificadas en la matriz MT-SGI-02 y las salvaguardas del Anexo A de la norma ISO/IEC 27001:2022.

La Declaración de Aplicabilidad fue formulada considerando la naturaleza operativa de Berruit S.A.S. y sus requerimientos legales, contractuales y de negocio. En este sentido, se definieron las no aplicabilidades justificadas del sistema, focalizadas en la exclusión de los controles de seguridad física sobre instalaciones e infraestructura propia (A.7.1 a A.7.4) y de desarrollo de código/aplicaciones (A.8.25 a A.8.31), en razón a que el modelo operativo de la compañía se fundamenta en esquemas de prestación de servicios 100 % remotos y en la nube, sin

administrar instalaciones de almacenamiento masivo físico de datos ni ejecutar desarrollo informático interno.

Entre las categorías de controles priorizados en la SoA se destacan:

- Gestión de activos de información: Inventario e identificación de plataformas (P-STE-11 / F-STE-11).
- Control de acceso y privilegios: Gestión de identidades y accesos (P-STE-02 / MT-STE-02).
- Gestión de incidentes de seguridad: Procedimiento de respuesta y notificación (P-STE-08).
- Seguridad en relaciones con proveedores: Criterios de evaluación y seguridad en compras (P-SGI-04).
- Respaldo y continuidad: Copias de seguridad y recuperación de información (P-STE-04).
- Concientización y formación: Programas de cultura en seguridad de la información (P-RH-02).

La estructura del Anexo C SOA-SGI-01 DECLARACIÓN DE APLICABILIDAD (SoA) se encuentra detallada a través de cuatro (4) hojas independientes que organizan la información así:

- Hoja 1 — Portada: Contiene la información general, versión del documento, datos legales de Berruit S.A.S., roles de aprobación y el marco normativo legal aplicable (Ley 1581 de 2012, Ley 1273 de 2009 y Decreto 338 de 2022).
- Hoja 2 — Declaración Completa: Relaciona los 93 controles de la norma ISO/IEC 27001:2022, estableciendo su aplicabilidad (SÍ, PARCIAL, NO), la justificación técnica de la inclusión o exclusión, la correlación directa con los códigos de riesgo de la matriz MT-SGI-02, el estado de implementación (Implementado, En proceso, Planificado), el responsable asignado y las evidencias documentales asociadas.

- Hoja 3 — Plan de Acción (Plan de Acción): Consolida la hoja de ruta para la ejecución de los controles calificados *En proceso* y *Planificados*, asignando la acción requerida, el nivel de prioridad, el líder responsable y la fecha sugerida de cumplimiento.
- Hoja 4 — Contexto Estratégico (Contexto Estratégico): Vincula las oportunidades y amenazas del análisis PESTAL con las subcláusulas del Anexo A de la SoA a las que impactan directamente.

Objetivos del Sistema Integrado de Gestión y planificación para lograrlos

En cumplimiento de los requisitos establecidos en el numeral 6.2 de las normas ISO 9001:2015 e ISO/IEC 27001:2022, se definieron objetivos integrados para el Sistema Integrado de Gestión (SIG), alineados con el direccionamiento estratégico de la organización, las políticas establecidas, el contexto organizacional y las necesidades y expectativas de las partes interesadas.

La definición de estos objetivos permitió establecer una ruta de seguimiento y control orientada al fortalecimiento de la calidad del servicio, la satisfacción del cliente, la mejora continua y la protección de la información. Para ello, se estructuró un proceso de planificación y gestión de objetivos mediante el documento “F-SGI-08 Planificación y Gestión de Objetivos” en el cual se establecieron indicadores de desempeño, metas, responsables, recursos requeridos y mecanismos de seguimiento para evaluar el cumplimiento de los resultados esperados.

Los objetivos definidos fueron formulados bajo criterios medibles y alcanzables, permitiendo realizar seguimiento periódico a la eficacia del Sistema Integrado de Gestión y al desempeño de los procesos organizacionales. Asimismo, estos objetivos fueron alineados con los riesgos y oportunidades identificados previamente, garantizando coherencia entre la planificación estratégica y las acciones de control implementadas por la organización.

Dentro de los objetivos establecidos se contemplaron aspectos relacionados con el mejoramiento continuo de los procesos, el fortalecimiento de la satisfacción del cliente, la optimización de tiempos de respuesta, el cumplimiento de requisitos legales y contractuales, el fortalecimiento de la seguridad de la información y el aumento de la eficacia operativa. Cada

objetivo contó con indicadores de medición y responsables definidos, facilitando la toma de decisiones y el seguimiento por parte de la alta dirección.

En el caso específico de la seguridad de la información, los objetivos permitieron orientar acciones relacionadas con la reducción de incidentes de seguridad, fortalecimiento de controles tecnológicos, sensibilización del personal y mejora de la capacidad de respuesta frente a amenazas y vulnerabilidades. Esto permitió integrar el enfoque de seguridad de la información dentro de la estrategia general del negocio y asegurar la alineación entre el SGSI y las necesidades operacionales de Berruit S.A.S.

De igual forma, la organización estableció mecanismos de seguimiento periódico para evaluar el cumplimiento de los objetivos definidos, mediante reuniones de seguimiento y análisis de indicadores. Estos mecanismos permitieron identificar desviaciones, establecer acciones correctivas y promover la mejora continua del Sistema Integrado de Gestión.

En conclusión, Berruit S.A.S. logró establecer objetivos integrados coherentes con su estrategia organizacional y con los requisitos de las normas ISO 9001:2015 e ISO/IEC 27001:2022 (F-SGI-08 Planificación y gestión de objetivos), garantizando la planificación, seguimiento y control de las acciones necesarias para alcanzar los resultados previstos del Sistema Integrado de Gestión.

Planificación de los cambios

Se abordó el numeral 6.3 de las normas ISO 9001:2015 e ISO/IEC 27001:2022, relacionado con la planificación y control de los cambios que puedan afectar el desempeño del sistema y la operación organizacional.

Teniendo en cuenta el entorno dinámico en el que opera la organización y la constante evolución de los servicios tecnológicos y de ciberseguridad, se identificó la necesidad de establecer mecanismos formales para gestionar de manera controlada cualquier modificación relacionada con procesos, infraestructura tecnológica, servicios, recursos humanos, documentación o cambios organizacionales.

Para ello, se desarrolló el procedimiento documentado “P-SGI-02 Procedimiento para la Gestión del Cambio”, mediante el cual se definieron lineamientos para identificar, evaluar, aprobar, implementar y hacer seguimiento a los cambios que puedan generar impacto sobre la calidad del servicio, la continuidad de las operaciones y la seguridad de la información.

Este procedimiento permitió establecer criterios para analizar previamente los posibles riesgos asociados a cada cambio, considerando aspectos como disponibilidad de recursos, afectación de procesos, impacto sobre activos de información, cumplimiento de requisitos legales y continuidad operativa. Asimismo, se definieron responsables y mecanismos de aprobación que garantizan que los cambios sean implementados de manera planificada y controlada.

Dentro del alcance del procedimiento se incluyeron cambios relacionados con:

- Modificaciones tecnológicas.
- Implementación de nuevos servicios.
- Cambios en infraestructura o plataformas.
- Ajustes organizacionales.
- Actualización documental.
- Cambios en proveedores tecnológicos.
- Implementación de controles de seguridad de la información.

En el contexto del SGSI, la gestión del cambio adquiere especial relevancia, debido a que cualquier modificación tecnológica u operacional puede generar nuevas vulnerabilidades o afectar los controles de seguridad implementados. Por esta razón, el procedimiento incorporó actividades de evaluación de riesgos y validación de controles antes de la ejecución de cambios significativos.

Adicionalmente, la organización estableció mecanismos de seguimiento y verificación posterior a la implementación de los cambios (P-SGI-02 Procedimiento para la Gestión del Cambio y F-SGI-10 Solicitud de cambio al sistema de gestión integrado), permitiendo evaluar su eficacia

y determinar si se generaron impactos no previstos sobre la operación o la seguridad de la información. Este enfoque contribuyó al fortalecimiento de la mejora continua y a la reducción de incidentes derivados de cambios no controlados.

En conclusión, Berruit S.A.S. logró implementar un proceso formal para la planificación y gestión de cambios, alineado con los requisitos establecidos en el numeral 6.3 de las normas ISO 9001:2015 e ISO/IEC 27001:2022.

8.3.7. Numeral 7 – Apoyo

El Capítulo 7 define los requisitos relativos al apoyo que Berruit S.A.S debe proporcionar para el funcionamiento eficaz del SGI y el cumplimiento de los objetivos definidos. Este capítulo contempla cinco grandes áreas: la gestión de recursos, la competencia del personal, la toma de conciencia, la comunicación y el control de la información documentada.

Para Berruit S.A.S., empresa especializada en soluciones de ciberseguridad e infraestructura tecnológica, el Capítulo 7 adquiere una relevancia estratégica importante, dado que su capital humano es el principal activo de la empresa, sus procesos funcionan en gran parte del conocimiento técnico especializado, es por este motivo que adquiere relevancia garantizar una buena gestión para determinar la calidad del servicio y la protección de la información.

Recursos

Dentro de este numeral para ambas normas se exige que la organización pueda suministrar los recursos necesarios para poder establecer, implementar, mantener y mejorar de manera continua el sistema integrado de gestión (SGI). Es así como para Berruit S.A.S, la alta dirección destinó recursos financieros específicos para actividades asociadas al diseño, mantenimiento y fortalecimiento del Sistema, incluyendo la ejecución de auditorías internas y externas, procesos de formación y capacitación, desarrollo documental y seguimiento a la mejora continua, por otro lado, determinó personal en exclusividad para administrar, llevar seguimiento y medición del sistema de gestión, que en este caso es el cargo de directora administrativa (Ver manual de funciones y perfil M-RH-02), quien se fortaleció en su competencia técnica mediante la financiación de formación especializada, incluyendo estudios de maestría relacionados con la gestión

organizacional y los sistemas integrados. Esta decisión evidencia el compromiso de la dirección con el fortalecimiento de capacidades internas y con la generación de conocimiento estratégico para la sostenibilidad del SIG, la infraestructura, el ambiente para la implementación y operación de los procesos (F-DE-01).

En cuanto a recursos tecnológicos, la organización dispuso herramientas informáticas, plataformas tecnológicas y servicios cloud necesarios para el desarrollo de sus actividades operacionales y para la gestión de la información asociada al sistema. Estos recursos permiten soportar los procesos organizacionales y fortalecer la seguridad, disponibilidad y trazabilidad de la información.

En conclusión, Berruit S.A.S. logró determinar y proporcionar los recursos necesarios para la operación eficaz del Sistema Integrado de Gestión, evidenciando el compromiso de la alta dirección con la mejora continua, en cumplimiento de los requisitos establecidos por las normas ISO 9001:2015 e ISO/IEC 27001:2022. En el F-DE-01 se puede visualizar el presupuesto y el acta de designación del responsable del sistema de gestión.

Personas (Numeral 7.1.2)

Berruit ha estructurado su equipo humano a partir de un organigrama formalizado con el documento (OR-RH-01) que define la jerarquía organizacional y las relaciones de dependencia entre cargos. Como parte de este ejercicio, se estructuraron perfiles de cargo y manuales de funciones (M-RH-01 al M-RH-08) mediante los cuales se definieron las responsabilidades, competencias, habilidades y requisitos asociados a cada rol dentro de la organización. El Gerente General actúa como máxima autoridad del SGI y tiene asignada, a través del Manual de Funciones (M-RH-01) la responsabilidad de asegurar los recursos necesarios para la operación y mejora del sistema, por su parte la directora Administrativa (M-RH-02) complementa esta función gestionando los recursos humanos, coordinando auditorías y supervisando el cumplimiento de los requisitos de ambas normas.

Esta documentación permitió establecer claramente la contribución de cada cargo al desempeño del Sistema Integrado de Gestión y asegurar la asignación adecuada de responsabilidades dentro de los procesos estratégicos, misionales y de apoyo.

Infraestructura (7.1.3)

En cumplimiento de los requisitos establecidos en el numeral 7.1.3 de las normas ISO 9001:2015 e ISO/IEC 27001:2022, Berruit S.A.S. definió la infraestructura considerando las necesidades tecnológicas para prestar el servicio ofrecido, el alcance del Sistema Integrado de Gestión y los riesgos identificados durante la planificación del sistema, es así como se identificaron recursos como equipos de cómputo, dispositivos móviles, plataformas tecnológicas, servicios cloud, herramientas de monitoreo, soluciones de seguridad informática y software especializado.

Para definir el control de estos recursos, se implementó mecanismos de administración y trazabilidad mediante un inventario tecnológico centralizado usando la herramienta Microsoft Intune, cuyo registro se consolida en el archivo “F-STE-11 INVENTARIO DE ACTIVOS Y PLATAFORMAS TI”, el cual permite mantener control sobre los equipos asignados, su estado, responsables y ciclo de vida. Adicionalmente, se establecieron formatos para la entrega y asignación de herramientas de trabajo como computadores, memorias y dispositivos móviles (F-RH-04), garantizando la adecuada administración y responsabilidad sobre los activos organizacionales.

En materia de seguridad tecnológica, Berruit S.A.S fortaleció su infraestructura mediante la implementación de herramientas especializadas de protección de endpoints y monitoreo de seguridad, incluyendo soluciones antivirus y plataformas orientadas a la prevención, detección y respuesta frente a amenazas informáticas y ciberdelincuentes. Se desarrollaron procedimientos relacionados con el control de acceso a sistemas (P-STE-02), la gestión de respaldo y restauración de datos (P-SE-039, permitiendo asegurar la disponibilidad, integridad y recuperación de la información crítica para la operación.

Así mismo, se incorporaron servicios de respaldo y recuperación de datos (P-STE-03) que permiten reducir riesgos asociados a pérdida de información o interrupciones operativas. Estas actividades fortalecen la capacidad de respuesta de la organización frente a incidentes tecnológicos y contribuyen al cumplimiento de los principios de confidencialidad, integridad y disponibilidad establecidos en la seguridad de la información.

En conclusión, Berruit S.A.S. logró establecer y mantener una infraestructura tecnológica alineada con las necesidades operacionales y estratégicas.

Recursos de seguimiento y medición (7.1.5)

La norma ISO 9001:2015, en su numeral 7.1.5 Recursos de seguimiento y medición, establece que la organización debe determinar y proporcionar los recursos necesarios para asegurar resultados válidos y confiables en las actividades de seguimiento y medición. Adicionalmente, el numeral 7.1.5.2 Trazabilidad de las mediciones exige la calibración, verificación y trazabilidad metrológica de los equipos de medición cuando estos sean necesarios para demostrar la conformidad de los productos y servicios.

De acuerdo con el alcance del Sistema Integrado de Gestión definido por Berruit S.A.S. en el documento D-DE-01 Alcance del Sistema Integrado de Gestión, la organización desarrolla actividades relacionadas con la comercialización de soluciones tecnológicas, la prestación de servicios de soporte técnico, ciberseguridad, consultoría especializada en tecnologías de la información y outsourcing tecnológico. En consecuencia, se determinó que el requisito 7.1.5.2 Trazabilidad de las mediciones no es aplicable dentro del alcance del sistema, debido a que los procesos desarrollados no requieren el uso de equipos o instrumentos de medición sujetos a calibración o control metrológico.

Esta exclusión se fundamenta en que los servicios prestados se apoyan principalmente en conocimientos técnicos especializados, plataformas tecnológicas, herramientas de software y metodologías de gestión, sin que la conformidad del servicio dependa de mediciones físicas realizadas mediante instrumentos que requieran calibración certificada o trazabilidad frente a patrones nacionales o internacionales. Por lo tanto, la organización no utiliza equipos de seguimiento y medición cuya exactitud deba demostrarse mediante procesos metrológicos formales.

No obstante, la no aplicabilidad del numeral 7.1.5.2 no exime a la organización del cumplimiento del numeral 7.1.5.1 Recursos de seguimiento y medición. Por el contrario, Berruit S.A.S. dispone de herramientas tecnológicas, metodologías y procedimientos documentados que permiten realizar el seguimiento, medición y control permanente de la infraestructura tecnológica y de los servicios prestados, garantizando resultados confiables para la toma de decisiones y la evaluación del desempeño de los procesos.

En este contexto, la organización ha documentado los procedimientos P-STE-07 Procedimiento de Monitoreo de Redes y Sistemas y P-STE-20 Monitoreo y Gestión de Alertas en Sistemas de TI, los cuales constituyen elementos fundamentales para garantizar la disponibilidad, integridad y confiabilidad de los servicios tecnológicos prestados. Estos procedimientos establecen los lineamientos necesarios para supervisar de forma continua la infraestructura tecnológica, permitiendo la detección temprana de fallas operativas, incidentes de seguridad y degradaciones en el desempeño de los sistemas.

El procedimiento P-STE-07 define un marco integral para la planificación, ejecución, control y mejora continua de las actividades de monitoreo de redes y sistemas. Su aplicación abarca tanto la infraestructura tecnológica propia de la organización como la infraestructura administrada para clientes externos. Asimismo, establece métricas de desempeño, umbrales de alerta, líneas base operativas y responsabilidades específicas para los diferentes roles involucrados en el proceso, garantizando una supervisión sistemática de servidores, dispositivos de red, aplicaciones, servicios en la nube y controles de seguridad de la información. Adicionalmente, incorpora actividades de análisis de tendencias, gestión de incidentes y generación de informes que facilitan la identificación de riesgos y oportunidades de mejora.

Complementariamente, el procedimiento P-STE-20 fortalece la estrategia de monitoreo mediante la operación de plataformas especializadas como Centreon y Wazuh, destinadas al monitoreo de infraestructura y al análisis de eventos de seguridad, respectivamente. A través de estas herramientas se realiza una supervisión continua de los activos tecnológicos, clasificando las

alertas de acuerdo con su nivel de criticidad y definiendo tiempos de respuesta específicos para cada tipo de evento. Este enfoque permite optimizar la atención de incidentes, asegurar la trazabilidad de las acciones ejecutadas y fortalecer los controles internos asociados a la gestión de servicios de tecnologías de la información.

Desde la perspectiva del Sistema Integrado de Gestión, ambos procedimientos constituyen evidencia del cumplimiento del numeral 7.1.5.1 Recursos de seguimiento y medición, dado que proporcionan los recursos tecnológicos, métodos de monitoreo, criterios de evaluación, responsabilidades y registros necesarios para obtener información confiable sobre el desempeño de los servicios. Asimismo, contribuyen al cumplimiento del numeral 9.1 Seguimiento, medición, análisis y evaluación, al contemplar indicadores de desempeño, reportes periódicos, análisis de tendencias y mecanismos de evaluación que apoyan la toma de decisiones y la mejora continua organizacional.

En conclusión, aunque el requisito 7.1.5.2 Trazabilidad de las mediciones no resulta aplicable al alcance del Sistema Integrado de Gestión de Berruit S.A.S., la organización cumple con los requisitos establecidos en el numeral 7.1.5.1 Recursos de seguimiento y medición mediante la implementación de procedimientos de monitoreo y gestión de alertas que permiten controlar y evaluar el desempeño de los servicios tecnológicos. De esta manera, se asegura la disponibilidad de información objetiva para la gestión de riesgos, la continuidad operativa y la mejora continua del sistema de gestión.

Conocimiento organizacional (7.1.6)

En cumplimiento de este numeral sobre la gestión del conocimiento organizacional como recurso esencial, Berruit S.A.S abordó el cumplimiento desde dos dimensiones, por un lado, la documentación de configuraciones, cambios, incidentes y procedimientos documentados, cronogramas de capacitación y programas de formación continua, responsabilidad explícita según sus manuales de funciones, y por otro, la transferencia del conocimiento mediante los procesos de

onboarding estructurados que se describen en el numeral 7.2. Estas herramientas permiten estructuras y preservar el conocimiento relacionado con las actividades críticas de la organización y disminuir la dependencia de conocimientos individuales.

En conclusión, Berruit S.A.S. estableció mecanismos orientados a la identificación, conservación y transferencia del conocimiento, fortaleciendo la capacidad institucional para mantener la continuidad de las operaciones y asegurar el cumplimiento de los objetivos estratégicos y del Sistema Integrado de Gestión.

Competencia (7.2)

Como mecanismo de fortalecimiento de competencias, se implementaron procedimientos para el tema de selección, contratación y vinculación de personal (P-RH-01), definiendo requisitos que garantizaran contrataciones que cumplan con las competencias requeridas para el desarrollo de sus funciones. Estos procedimientos contemplan las competencias tales como experiencia, formación académica, habilidades técnicas y capacidades relacionadas con la gestión de calidad y seguridad de la información, Berruit S.A.S ha diseñado e implementado ocho Manuales de Funciones y Perfil de uno por cada rol definido en el organigrama, que constituyen el instrumento central para la gestión de competencias.

Este enfoque responde directamente al requisito normativo de determinar la competencia necesaria, ya que los perfiles definidos constituyen el estándar frente al cual se evalúa tanto la idoneidad de los candidatos durante la selección como el desempeño de los colaboradores en ejercicio.

Para los cargos técnicos del área de Soporte IT, los manuales establecen adicionalmente el requisito de certificaciones técnicas por fabricante como condición de competencia obligatoria, gestionadas por Recursos Humanos y con evidencia documentada (M-RH-01 a M-RH-08). Esta disposición es especialmente relevante para la ISO/IEC 27001:2022, que demanda personal con conocimiento demostrable en los sistemas y controles de seguridad que la organización implementa.

Estos documentos no son simples listas de verificación administrativas: están estructurados como rutas de aprendizaje que integran el conocimiento de la organización, las políticas del SGI, las herramientas de trabajo,

La norma ISO/IEC 27001:2022 establece en la cláusula A.6.3 (Concientización, educación y capacitación en seguridad de la información) que el personal debe recibir formación apropiada sobre seguridad de la información. Berruit S.A.S ha implementado procesos de onboarding específicos por cargo (Analista IT, Coordinador Soporte IT, Ejecutivos B2B, Auxiliar Mesa de Ayuda), los cuales constituyen un instrumento diferencial en la gestión de competencias, este control incluye, de forma estructurada y verificable, la revisión de políticas de seguridad, el uso correcto de contraseñas y autenticación multifactor, el reporte de incidentes y el manejo de herramientas de seguridad y trabajo, las responsabilidades del cargo y los primeros objetivos de desempeño.

Toma de conciencia (7.3)

Este numeral exige que las personas que están bajo el control de la organización sean conscientes de la política del sistema de gestión, los objetivos, su contribución a la eficacia del sistema y las consecuencias de no cumplir los requisitos, es por esta razón que en Berrutir S.A.S se implementaron actividades de sensibilización e inducción mediante procesos de onboarding y capacitaciones.

Se creo el procedimiento de capacitación (P-RH-02) y el cronograma anual de capacitaciones (CR-RH-01) para desarrollo e implementación en el año 2026, estos instrumentos operacionalizan el requisito de toma de conciencia. El cronograma, con una meta de cumplimiento del 80%, incluye cuatro actividades planificadas para la vigencia 2026:

- Inducción al Sistema de Gestión Integrado (junio 2026): orientada a todo el personal, con el objetivo de sensibilizar sobre las políticas, objetivos y responsabilidades individuales en el SGI. Responsable: directora administrativa.
- Buenas prácticas de ciberseguridad (julio 2026): orientada a todo el personal, con el objetivo de reducir riesgos por errores humanos, phishing, malware y accesos no autorizados. Responsable: Personal TI.

- Reinducción al SGI (agosto 2026): refuerzo de políticas y responsabilidades para todo el personal.
- Gestión de incidentes de seguridad de la información (septiembre 2026): orientada al Personal TI, sobre identificación, reporte y manejo de incidentes. Responsable: Coordinador TI.

El programa incluye indicadores de seguimiento (cumplimiento, cobertura y eficiencia) que permiten verificar no solo la ejecución de las actividades sino su alcance e impacto. La eficiencia se mide por la proporción de capacitaciones calificadas óptimamente, lo que exige evaluar el aprendizaje y no solo la asistencia.

Por otro lado, se creó el Acuerdo de Confidencialidad y Compromiso de Buen Uso de Activos de Información (F-RH-02) como instrumento de conciencia individual, al firmarlo, cada colaborador declara conocer y aceptar sus responsabilidades respecto a la protección de la información, el uso adecuado de los activos tecnológicos entregados y el cumplimiento de las políticas SGI.

Este documento satisface simultáneamente requisitos de las cláusulas 7.3 (toma de conciencia) y A.6.2 (términos y condiciones del empleo) del Anexo A de ISO/IEC 27001:2022.

Comunicación (7.4)

Este numeral establece que la organización debe determinar las comunicaciones internas y externas pertinentes al SGI, especificando qué se comunica, cuándo, a quién, cómo y quién comunica.

En Berruit S.A.S se formalizó el cumplimiento a través de la Matriz de Comunicaciones (MT-SGI-01) (Ver tabla 07), documento que cubre todos los procesos del SGI y define, para cada flujo de información, los cinco elementos normativamente exigidos: el contenido de la comunicación, el emisor, el receptor, el canal utilizado y la frecuencia de emisión.

Tabla 8 Matriz de comunicaciones

Proceso	Qué comunica	Quién	A quién	Frecuencia
Dirección Estratégica	Política y objetivos SGI	Gerencia	Todo el personal	Anual / cambios
Gestión Comercial	Portafolio / propuestas	Comercial	Clientes / SGI	Permanente / por proyecto
Soporte IT	Incidentes, cambios técnicos, vulnerabilidades	Soporte IT	Clientes / SGI	Según necesidad / SLA
SGI	Auditorías, riesgos, incidentes de seguridad	Resp. SGI / SGSI	Alta Dirección / Procesos	Anual / cuando aplique
Recursos Humanos	Programa de formación, competencias, concientización	RRHH / SGI	Todo el personal	Anual / ingreso

Fuente: Propia

La trazabilidad de las comunicaciones queda asegurada mediante los registros especificados de la matriz (MT-SGI-01) tales como actas, informes, registros de incidentes, listas de asistencia.

Los canales de comunicación interna utilizados en Berruit incluyen correo electrónico corporativo, Microsoft Teams, reuniones de equipo y WhatsApp para comunicaciones operativas urgentes. Para la comunicación externa con clientes se utilizan correo electrónico, la plataforma de tickets GLPI para incidentes de soporte y comunicaciones formales. Todos estos canales están referenciados en los procesos de onboarding de cada cargo, garantizando que cada colaborador los conozca y utilice desde el inicio de su vinculación.

Información documentada

La cláusula 7.5 exige que el SGI incluya la información documentada requerida por las normas y la que la organización ha determinado como necesaria para la eficacia del sistema. Dado lo anterior se creó el procedimiento para la Elaboración, Control y Actualización de Documentos del SGI (P-SGI-01) dentro de este se incorpora el manejo de la información para ser controlada, protegida, disponible y adecuada para su uso, también su distribución, acceso, recuperación, almacenamiento, conservación y disposición final, y la protección contra pérdida de confidencialidad, uso inadecuado o pérdida de integridad.

El procedimiento establece un formato corporativo con encabezado, código, versión, fechas de emisión y datos de elaboración, revisión y aprobación. Una tipología de documentos que distingue entre manuales, políticas, procedimientos, instructivos, formatos, entre otros. Un proceso de elaboración, revisión y aprobación con roles claramente asignados: la Alta Dirección aprueba documentos estratégicos; el responsable del SGI aprueba procedimientos e instructivos operativos.

Un mecanismo de control de versiones y registro de cambios que garantiza trazabilidad histórica y evita el uso no intencionado de versiones obsoletas.

Un repositorio oficial en OneDrive corporativo como único punto de distribución y consulta de documentos vigentes.

Una tabla de retención documental que establece plazos de conservación no inferiores a 10 años para documentos internos y externos, en cumplimiento de requisitos legales, normativos y contractuales. El Listado Maestro de Documentos (L-SGI-01) es el instrumento de control que consolida la totalidad de la información documentada del SGI, con identificación de proceso, área, código, versión, nombre, numeral normativo correspondiente, medio de almacenamiento, lugar de custodia, tiempo de retención, próxima revisión y responsable.

A la fecha de elaboración de este trabajo, el Listado Maestro registra más de 50 documentos vigentes distribuidos en tres categorías de procesos: Procesos Estratégicos (Dirección Estratégica y SGI), Procesos Misionales (Comercial y Soporte Técnico Externo) y Procesos de Apoyo (Recursos Humanos, Infraestructura y SST). Para el proceso de Soporte IT, el listado incluye 13

procedimientos técnicos específicos (P-ST-01 a P-ST-13), lo que evidencia el nivel de madurez documental alcanzado en el área más crítica para la gestión de seguridad de la información.

El Capítulo 7 del SGI de Berruit no opera de forma aislada respecto a los controles del Anexo A de ISO/IEC 27001:2022. La documentación implementada en este capítulo satisface directamente varios de los controles del Anexo A, particularmente los del Tema 5 (Controles Organizacionales) y el Tema 6 (Controles sobre las Personas). La tabla 9 presenta esta correspondencia:

Tabla 9 Creación documental Anexo 2 ISO/IEC 27001:2022

Control Anexo A	Título del Control	Evidencia en Berruit
A.6.1	Selección y verificación	P-RH-01 Procedimiento de Selección de Personal; perfiles definidos en manuales M-RH-01 a M-RH-08
A.6.2	Términos y condiciones del empleo	Acuerdo de Confidencialidad F-RH-02; compromisos de uso adecuado de activos firmados al inicio de la relación laboral
A.6.3	Concientización, educación y capacitación en SI	P-RH-02 + CR-RH-01: capacitaciones en SGI, ciberseguridad, phishing, malware, incidentes; onboarding por cargo
A.5.1	Políticas de SI	Política del SGI comunicada a todo el personal a través de la Matriz MT-SGI-01 y el cronograma de capacitación
A.5.2	Roles y responsabilidades de SI	Manuales de funciones M-RH-01 a M-RH-08: sección explícita de responsabilidades en seguridad de la información por cargo
A.5.9	Inventario de activos de información	Inventario de Equipos F-STE-11 INVENTARIO DE ACTIVOS Y PLATAFORMAS TI; Listado Maestro de Documentos L-SGI-01 con clasificación por proceso y tiempo de retención
A.5.10	Uso aceptable de activos	F-RH-02 y Onboarding: compromisos de uso exclusivo para fines del cargo, prohibición de software no autorizado
A.5.13	Etiquetado de la información	L-SGI-01 clasifica documentos por tipo (interno/externo), medio (digital) y tiempo de retención; P-SGI-01 define estados: vigente / obsoleto
A.5.14	Transferencia de información	MT-SGI-01: canales, frecuencias y responsables definidos por proceso; P-STE-02 regula acceso y comunicación en sistemas

A.6.4	Proceso disciplinario	F-RH-02: incumplimientos al acuerdo de confidencialidad activan acciones disciplinarias y legales
A.6.5	Responsabilidades tras cese del empleo	F-RH-02: compromisos de confidencialidad se mantienen indefinidamente después de la terminación laboral o contractual
A.8.1	Dispositivos de usuario final	Inventario de Equipos F-STE-11 INVENTARIO DE ACTIVOS Y PLATAFORMAS TI; F-RH-02 y Onboarding: devolución de activos al finalizar la relación laboral

Fuente: Creación propia

La implementación del Capítulo 7 del SGI en Berruit S.A.S. representa uno de los pilares más sólidos del sistema, en tanto aborda de manera integral los requisitos de apoyo que determinan la capacidad real de la organización para operar y mantener su SGI más allá del cumplimiento documental.

8.3.8. Numeral 8 – Operación

El capítulo 8 de las normas ISO 9001:2015 e ISO/IEC 27001:2022 constituye el núcleo operacional del Sistema de Gestión Integrado (SGI), pues traduce los compromisos estratégicos de la organización establecidos en su política, sus objetivos y su planificación en actividades concretas, controladas y medibles, es decir, la materialización operativa de la ejecución de los procesos.

Es así como en el numeral 8.1 de la ISO 9001: 2015 se exige la planificación, implementación y control de todos los procesos para cumplir con los requisitos de la prestación del servicio, por su parte la cláusula 8.1 de ISO/IEC 27001:2022 complementa esta exigencia al requerir que dicha planificación incluya la gestión de los riesgos en seguridad de la información. Asimismo, las cláusulas 8.2 y 8.3 de esta última norma, indica que se requiere una realización periódica de evaluaciones de riesgos y la implementación de planes de tratamiento que aterricen los controles seleccionados en la Declaración de Aplicabilidad (SoA).

Dado que Berruit S.A.S. desarrolla actividades relacionadas con consultoría IT, ciberseguridad, outsourcing tecnológico, soporte técnico, infraestructura y soluciones cloud, la

operación del sistema se construyó sobre tres pilares: (1) un marco procedimental robusto que abarca más de cuarenta y cinco procedimientos documentados en el proceso misional de Soporte IT Externo; (2) una metodología de gestión de riesgos que, al momento de la elaboración de este informe, identifica sesenta y un riesgos activos distribuidos en siete procesos del SGI (MT-SGI-02); y (3) una Declaración de Aplicabilidad (código SOA-SGI-01, versión 1) que registra noventa y tres controles del Anexo A de ISO/IEC 27001:2022, de los cuales setenta y ocho son aplicables, cinco de aplicación parcial y diez excluidos con justificación documentada. La implementación de esta arquitectura operacional es el objeto del presente capítulo. Ver anexo C y E.

8.1 Planificación y control operacional

La operación de Berruit SAS está articulada en tres macroprocesos que conforman el mapa del SGI: (1) Proceso Estratégico (Dirección Estratégica y Sistema de Gestión Integrado); (2) Proceso Misional (Soporte IT Externo y Comercial); (3) Procesos de Apoyo (Compras, Recursos Humanos y Soporte Técnico Interno). La planificación operacional de cada uno de estos macroprocesos se concreta en un conjunto de procedimientos, formatos, guías e instructivos que, en conjunto, constituyen la documentación del SGI.

8.1.1 Estructura Procedimental Operacional

El proceso misional de Soporte IT Externo, el más crítico para la generación de valor de la empresa, está respaldado por más de cuarenta y nueve procedimientos específicos (P-STE-01 a P-STE-49) que establecen paso a paso cómo se ejecutan las actividades del servicio de tecnología: desde la recepción y clasificación de tickets en GLPI (P-STE-01) hasta la gestión de la continuidad del negocio en escenarios de crisis (P-STE-24), pasando por la gestión de accesos (P-STE-02), los respaldos de datos (P-STE-03), la gestión de parches (P-STE-05), el control de cambios en el entorno TI (P-STE-06), la gestión de contraseñas (P-STE-08), la gestión de inventario de activos (P-STE-11), la gestión de incidentes de seguridad (P-STE-09) y el control de vulnerabilidades (P-STE-27), entre otros.

El procedimiento P-STE-01 (Procedimiento de Soporte IT) es el de mayor importancia del proceso misional. Define tres niveles de soporte diferenciados por complejidad y escalamiento: el Nivel 1 corresponde a la mesa de ayuda para incidentes de bajo impacto; el Nivel 2 atiende

requerimientos técnicos de complejidad media que requieren diagnóstico especializado; y el Nivel 3 gestiona incidentes críticos que demandan intervención de ingenieros senior o proveedores externos. Este procedimiento integra referencias explícitas a ISO 9001:2015, ISO/IEC 27001:2022, la Ley 1581 de 2012 (protección de datos personales), la Ley 1273 de 2009 (delitos informáticos) y el marco ITIL v4 (Infraestructura de Tecnologías de la Información), marco de buenas prácticas más reconocido a nivel mundial para la Gestión de Servicios de TI, evidenciando la alineación normativa de la operación.

8.1.2 Planificación de la seguridad de la información

La planificación inicia con la Política de Seguridad de la Información y Ciberseguridad (PO-STE-01), que establece los principios de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad como pilares de la gestión informacional. Esta política es complementada por la Política del Sistema de Gestión Integrado, que alinea los objetivos de calidad con los objetivos de seguridad.

La planificación operacional de la seguridad se materializa en una arquitectura de controles técnicos y organizacionales que incluye: la segmentación de redes mediante VLANs y DMZ (P-STE-38), la gestión de accesos privilegiados con KeePass bajo cifrado AES-256 (P-STE-08, P-STE-26), la autenticación multifactor obligatoria en plataformas críticas (Microsoft 365, Azure, SharePoint), la monitorización continua mediante SIEM Wazuh y la plataforma de supervisión Centreon, la gestión de endpoints con soluciones EDR y Fortinet, y la aplicación de políticas de dispositivos móviles bajo un esquema BYOD con cumplimiento MDM. Cada uno de estos controles está respaldado por un procedimiento documentado que define roles, responsabilidades, frecuencias de ejecución y evidencias requeridas.

La Guía de Privilegio Mínimo por Rol (G-STE-01) complementa este esquema al definir, para cada rol organizacional, el conjunto mínimo de permisos necesarios para ejercer sus funciones, en alineación con los controles A.5.15, A.5.18 y A.8.2 del Anexo A de ISO/IEC 27001:2022. La Matriz de Permisos por Rol y Plataforma (MT-STE-02) traduce estos principios en un control operativo que registra el estado de acceso de cada usuario a cada plataforma del ecosistema TI de la empresa.

8.1.3 Comunicación operacional

Para Berruit SAS se creó un instrumento a través de la Matriz de Comunicación (MT-SGI-01), este documento define los siguientes elementos: qué se comunica, a quién, a través de qué medio, con qué frecuencia y qué evidencia debe generarse. Las comunicaciones cubren el nivel estratégico (Alta Dirección, Sistema de gestión Integrado), Misional (Comercial, Soporte Técnico Externo) y apoyo (Compras, Recursos Humanos, Soporte Técnico Interno).

Los canales de comunicación formalizados incluyen reuniones de revisión por la dirección, informes de gestión mensuales, comunicaciones mediante la plataforma de tickets GLPI, correo electrónico corporativo bajo Microsoft 365 y las encuestas de satisfacción al cliente instrumentalizadas en el formato F-STE-07 (Encuesta de Satisfacción al Cliente), que evalúa seis dimensiones: tiempo de respuesta, tiempo de resolución, claridad en la comunicación, actitud del personal técnico, efectividad de la solución implementada y facilidad de contacto con el equipo de soporte.

8.2 Requisitos para los Productos y servicios (ISO 9001:2015)

Este numeral solicita el proceso de determinación, revisión y gestión de los requisitos relacionados con los productos y servicios. Para Berruit SAS, se cumple a través del proceso comercial con el documento (P-CL.01).

8.2.1 Comunicación con el cliente

El procedimiento comercial (P-CL-01) define el ciclo completo del relacionamiento que se tiene con el cliente, desde la prospección hasta el cierre o entrega del producto o servicio. Berruit SAS dispone de modelos estandarizados de propuesta para servicios y para productos tecnológicos, garantizando la consistencia en la presentación de ofertas y la trazabilidad de los compromisos adquiridos.

La comunicación con el cliente incluye la definición explícita de los niveles de servicio acordados, formalizados en el Acuerdo de Nivel de Servicio (F-CL-01 ANS/SLA). Este

documento establece cuatro niveles de prioridad con tiempos de respuesta y resolución diferenciados: Crítico (respuesta ≤ 30 minutos, resolución ≤ 4 horas), Alto (respuesta ≤ 1 hora, resolución ≤ 8 horas), Medio (respuesta ≤ 4 horas, resolución ≤ 24 horas) y Bajo (respuesta ≤ 8 horas, resolución en hasta 5 días hábiles). El cumplimiento de estos compromisos es monitoreado de manera continua a través de la plataforma GLPI y reportado periódicamente al cliente.

8.2.2 Determinación de los requisitos para productos y servicios

La revisión de los requisitos se realiza en dos momentos: antes de asumir el compromiso de proveer el servicio (etapa comercial, bajo P-CL-01) y de manera continua durante la prestación del servicio. Cualquier modificación a los requisitos acordados activa el proceso de Gestión de Cambios en el Entorno de TI (P-STE-06), que exige la elaboración de una Solicitud de Cambio (RFC, formato F-STE-04), la evaluación de impacto técnico, la aprobación por el nivel competente y la documentación de los resultados de la implementación. Este mecanismo garantiza que los cambios en los requisitos del cliente sean procesados de manera controlada, sin riesgo de afectar otros compromisos contractuales o la integridad de los sistemas bajo administración.

8.2.3 Revisión de los requisitos para productos y servicios

La revisión de los requisitos se realiza en dos momentos: antes de asumir el compromiso de proveer el servicio (etapa comercial, bajo P-CL-01) y de manera continua durante la prestación del servicio. Cualquier modificación a los requisitos acordados activa el proceso de gestión de cambios (P-STE-06), que exige la elaboración de una solicitud de cambio (F-STE-04), la evaluación de impacto técnico, la aprobación por el nivel competente y la documentación de los resultados de la implementación. Este mecanismo garantiza que los cambios en los requisitos del cliente sean procesados de manera controlada, sin riesgo de afectar otros compromisos contractuales o la integridad de los sistemas bajo administración.

8.3 Diseño y Desarrollo de los Productos y Servicios (ISO 9001:2015)

Berruit SAS es una empresa de servicios de tecnología de la información que no desarrolla software ni productos propietarios. Su modelo de negocio se basa en la integración, configuración, administración y soporte de soluciones tecnológicas de terceros para sus clientes. Por esta razón, la cláusula 8.3 de ISO 9001:2015 tiene una aplicabilidad restringida en el contexto de la organización: no existe un proceso formal de diseño y desarrollo de producto, dado que Berruit SAS actúa como integrador de soluciones existentes.

Sin embargo, existe un proceso implícito de diseño de soluciones en la etapa de propuesta comercial, en el cual el equipo técnico define la arquitectura de la solución a implementar en el entorno del cliente, los componentes requeridos, las interdependencias y los riesgos técnicos asociados. Este proceso está respaldado por la Guía de Principios de Arquitectura Segura (G-STE-07), la Guía de Estándares de Configuración Segura (G-STE-02) y la Lista de Chequeo de Seguridad en Software (G-STE-06), que en conjunto garantizan que las soluciones propuestas e implementadas cumplan con los principios de seguridad.

Es pertinente señalar que la no aplicabilidad de los controles A.8.25 (Ciclo de vida de desarrollo seguro), A.8.26 (Requisitos de seguridad de las aplicaciones), A.8.27 (Principios de arquitectura de sistemas seguros), A.8.28 (Codificación segura), A.8.29 (Pruebas de seguridad en desarrollo y aceptación) y A.8.30 (Desarrollo externalizado) de la Declaración de Aplicabilidad (SOA-SGI-01) se fundamenta precisamente en que Berruit SAS no lleva a cabo actividades de desarrollo de software, como se documenta con justificación formal en el SoA.

8.4 Control de los Procesos, Productos y Servicios Suministrados Externamente (ISO 9001:2015)

La cláusula 8.4 de ISO 9001:2015 exige que la organización asegure que los procesos, productos y servicios suministrados externamente son conformes con los requisitos especificados. Esta cláusula adquiere especial relevancia para Berruit SAS dado que el modelo operativo de la compañía depende significativamente de proveedores de software, hardware y servicios de nube, cuya calidad y seguridad afectan directamente la prestación del servicio al cliente final.

8.4.1 Generalidades

El Procedimiento de Compras (P-CM-01) integra explícitamente los requisitos de ISO 9001:2015 (cláusula 8.4) y de ISO/IEC 27001:2022 (cláusula 8.1 y controles del Anexo A relativos a seguridad en la cadena de suministro), garantizando que los criterios de selección y evaluación de proveedores incluyan criterios tanto de calidad como de seguridad de la información.

El Formato de Selección y Evaluación de Proveedor (F-CM-01) instrumentaliza este proceso mediante un sistema de puntuación sobre cien puntos que evalúa ocho criterios: reconocimiento de marca (30 puntos), certificación SGSST —Sistema de Gestión de Seguridad y Salud en el Trabajo— (10 puntos), garantía de suministro (10 puntos), política de devoluciones (10 puntos), precio (20 puntos), condiciones de pago (10 puntos), experiencia en el sector (5 puntos) y personal calificado (5 puntos). Los proveedores que no superan el umbral mínimo de puntuación no son habilitados para ser incluidos como proveedores.

También se cuenta con el formato de Confidencialidad de Proveedores y Terceros (F-CM-05) que formaliza los compromisos de seguridad de la información con los proveedores que tienen acceso a información sensible o a los entornos tecnológicos administrados por Berruit SAS, en alineación con el control A.5.19 (Seguridad de la información en las relaciones con proveedores) del Anexo A de ISO/IEC 27001:2022.

8.4.2 Tipo y Alcance del Control

El control sobre los proveedores se ejerce en tres momentos del ciclo de vida: la selección inicial (F-CM-01), la verificación de calidad durante la entrega de productos (P-CM-06) y la reevaluación periódica del desempeño del proveedor (F-CM-04). El Procedimiento de Verificación de Calidad durante la Entrega de Productos (P-CM-06) es particularmente relevante dado que Berruit SAS no dispone de almacén propio: los productos tecnológicos son entregados directamente desde el proveedor al cliente final, lo que exige un proceso de verificación en el punto de entrega que garantice la conformidad con las especificaciones acordadas. El Acta de Entrega (F-CM-02) y la Orden de Compra (F-CM-03) formalizan estos procesos y generan la evidencia documentada requerida por el SGI.

8.4.3 Información para los Proveedores Externos

Berruit SAS comunica a sus proveedores, antes del inicio de las relaciones comerciales, los requisitos de calidad y seguridad que deben cumplir, incluyendo: especificaciones técnicas de productos, condiciones de embalaje y transporte, requisitos de garantía, criterios de aceptación y rechazos, y compromisos de confidencialidad. La Orden de Compra (F-CM-03) actúa como el instrumento contractual que materializa esta comunicación, mientras que la Reevaluación de Proveedor (F-CM-04) cierra el ciclo de retroalimentación con datos objetivos de desempeño.

8.5 - Producción y Provisión del Servicio (ISO 9001:2015)

La cláusula 8.5 de ISO 9001:2015 regula las condiciones bajo las cuales se realiza la producción y la provisión del servicio, incluyendo la disponibilidad de información documentada, el uso de recursos de seguimiento y medición, la gestión de la propiedad del cliente y la prevención de la contaminación. Para Berruit SAS, la provisión del servicio de soporte IT externo es la actividad principal que genera valor para el cliente y que moviliza la totalidad de los recursos organizacionales.

8.5.1 Control de la Producción y de la Provisión del Servicio

El control de la provisión del servicio de soporte IT en Berruit SAS se ejerce principalmente a través del Procedimiento de Soporte IT (P-STE-01), que establece el flujo operativo completo desde la recepción del requerimiento hasta su resolución y documentación. La plataforma GLPI actúa como el sistema de gestión de tickets que registra, clasifica, asigna, escala y cierra todos los requerimientos, garantizando la trazabilidad completa de cada intervención técnica.

El proceso de soporte contempla cuatro tipos de requerimientos: incidentes (interrupciones no planificadas del servicio), requerimientos (solicitudes de cambio o instalación), solicitudes informativas (consultas técnicas) y alertas de ciberseguridad (eventos detectados por las herramientas de monitorización). Cada tipo de requerimiento sigue un flujo diferenciado de atención, con tiempos de respuesta y resolución definidos en el Acuerdo de Nivel de Servicio (F-CL-01) y monitoreados de manera continua en GLPI.

Los controles técnicos que respaldan la provisión del servicio incluyen: la gestión de accesos basada en mínimo privilegio (P-STE-02, G-STE-01), la gestión de contraseñas con KeePass AES-256 y MFA (P-STE-08), la monitorización continua de la infraestructura con Centreon y Wazuh (P-STE-35), la gestión de inventario de activos TI (P-STE-11, F-STE-11), la segmentación de redes con VLANs y DMZ (P-STE-38), el filtrado de contenido web (P-STE-40) y la gestión de firewalls e IDS/IPS con Fortinet (P-STE-37).

El Cronograma de Mantenimiento (CR-STE-01) planifica las intervenciones preventivas periódicas sobre la infraestructura tecnológica de los clientes, incluyendo actualizaciones de firmware, limpieza de equipos, verificación de respaldos y revisión de configuraciones de seguridad. Este cronograma es gestionado en coordinación con los responsables técnicos del cliente y validado contra los acuerdos de nivel de servicio para minimizar el impacto operacional de las intervenciones.

8.5.2 Identificación y Trazabilidad

La trazabilidad de la prestación del servicio es garantizada por la plataforma GLPI, que asigna un número único de ticket a cada requerimiento y registra el historial completo de intervenciones, responsables, tiempos de atención, soluciones aplicadas y evidencias documentadas. El Inventario de Activos y Plataformas TI (F-STE-11) complementa esta trazabilidad al registrar, para cada activo bajo administración, sus características técnicas y estado operacional.

La identificación de los activos de información gestionados por Berruit SAS para sus clientes sigue el marco del Procedimiento de Control de Inventario de Activos de IT (P-STE-11), alineado con los controles A.5.9 (Inventario de activos de información), A.8.1 (Dispositivos de usuario final) y A.8.8 (Gestión de vulnerabilidades técnicas) del Anexo A de ISO/IEC 27001:2022.

8.5.3 Propiedad Perteneciente a los Clientes o Proveedores Externos

Berruit SAS gestiona, en el marco de sus servicios, activos tecnológicos y datos que son propiedad de sus clientes. El P-STE-01 establece que todo acceso a los entornos tecnológicos del cliente debe estar autorizado formalmente, documentado y restringido al mínimo necesario para la ejecución del requerimiento. El Formato de Solicitud de Acceso (F-STE-03) formaliza este proceso de autorización. Los Acuerdos de Confidencialidad y Compromiso de Uso Adecuado de

los Activos de Información (F-RH-02) suscritos por todo el personal técnico de Berruit SAS extienden estas obligaciones de cuidado y confidencialidad al ámbito laboral, incluyendo obligaciones post-empleo.

En materia de respaldo de datos, el Procedimiento de Respaldo y Restauración de Datos (P-STE-03) establece los protocolos para la gestión de copias de seguridad de los entornos de clientes, utilizando soluciones como Veeam, Acronis y Azure Backup, con rutas de respaldo documentadas en el Listado de Rutas de Backups (L-STE-01). La Política de Seguridad de la Información (PO-STE-01) garantiza que los datos de los clientes son tratados con los más altos estándares de confidencialidad, en cumplimiento de la Ley 1581 de 2012 de Protección de Datos Personales.

8.5.4 Preservación

La preservación de la conformidad del servicio durante la prestación se garantiza a través de múltiples mecanismos complementarios. La gestión de parches y actualizaciones de seguridad (P-STE-05) asegura que los sistemas bajo administración se mantienen en el nivel de parchado requerido por los fabricantes y por las políticas de seguridad del SGI. La gestión de cambios en el entorno TI (P-STE-06) controla que cualquier modificación al entorno tecnológico del cliente sea evaluada, aprobada y documentada antes de su implementación, mediante la emisión de una Solicitud de Cambio (RFC, F-STE-04). El Procedimiento de Gestión de Configuraciones Seguras (P-STE-30) establece las líneas base de configuración segura para los sistemas y dispositivos administrados, en alineación con el control A.8.9 del Anexo A de ISO/IEC 27001:2022.

8.5.5 Actividades Posteriores a la Entrega

Las actividades posteriores a la entrega del servicio en Berruit SAS incluyen: el seguimiento del cumplimiento de los SLA acordados, la aplicación de la Encuesta de Satisfacción al Cliente (F-STE-07), la gestión de PQRSF mediante el Procedimiento P-SGI-03, y el procesamiento de devoluciones de productos tecnológicos según el Procedimiento de Devolución de Productos (P-SGI-05) y el formato de Nota de Devolución (RMA, F-SGI-04). Estas actividades cierran el ciclo de calidad del servicio y generan los insumos para la mejora continua del SGI.

8.5.6 Control de los Cambios

El control de cambios en la operación de Berruit SAS es gestionado por el Procedimiento de Gestión de Cambios en el Entorno de TI (P-STE-06), que establece las categorías de cambio (estándar, menor, mayor y de emergencia), los niveles de aprobación requeridos, las pruebas previas a la implementación y los procedimientos de reversión en caso de fallo. Este procedimiento está alineado con el control A.8.32 (Gestión de cambios) del Anexo A de ISO/IEC 27001:2022 y con la cláusula 8.1 de ISO 9001:2015 relativa al control de cambios planificados. El formato F-STE-04 (Formato RFC — Request for Change) es el instrumento documentado que registra cada cambio, su evaluación de riesgo, el plan de implementación, los responsables y la evidencia de aprobación.

8.6 Liberación de los Productos y Servicios (ISO 9001:2015)

La cláusula 8.6 de ISO 9001:2015 establece que la organización debe implementar las disposiciones planificadas en las etapas adecuadas para verificar que se cumplen los requisitos de los productos y servicios antes de ser liberados al cliente. En el contexto de Berruit SAS, la liberación del servicio se produce cuando el requerimiento atendido es verificado técnicamente, documentado en GLPI y validado por el cliente, proceso que genera la evidencia de conformidad exigida por la norma.

La liberación del servicio de soporte IT está condicionada al cumplimiento de los siguientes criterios de aceptación: (1) la solución implementada resuelve el problema reportado en los términos del ticket de GLPI; (2) la intervención no introduce nuevas vulnerabilidades ni degradaciones en el entorno del cliente; (3) los tiempos de respuesta y resolución son conformes con el SLA vigente; (4) el técnico responsable documenta las acciones realizadas, herramientas utilizadas y configuraciones modificadas en el registro del ticket; y (5) el cliente o su representante técnico valida la solución antes del cierre formal del ticket.

Para la liberación de productos tecnológicos, el Procedimiento de Verificación de Calidad durante la Entrega de Productos (P-CM-06) establece los criterios de inspección en el punto de entrega, y el Acta de Entrega (F-CM-02) registra la conformidad del producto con las especificaciones de la orden de compra (F-CM-03). Esta cadena documental garantiza la trazabilidad completa desde el pedido hasta la entrega y la aceptación formal por parte del cliente.

La Encuesta de Satisfacción al Cliente (F-STE-07) actúa como instrumento complementario de verificación de la conformidad del servicio percibida por el cliente. Los resultados de estas encuestas son analizados periódicamente por la Dirección de Calidad y reportados en el Informe de Indicadores del proceso SGI, alimentando el ciclo de mejora continua del sistema.

8.7 Control de las Salidas No Conformes (ISO 9001:2015)

La cláusula 8.7 de ISO 9001:2015 exige que la organización identifique y controle las salidas no conformes para prevenir su uso o entrega no intencional. En Berruit SAS, este requisito se gestiona a través del Procedimiento para el Control de Salidas No Conformes, No Conformidades y Acciones Correctivas (P-SGI-04), que integra los requisitos de la cláusula 8.7 de ISO 9001:2015 con los de la cláusula 10.1 de ISO 9001:2015, la cláusula 10.2 de ISO 9001:2015 y la cláusula 10.1 de ISO/IEC 27001:2022.

El P-SGI-04 establece que una salida no conforme se produce cuando el resultado de un proceso no cumple con los criterios de aceptación definidos, ya sea por incumplimiento de los requisitos del cliente, incumplimiento de los estándares de seguridad del SGI o incumplimiento de los SLA acordados. Las salidas no conformes identificadas se registran en el Formato de Salidas No Conformes (F-SGI-03) y son sometidas a uno de los siguientes tratamientos: corrección inmediata (en el caso de salidas corregibles), contención (aislamiento de la salida para evitar daños adicionales), comunicación al cliente (cuando la no conformidad afecta los compromisos contractuales) o inicio de un proceso formal de acción correctiva.

El alcance del P-SGI-04 abarca explícitamente los incidentes de seguridad de la información, lo que establece un vínculo formal entre el sistema de gestión de calidad y el sistema de gestión de seguridad de la información. Un incidente de seguridad detectado a través del SIEM Wazuh, del sistema IDS/IPS Fortinet o de las herramientas EDR puede generar simultáneamente una salida no conforme (bajo ISO 9001 8.7) y un evento de seguridad a gestionar bajo el Procedimiento de Respuesta ante Incidentes de Seguridad en TI (P-STE-09). Este procedimiento integra la respuesta técnica (contención, erradicación, recuperación) con los requisitos documentales del SGI y la coordinación con los planes de continuidad del negocio (P-STE-24).

El ciclo completo de gestión de no conformidades incluye: la identificación y registro de la no conformidad, el análisis de causa raíz (utilizando metodologías como los 5 por qué o el diagrama de Ishikawa), la definición e implementación de acciones correctivas, el seguimiento de la eficacia de las acciones implementadas y el cierre formal de la no conformidad con evidencia documentada. El Indicador de Conformidad del proceso SGI establece como meta que al menos el 95% de las acciones correctivas sean implementadas dentro del plazo definido y que al menos el 95% de las no conformidades sean resueltas satisfactoriamente.

8.2 Evaluación de los Riesgos de Seguridad de la Información (ISO/IEC 27001:2022)

La cláusula 8.2 de ISO/IEC 27001:2022 establece que la organización debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se proponga u ocurra cambios significativos, tomando como referencia los criterios establecidos en la cláusula 6.1.2. Esta cláusula es uno de los pilares más exigentes de la norma, ya que requiere no solo la ejecución de la evaluación sino la conservación de los resultados como información documentada que demuestre la capacidad de la organización para gestionar sus riesgos de manera sistemática y reproducible.

8.2.1 Metodología de Evaluación de Riesgos

Berruit SAS ha adoptado una metodología de evaluación de riesgos basada en el análisis probabilístico del binomio Probabilidad $\times$ Impacto ($P \times I$), implementada en la Matriz de Riesgos del SGI (MT-SGI-02). La metodología utiliza escalas cuantitativas de 1 a 5 para cada variable, generando un valor de riesgo inherente en el rango de 1 a 25. El umbral de aceptabilidad del riesgo está definido de la siguiente manera: riesgos con valor entre 1 y 12 son clasificados como Aceptables (susceptibles de aceptación con controles existentes), mientras que riesgos con valor entre 13 y 25 son clasificados como Inaceptables (requieren tratamiento mediante controles adicionales o acciones correctivas).

La evaluación cubre los siete procesos del mapa del SGI: Sistema de Gestión Integrado, Dirección Estratégica, Soporte IT Externo, Comercial, Compras, Recursos Humanos y Soporte Técnico Interno. La evaluación es realizada por los responsables de cada proceso con el apoyo de

la Dirección Administrativa, y los resultados son revisados por la Alta Dirección en el marco de las revisiones del sistema.

8.2.2 Resultados de la Evaluación de Riesgos

Al momento de elaboración de este informe, la Matriz de Riesgos del SGI (MT-SGI-02) registra sesenta y un (61) riesgos activos distribuidos en los siete procesos del SGI. La Tabla 13 presenta el resumen de la distribución de riesgos por proceso y nivel de criticidad.

Tabla 10 Distribución de riesgos por proceso y nivel de criticidad

Proceso	Total Riesgos	Aceptables	Inaceptables	Críticos (V≥20)	% Inaceptables
Sistema de Gestión Integrado	9	4	5	1	55.6%
Dirección Estratégica	7	4	3	0	42.9%
Soporte IT Externo	14	6	8	3	57.1%
Comercial	8	4	4	1	50.0%
Compras	8	5	3	1	37.5%
Recursos Humanos	7	4	3	0	42.9%
Soporte Técnico Interno	8	4	4	0	50.0%
TOTAL	61	31	30	6	49.2%

Fuente: Elaboración propia

Los resultados de la evaluación revelan un perfil de riesgo que demanda atención prioritaria: el 49.2% de los riesgos identificados se clasifican como Inaceptables, lo que indica que cerca de la mitad de los riesgos del portafolio superan el umbral de aceptabilidad definido por la Alta Dirección. Adicionalmente, seis riesgos presentan valores iguales o superiores a 20 (en la escala de 25), posicionándose en la categoría de riesgos críticos que exigen tratamiento urgente. El proceso de Soporte IT Externo concentra la mayor cantidad de riesgos totales (14) e inaceptables

(8), lo cual es consistente con la naturaleza de alta exposición informacional que caracteriza la prestación de servicios de ciberseguridad y administración de infraestructura tecnológica para clientes externos.

Entre los riesgos críticos identificados destacan: la exfiltración de datos sensibles de clientes ($P \times I = 25$, Soporte IT), la indisponibilidad prolongada de sistemas críticos por ransomware ($P \times I = 20$, Soporte IT), el acceso no autorizado a entornos productivos de clientes ($P \times I = 20$, Soporte IT) y la pérdida de confidencialidad de propuestas comerciales ($P \times I = 20$, Comercial). Estos riesgos son objeto de planes de tratamiento específicos que articulan controles técnicos, procedimentales y organizacionales del SGI.

8.3 Tratamiento de los Riesgos de Seguridad de la Información (ISO/IEC 27001:2022)

La cláusula 8.3 de ISO/IEC 27001:2022 establece que la organización debe implementar el plan de tratamiento de riesgos de seguridad de la información definido en la cláusula 6.1.3, conservando los resultados como información documentada. El tratamiento de riesgos en Berruit SAS sigue cuatro opciones estratégicas: mitigación (implementación de controles que reducen la probabilidad o el impacto del riesgo), transferencia (contratación de seguros o tercerización de la gestión del riesgo), aceptación (cuando el costo del tratamiento supera el beneficio) y evitación (eliminación de la actividad que genera el riesgo).

La estrategia predominante es la mitigación a través de controles del Anexo A de ISO/IEC 27001:2022, seleccionados en función de su pertinencia para los riesgos identificados y documentados en la Declaración de Aplicabilidad (SOA-SGI-01). La efectividad de los controles implementados es monitoreada periódicamente a través de los indicadores de gestión definidos en el proceso SGI y revisada en las evaluaciones de riesgos subsiguientes.

8.3.1 Controles de Tratamiento Implementados

El tratamiento de los riesgos inaceptables identificados en MT-SGI-02 se instrumentaliza a través de un conjunto articulado de controles técnicos y procedimentales. Los más relevantes, organizados por las categorías del Anexo A de ISO/IEC 27001:2022, son los siguientes:

En materia de controles organizacionales (Anexo A.5), Berruit SAS ha implementado: políticas de seguridad de la información (PO-STE-01), definición de roles y responsabilidades de seguridad (M-RH-01 a M-RH-08), separación de funciones para usuarios privilegiados (P-STE-26, G-STE-01), gestión de activos de información (P-STE-11), acuerdos de confidencialidad con empleados y terceros (F-RH-02, F-CM-05), gestión de la seguridad en la cadena de suministro (P-CM-01, F-CM-01), gestión de incidentes de seguridad de la información (P-STE-09), y gestión de la continuidad del negocio (P-STE-24).

En materia de controles para las personas (Anexo A.6), se han implementado: verificación de antecedentes en el proceso de selección de personal (P-RH-01), términos y condiciones de empleo que incluyen obligaciones de seguridad de la información (F-RH-02), concienciación, educación y formación en seguridad de la información (P-RH-02, CR-RH-01), procesos disciplinarios documentados para violaciones de seguridad (P-SGI-04), y gestión segura del cese o cambio de empleo incluyendo la revocación de accesos (P-STE-02).

En materia de controles físicos (Anexo A.7), y considerando que Berruit SAS opera en modalidad de trabajo remoto sin instalaciones físicas propias, se han implementado controles adaptados a este contexto: políticas para trabajo remoto y BYOD (PO-STE-01), gestión de dispositivos móviles con MDM (F-STE-11), y protección del puesto de trabajo en entornos de trabajo remoto. Los controles A.7.3 (Asegurar las oficinas, despachos e instalaciones), A.7.4 (Supervisión de la seguridad física) y A.7.12 (Cableado de seguridad) han sido excluidos del SoA con justificación basada en la ausencia de instalaciones físicas propias de la organización.

En materia de controles tecnológicos (Anexo A.8), que constituyen el núcleo del tratamiento de riesgos en una organización de servicios TI, Berruit SAS ha implementado o está implementando: gestión de dispositivos de usuario final (F-STE-11, P-STE-11), gestión de accesos privilegiados (P-STE-26, P-STE-08), restricción de acceso a la información (P-STE-02, MT-STE-02, G-STE-01), autenticación segura con MFA (P-STE-08), protección contra software malicioso con EDR (P-STE-29), gestión de eventos de seguridad con SIEM Wazuh (P-STE-35), filtrado web (P-STE-40), gestión de vulnerabilidades (P-STE-27), gestión de la configuración (P-STE-30), eliminación segura de información (P-STE-32), enmascaramiento de datos (P-STE-33), prevención de fugas de datos DLP (P-STE-34), monitorización de redes (P-STE-35), gestión de

firewalls e IDS/IPS (P-STE-37), segmentación de redes con VLANs y DMZ (P-STE-38), y criptografía (P-STE-41, G-STE-05).

8.4 Declaración de Aplicabilidad (Statement of Applicability — SoA) (ISO/IEC 27001:2022)

La Declaración de Aplicabilidad constituye uno de los documentos más relevantes del SGSI, ya que sintetiza las decisiones de tratamiento de riesgos de la organización en relación con los noventa y tres controles del Anexo A de ISO/IEC 27001:2022. La SoA de Berruit SAS (código SOA-SGI-01, versión 1, fecha de elaboración 16 de mayo de 2026) fue elaborada por el director del SGI y aprobada por el Gerente General, y establece para cada control: si es aplicable o no, la justificación de la decisión, el estado de implementación y la referencia a los documentos del SGI que lo soportan. Ver SOA-SGI-01 DECLARACIÓN DE APLICABILIDAD (SoA).

8.4.1 Estadísticas de la Declaración de Aplicabilidad

La Tabla 11 sintetiza el diagnóstico de aplicabilidad y el estado de implementación de los 93 controles de seguridad de la información establecidos en el Anexo A de la norma ISO/IEC 27001:2022 para Berruit S.A.S.

El análisis estadístico de la Declaración de Aplicabilidad (SoA) evidencia que Berruit S.A.S. ha definido una cobertura del 89.2 % de los controles del Anexo A de la ISO/IEC 27001:2022 (78 aplicables y 5 parciales), declarando 10 exclusiones justificadas en materia física y tecnológica (10.8 %) en coherencia con su modelo operativo en la nube. Asimismo, el estado de avance refleja una fase sólida de transición: mientras que el 16.1 % de los controles ya se encuentra completamente implementado, el 55.9 % se halla en proceso activo de ejecución y un 17.2 % queda proyectado en fase de planificados, garantizando un marco estructurado hacia la consolidación total de la ciberseguridad en la organización.

Tabla 11 Resumen estadístico de la declaración de aplicabilidad

Categoría	Total	Aplicables	Parciales	Excluidos	Implementados	En Proceso	Planificados
-----------	-------	------------	-----------	-----------	---------------	---------------	--------------

A.5 Organizacionales	37	37	0	0	6	22	9
A.6 Personas	8	8	0	0	2	6	0
A.7 Físicos	14	6	5	3	2	6	3
A.8 Tecnológicos	34	27	0	7	5	18	4
TOTAL	93	78	5	10	15	52	16

Fuente: Elaboración propia

8.4.2 No aplicabilidad de controles

La SoA (SOA-SGI -01) documenta la no aplicabilidad de diez controles del Anexo A de ISO/IEC 27001:2022, con las siguientes justificaciones:

Tres controles de la categoría A.7 (Controles físicos) son no aplicables por ausencia de instalaciones físicas propias: A.7.3 (Asegurar oficinas, despachos e instalaciones), A.7.4 (Supervisión de la seguridad física) y A.7.12 (Seguridad del cableado). Berruit SAS opera en modalidad de trabajo remoto distribuido, sin una sede física que requiera los controles de seguridad perimetral y ambiental contemplados en estos apartados del Anexo A.

Siete controles de la categoría A.8 (Controles tecnológicos) son no aplicables por ausencia de actividades de desarrollo de software propio: A.8.4 (Acceso al código fuente), A.8.25 (Ciclo de vida de desarrollo seguro), A.8.26 (Requisitos de seguridad de las aplicaciones), A.8.27 (Principios de arquitectura de sistemas seguros), A.8.28 (Codificación segura), A.8.29 (Pruebas de seguridad en desarrollo y aceptación) y A.8.30 (Desarrollo externalizado). Como integrador de soluciones tecnológicas de terceros, Berruit SAS no desarrolla código ni mantiene repositorios de software propietario que requieran la aplicación de estos controles.

8.4.3 Estado de Implementación y Plan de Acción

El estado de implementación de los controles aplicables de la SoA refleja la madurez del SGSI en el momento de elaboración de este informe: doce controles (14.45%) están

completamente implementados, cincuenta y cinco (66.26%) están en proceso de implementación y dieciséis (18%) están planificados para implementación futura. Este perfil es coherente con una organización que se encuentra en la fase de implementación inicial de su SGSI y que ha optado por una estrategia de implementación escalonada basada en la priorización de riesgos.

La hoja 'Plan de Acción' de la SoA (SOA-SGI-01) detalla, para cada control pendiente de implementación, el responsable designado, la prioridad asignada (Alta, Media, Baja) y la fecha límite de implementación. Los controles con mayor impacto sobre los riesgos críticos identificados en MT-SGI-02 han sido priorizados con clasificación Alta, garantizando que los recursos organizacionales se concentren en las áreas de mayor exposición al riesgo.

8.5 Gestión de la Continuidad del Negocio (ISO/IEC 27001:2022)

El Procedimiento de Continuidad del Negocio (P-STE-24) establece el marco para la gestión de la continuidad operacional de Berruit SAS y de sus clientes en escenarios de interrupción. Siguiendo los principios del Business Continuity Management (BCM), el procedimiento contempla: la identificación y análisis de amenazas (eventos de fuerza mayor, ciberataques, fallos de infraestructura, pérdida de personal clave), el Análisis de Impacto en el Negocio (BIA), el diseño de estrategias de continuidad diferenciadas por nivel de criticidad del servicio, la definición de objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) por proceso, la coordinación con los planes de respaldo de datos (P-STE-03) y la activación de los SLA con clientes en situaciones de contingencia.

La articulación entre la continuidad del negocio (P-STE-24) y la respuesta ante incidentes de seguridad (P-STE-09) garantiza que los eventos de ciberseguridad que afectan la continuidad operacional sean gestionados de manera integrada, evitando respuestas fragmentadas que puedan agravar el impacto del incidente. El Procedimiento de Respuesta ante Incidentes (P-STE-09) integra las fases de detección (SIEM Wazuh, IDS Fortinet), contención, erradicación, recuperación y lecciones aprendidas, con la documentación forense requerida para el análisis post-incidente y la eventual presentación ante autoridades competentes.

8.6 Seguridad del Talento Humano en la Operación del SGI (ISO/IEC 27001:2022)

La dimensión humana de la seguridad de la información es gestionada en Berruit SAS a través de un ciclo integral que abarca desde la selección del personal hasta la terminación de la relación laboral. El Procedimiento de Selección de Personal (P-RH-01) incorpora la verificación de antecedentes y la evaluación de competencias de seguridad como criterios de selección, en alineación con los controles A.6.1 (Selección) y A.6.2 (Términos y condiciones de empleo) del Anexo A de ISO/IEC 27001:2022.

Los perfiles de cargo de los ocho roles organizacionales (Gerente General, Director Administrativo, Director Comercial, Ejecutivo B2B, Analista de Prospección, Analista IT, Coordinador de Soporte IT y Auxiliar de Mesa de Ayuda), documentados en M-RH-01 a M-RH-08, definen explícitamente las competencias de seguridad requeridas para cada rol, articulando los requisitos de la cláusula 7.2 (Competencia) de ISO 9001:2015 con los controles de seguridad asociados a personas del Anexo A de ISO/IEC 27001:2022.

El Procedimiento de Capacitación (P-RH-02) y el Cronograma de Capacitación (CR-RH-01) instrumentalizan el programa de concienciación y formación en seguridad de la información, que incluye: inducción al SGI para nuevos empleados, formación en seguridad de la información y ciberseguridad, entrenamiento en los procedimientos del proceso de Soporte IT Externo, y formación técnica especializada para el personal de ingeniería. El cumplimiento del programa de capacitación es registrado en las Listas de Asistencia (L-RH-01) y monitorizado a través de los indicadores del proceso de Recursos Humanos.

El Acuerdo de Confidencialidad y Compromiso de Uso Adecuado de los Activos de Información (F-RH-02) es suscrito por todos los empleados al inicio de la relación laboral y establece obligaciones de confidencialidad de carácter indefinido respecto a la información y los activos tecnológicos gestionados por Berruit SAS, incluyendo los datos de los clientes. Este acuerdo implementa el control A.6.6 (Acuerdos de confidencialidad o no divulgación) del Anexo A de ISO/IEC 27001:2022 y es consistente con los requisitos de la Ley 1581 de 2012 de Protección de Datos Personales.

El proceso de desvinculación laboral incluye la revocación inmediata de todos los accesos del empleado a los sistemas de información de Berruit SAS y de sus clientes (P-STE-02), la entrega

de los activos tecnológicos asignados (verificada contra el inventario F-STE-11) y la entrega de las contraseñas de cuentas privilegiadas gestionadas durante el período de empleo. La Política de Seguridad de la Información (PO-STE-01) establece que los accesos privilegiados a entornos de clientes deben ser rotados inmediatamente tras la desvinculación de cualquier empleado con acceso a dichos entornos.

8.7 Gestión de PQRSF (ISO 9001:2015 e ISO/IEC 27001:2022)

El Procedimiento para el Manejo de PQRSF (P-SGI-03) establece el proceso para la recepción, registro, seguimiento y respuesta a Peticiones, Quejas, Reclamos, Sugerencias y Felicitaciones provenientes de clientes, usuarios, empleados o partes interesadas externas. Los canales habilitados para la recepción de PQRSF incluyen el formulario web en www.berruit.com y los canales de correo electrónico corporativo, garantizando accesibilidad y trazabilidad de cada comunicación recibida.

Cada PQRSF recibida es registrada en el Formato de Registro de PQRSF (F-SGI-02), asignada a un responsable de gestión y atendida dentro de los plazos definidos en el procedimiento, en cumplimiento de los términos legales establecidos por la legislación colombiana. El análisis periódico de las PQRSF alimenta el proceso de mejora continua del SGI, generando insumos para la identificación de oportunidades de mejora en la prestación del servicio.

8.8 Síntesis: La Operación como Eje del SGI

El análisis de la dimensión operacional del SGI de Berruit SAS revela una arquitectura de gestión que integra coherentemente los requisitos de ISO 9001:2015 e ISO/IEC 27001:2022 en un único sistema de gestión con procedimientos, indicadores y controles compartidos. La operación del SGI descansa sobre cuatro pilares fundamentales:

El primer pilar es el marco procedimental integrado, compuesto por más de cuarenta y cinco procedimientos documentados que cubren la totalidad del ciclo de vida del servicio de TI: desde la prospección comercial (P-CL-01) hasta la gestión de incidentes de seguridad (P-STE-09),

pasando por el control de accesos (P-STE-02), la gestión de cambios (P-STE-06), la continuidad del negocio (P-STE-24) y la gestión de no conformidades (P-SGI-04). Este marco procedimental garantiza la estandarización, la reproducibilidad y la trazabilidad de los procesos operacionales.

El segundo pilar es la gestión basada en riesgos, instrumentalizada a través de la Matriz de Riesgos del SGI (MT-SGI-02), que identifica sesenta y un riesgos activos y define planes de tratamiento específicos para los treinta riesgos inaceptables. La gestión de riesgos alimenta directamente la selección y priorización de los controles del Anexo A de ISO/IEC 27001:2022 documentados en la Declaración de Aplicabilidad (SOA-SGI -01).

El tercer pilar es la arquitectura de controles de seguridad, articulada en la Declaración de Aplicabilidad (SOA-SGI -01) con setenta y ocho controles aplicables del Anexo A, quince ya implementados y cincuenta y dos en proceso de implementación. Esta arquitectura cubre los controles organizacionales, de personas, físicos (adaptados al contexto de trabajo remoto) y tecnológicos requeridos para proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información gestionada.

El cuarto pilar es el ciclo de mejora continua, sostenido por los indicadores de gestión de cada proceso (documentados en las fichas técnicas F-SGI-07), la gestión de no conformidades y acciones correctivas (P-SGI-04), la medición de la satisfacción del cliente (F-STE-07), la gestión de PQRSF (P-SGI-03) y las revisiones periódicas del SGI por la Alta Dirección. Este ciclo garantiza que el sistema evoluciona de manera sistemática hacia niveles crecientes de madurez y conformidad normativa.

La implementación del Capítulo 8 del SGI en Berruit SAS demuestra que la integración de ISO 9001:2015 e ISO/IEC 27001:2022 no solo es viable sino deseable para una organización de servicios TI: los controles de seguridad de la información refuerzan la calidad del servicio, y los requisitos de calidad operacional estructuran la gestión de la seguridad de una manera más sistemática y sostenible que si ambas normas se implementaran de forma independiente.

8.3.9. Cierre de la implementación del sistema integrado de gestión

Como resultado del proceso de consultoría desarrollado en Berruit S.A.S., se logró diseñar y ejecutar un plan de implementación para los requisitos correspondientes a los capítulos 4 al 8 de

las normas ISO 9001:2015 e ISO/IEC 27001:2022 en un 100%, estableciendo las bases estratégicas, operacionales y documentales necesarios para la consolidación de un Sistema Integrado de Gestión orientado a la calidad y la seguridad de la información. Respecto al proyecto total de Berruit para desarrollar la implementación de todos los numerales, se consolida un 82.7 % de cumplimiento global en el cuerpo de las normas y un 90.3 % en el marco de controles del Anexo A (destacando un 100 % en la categoría de Personas A.6, 90.9 % en Físico A.7, 85.2 % en Tecnológico A.8 y 85.1 % en Organizacional A.5). La brecha para alcanzar el 100 % de implementación institucional reside en actividades operativas a cargo de la empresa: el fortalecimiento puntual del Capítulo 5 (Liderazgo, 87.5 %) y la puesta en marcha de los Capítulos 9 (Evaluación del desempeño, 25.0 %) y 10 (Mejora, 66.7 %), escenarios que requieren el desarrollo formal de la auditoría interna y la revisión por la dirección. Ver Anexo D Resultado plan de implementación y anexo Ver Anexo D Integración de numerales y controles.

Durante el desarrollo del proyecto se abordaron aspectos fundamentales relacionados con la comprensión del contexto organizacional, la identificación de las necesidades y expectativas de las partes interesadas, la definición del alcance, la estructuración del mapa de procesos, el liderazgo y compromiso de la alta dirección, la planificación basada en riesgos y oportunidades, la definición de objetivos estratégicos, la asignación de recursos, la gestión del talento humano y la implementación de controles operacionales necesarios para garantizar la prestación de servicios bajo criterios de calidad y protección de la información.

A continuación en la tabla 12 ver resultado final del plan de implementación de los numerales del 4 al 8 de las normas y el Anexo A de controles de seguridad de la información:

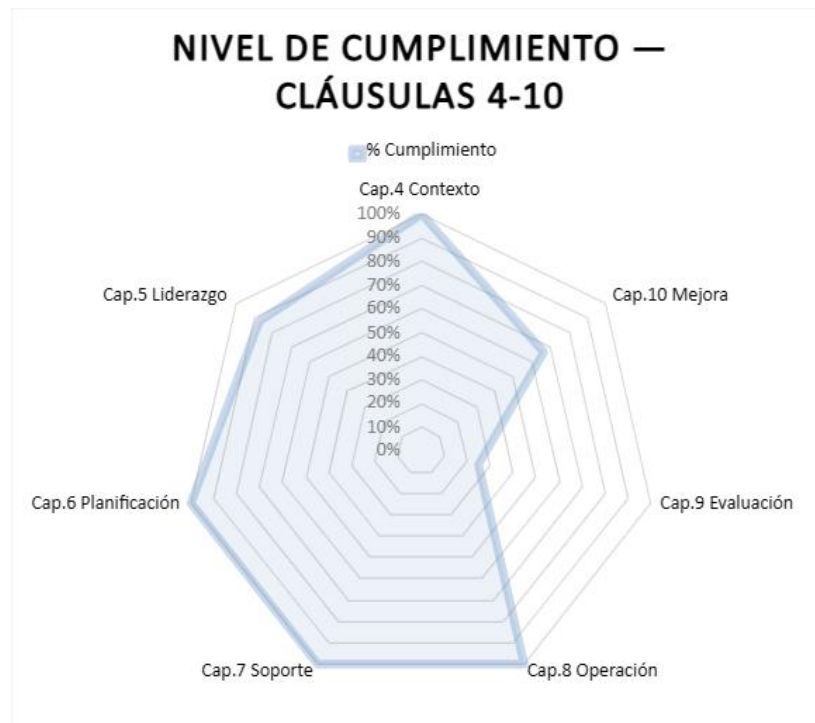
Tabla 12 Cumplimiento por capítulo de normas – Clausulas 4 al 10

CUMPLIMIENTO POR CAPÍTULO — CLÁUSULAS 4 AL 10						
Capítulo	Nombre	Cumple	Cumple Parc.	No Cumple	No Aplica	% Cumplimiento
Capítulo 4	Contexto	4	0	0	0,0%	100,0%
Capítulo 5	Liderazgo	3	1	0	0,0%	87,5%
Capítulo 6	Planificación	5	0	0	0,0%	100,0%

Capítulo 7	Soporte	5	0	0	0,0%	100,0%
Capítulo 8	Operación	4	0	0	0,0%	100,0%
Capítulo 9	Evaluación del Desempeño	0	2	2	0,0%	25,0%
Capítulo 10	Mejora	1	2	0	0,0%	66,7%
PROMEDIO GENERAL SGI		3,142857143	0,714285714	0,285714286	0	82,7%
PROMEDIO DEL CAPITULO 4 AL 8						97,5%

Fuente: Elaboración propia

El Capítulo 5 registra un cumplimiento del **87,5%** debido a una brecha en la Cláusula 5.1 de ISO 9001 e ISO/IEC 27001, originada porque la Alta Dirección aún no evidencia formalmente su liderazgo activo en la revisión de objetivos y en la rendición de cuentas ante las partes interesadas. Aunque el SGI refleja un sólido **97,5%** de avance entre los capítulos 4 y 8, esta conformidad parcial en el componente estratégico representa un riesgo metodológico para el proyecto; la falta de registros formales (como actas de revisión) desarticula la conexión entre la planificación operativa del sistema y el respaldo gerencial indispensable para garantizar su sostenibilidad técnica.

Figura 26 Nivel de cumplimiento de cláusulas 4 al 10

Fuente: Elaboración propia

La evaluación de los 93 controles del Anexo A de la norma ISO/IEC 27001:2022 se realizó por las cuatro categorías definidas en la versión 2022 del estándar: organizacional (A.5), personas (A.6), físico (A.7) y tecnológico (A.8). El resultado global fue del 93 % de cumplimiento, superando el umbral de pre-certificación del 80 %, con un único control en estado Cumple parcialmente (A.8, controles tecnológicos). La Tabla 12 y la Figura 30 presentan el detalle por categoría.

Tabla 13 Cumplimiento por categoría – Anexo A ISO/EIC 27001:2022

CUMPLIMIENTO POR CATEGORÍA — ANEXO A (93 CONTROLES ISO/IEC 27001:2022)						
Categoría	Descripción	Cumple	Cumple Parc.	No Cumple	No Aplica	% Cumplimiento
A.5	Organizacional (37 controles)	26	11	0	0	85,1%
A.6	Personas (8 controles)	8	0	0	0	100,0%
A.7	Físico (14 controles)	9	2	0	3	90,9%
A.8	Tecnológico (34 controles)	20	6	1	7	85,2%
PROMEDIO GENERAL ANEXO A		15,75	4,75	0,25	2,5	90,3%

Fuente: Elaboración propia

El diagnóstico general del Sistema de Gestión de la Seguridad de la Información (SGSI) para Berruit S.A.S. evidencia un diseño metodológico integral. Sin embargo, debido a las limitaciones de tiempo inherentes al desarrollo del trabajo de grado, la organización registra un estado de "Cumplimiento Parcial" en ciertos controles.

Las brechas se estructuran y detallan de la siguiente manera:

1. Brechas Organizacionales (Políticas y Gestión Documental)

- A.5.4 Responsabilidades de la dirección: El diseño conceptual del SGSI está terminado, pero falta la generación histórica de las actas de revisión formal por parte de la alta gerencia.
- A.5.6 Contacto con grupos de interés especial: Se requiere formalizar e institucionalizar la suscripción activa a fuentes externas de inteligencia de amenazas (tales como *CVE*, *CISA*, *MITRE ATT&CK*).
- A.5.13 Etiquetado de la información: Aunque existe un procedimiento de clasificación de la información, el etiquetado físico y digital sistemático en correos electrónicos, documentos y activos aún no se ejecuta de forma automatizada.

- A.5.14 y A.5.20 Seguridad en contratos (Clientes/Proveedores): Es necesario incorporar de manera obligatoria y estándar las cláusulas de seguridad de la información, protección de datos y acuerdos de confidencialidad en los contratos formales de ambas partes.
- A.5.16 y A.5.18 Control de accesos e identidades: Se definieron los roles, pero queda pendiente la implementación de revisiones periódicas del inventario de identidades, control de cuentas inactivas y el registro de aprobación formal por parte de cada líder de proceso.
- A.5.28, A.5.35 y A.5.36 Evaluaciones y Evidencia: Queda como proyección estructurar auditorías independientes anuales, autoevaluaciones por proceso basadas en listas de verificación, y simulacros prácticos sobre procedimientos de cadena de custodia para incidentes forenses.

2. Brechas Físicas (Operaciones en Campo)

- A.7.1 y A.7.2 Perímetros y controles de entrada física: Al ser una empresa con operaciones deslocalizadas o servicios externos, este requisito no aplica directamente a sedes físicas complejas de Berruit, pero se identifica la necesidad de diseñar un *checklist* de seguridad física mínima que los técnicos deban validar de forma obligatoria antes de intervenir o prestar servicios en las instalaciones del cliente.

3. Brechas Tecnológicas (Seguridad Lógica e Infraestructura)

- A.8.9 Gestión de la configuración: Se requiere la adopción futura de herramientas de automatización (como *Ansible*, *SCCM*, etc.) que verifiquen de forma sistemática la aplicación de las líneas base (*baselines*) de seguridad en los equipos de cómputo y servidores.
- A.8.21 Seguridad en los servicios de red: Falta la documentación explícita de los Acuerdos de Nivel de Servicio (SLA) específicos de seguridad con los proveedores de Internet y la activación de alertas de anomalías en tráfico de red.
- A.8.22 Segregación de redes: Queda estructurada metodológicamente en los mapas de arquitectura de red, pero su efectividad técnica total requiere ser validada y documentada formalmente en los planes de auditoría de infraestructura.
- A.8.31 y A.8.32 Gestión de cambios y entornos: Aunque la operación técnica se apoya en plataformas como *GLPI*, se debe fortalecer la gobernanza a través de la aprobación previa documentada de cada cambio en la infraestructura y asegurar de forma estricta la separación lógica total entre entornos de desarrollo, pruebas y producción.
- A.8.33 Información de prueba: Se identificó la necesidad de aplicar técnicas obligatorias y sistemáticas de anonimización o seudonimización de datos reales cuando se utilicen bases de datos o información operativa dentro de las fases de prueba del software.

Conclusión Estratégica

A nivel estratégico, los hallazgos descritos en los tres pilares evaluados (organizacional, físico y tecnológico) revelan que la organización cuenta con una estructura de gobierno de seguridad de la información planificada, cuya brecha principal radica en la formalización de la evidencia y la automatización operativa. Los controles pendientes —tales como la estandarización de cláusulas contractuales, la automatización de líneas base de configuración y la segregación técnica de entornos— constituyen un plan de acción preventivo indispensable para asegurar la sostenibilidad del sistema. La alta dirección debe asumir estas brechas como prioridades de inversión táctica, entendiendo que el cierre de estos compromisos parciales es el paso crítico para mitigar de manera efectiva los riesgos operacionales remanentes y consolidar un entorno tecnológico blindado que respalde las operaciones internas y externas de la compañía.

Hoja de Ruta para los Capítulos 9 y 10

Como parte de la transición hacia las etapas de seguimiento y mejora del sistema, se desarrolló la estructura de medición y seguimiento mediante la definición del cuadro de mando de indicadores, permitiendo establecer los mecanismos necesarios para evaluar el desempeño de los procesos, el cumplimiento de los objetivos del Sistema Integrado de Gestión y la eficacia de las acciones implementadas. Esta herramienta constituye el punto de partida para la ejecución de las actividades contempladas en el capítulo 9 de ambas normas, relacionadas con el seguimiento, medición, análisis y evaluación del desempeño organizacional.

No obstante, considerando el alcance definido para el presente trabajo de grado y el tiempo disponible para la ejecución de la consultoría, las actividades correspondientes a la operación prolongada del sistema, la generación de registros de desempeño, la realización de auditorías internas, las revisiones por la dirección, el tratamiento de no conformidades, la implementación de acciones correctivas y la consolidación de los procesos de mejora continua asociados a los capítulos 9 y 10 de las normas ISO 9001:2015 e ISO/IEC 27001:2022 deberán ser ejecutadas por Berruit S.A.S. durante la etapa de maduración del Sistema Integrado de Gestión.

En consecuencia, la organización cuenta actualmente con una estructura documental, metodológica y operativa que le permitirá continuar con la implementación del sistema, generar las evidencias requeridas por las normas internacionales y avanzar hacia un proceso formal de auditoría de certificación. De esta manera, el presente trabajo constituye un aporte significativo para el fortalecimiento organizacional de Berruit S.A.S., dejando establecidas las condiciones necesarias para la sostenibilidad, mejora continua y futura certificación de su Sistema Integrado de Gestión. Ver anexo D Resultado del plan de implementación y Anexo E Integración de numerales y controles.

9. Conclusiones y Recomendaciones

9.1. Conclusiones

- **Conclusiones respecto al Objetivo Específico 1: Diagnóstico Inicial de Cumplimiento**

(Objetivo: Diagnosticar el cumplimiento de los requisitos de las normas ISO 9001:2015 e ISO/IEC 27001:2022 con el fin de establecer el nivel de cumplimiento de Berruit S.A.S.)

- **Establecimiento de la Línea Base de Madurez:**

El diagnóstico inicial permitió consolidar una línea base objetiva sobre el estado de la organización, evidenciando un nivel de cumplimiento inicial del 15 % para la norma ISO 9001:2015, del 15 % para la norma ISO/IEC 27001:2022 y un nivel global del 15 % para el Sistema de Gestión Integrado (SGI). Este resultado cuantitativo confirmó la existencia de brechas críticas en materia de gestión por procesos, planificación estratégica, seguimiento al desempeño y controles de seguridad de la información, justificando plenamente la necesidad técnica y operativa de ejecutar el presente proyecto de consultoría.

- **Conclusiones respecto al Objetivo Específico 2: Plan de Trabajo e Interacción de Procesos**

(Objetivo: Establecer el plan de trabajo identificando los procesos clave y sus interacciones para cumplir los requisitos del Sistema de Gestión Integral ISO 9001 e ISO/IEC 27001).

- **Gestión Eficiente de Recursos y Control Operativo del Plan**

El cumplimiento en el tiempo del plan de trabajo propuesto, se logró gracias a una asignación estratégica y oportuna de los recursos humanos, tecnológicos y administrativos requeridos en cada fase de la consultoría. Esta disponibilidad de recursos facilitó una interacción fluida con los líderes de proceso y aseguró la consecución ordenada de los hitos normativos

comprendidos entre los numerales 4 al 8 de las normas ISO 9001 e ISO/IEC 27001, así como la integración metodológica de los controles del Anexo A.

Asimismo, el monitoreo constante y la mitigación anticipada de los riesgos de incumplimiento asociados al proyecto (como desviaciones en tiempos, resistencia al cambio o inconsistencias documentales) mantuvieron la ejecución dentro de los márgenes planificados. Como resultado, la interacción entre los procesos estratégicos, misionales y de apoyo quedó totalmente formalizada y alineada con la Estructura Armonizada, garantizando un sistema de gestión integrado, funcional y preparado para su sostenibilidad operativa.

- **Conclusiones respecto al Objetivo Específico 3: Desarrollo del Plan de Implementación (Cláusulas 4 a 8)**

(Objetivo: Desarrollar el plan de implementación del SGI desde el análisis del contexto hasta el control operacional, con el propósito de alcanzar un nivel de cumplimiento superior al 80 % de los requisitos aplicables).

- **Superación de la Meta de Cumplimiento Normativo:**

Se alcanzó un nivel final de cumplimiento del 97.5 % en las cláusulas operativas y de soporte (Capítulos 4 al 8) del Sistema de Gestión Integrado, así como un 90.3 % de cobertura en los controles aplicables del Anexo A de la norma ISO/IEC 27001:2022 (con un promedio general acumulado del SGI del 82.7 %). Estos porcentajes superan la meta planteada del 80 %, demostrando la efectividad de la ruta metodológica adoptada para el fortalecimiento de las capacidades institucionales.

- **Consolidación del Activo Documental y Arquitectura del SGI:**

El desarrollo del plan de implementación dotó a Berruit S.A.S. de un activo estratégico compuesto por **más de 80 documentos codificados**, que incluyen 49 procedimientos operacionales de seguridad de la información, 7 guías técnicas especializadas, la caracterización de procesos y la Declaración de Aplicabilidad (SOA-SGI-01). Esta infraestructura documental trasciende el mero formalismo normativo, convirtiéndose en un soporte operativo directo para la prestación de servicios de consultoría, outsourcing IT y ciberseguridad.

- **Conclusiones respecto al Objetivo General y Valor Estratégico Organizacional**

(Objetivo General: Diseñar y desarrollar un plan de implementación para un SGI basado en ISO 9001:2015 e ISO/IEC 27001:2022 para Berruit S.A.S., abarcando hasta el numeral 8).

- **Cumplimiento del Alcance de la Consultoría:**

Se dio cumplimiento al 100 % del alcance formulado para la consultoría académica, logrando estructurar el Sistema de Gestión Integrado desde el análisis del contexto organizacional (Capítulo 4) hasta el control operacional (Capítulo 8) y el Anexo A de la ISO/IEC 27001:2022. La organización alcanza así un nivel de madurez ESTABLECIDO, con una base técnica y metodológica sólida para operar bajo estándares internacionales.

- **Proyección de los Numerales 9 y 10 (Evaluación del Desempeño y Mejora):**

En consonancia con los límites fijados para el proyecto, la ejecución de las actividades de los Capítulos 9 (Evaluación del desempeño - 25.0 % de avance) y 10 (Mejora - 66.7 % de avance) —tales como la realización de la auditoría interna combinada y la revisión por la dirección— quedan formuladas en fase de planeación dentro del *Anexo B*. Estas etapas deberán ser ejecutadas directamente por Berruit S.A.S. durante la fase de maduración operativa del sistema.

- **Impacto Comercial y Posicionamiento Internacional:**

El fortalecimiento en la gestión de riesgos y la estandarización de procesos derivada del SGI contribuyó directamente al incremento de la confianza de clientes y aliados estratégicos. Este respaldo metodológico actuó como un catalizador de madurez comercial que facilitó hitos de expansión internacional altamente relevantes, como la apertura de la nueva sede corporativa de la compañía en Miami, Florida (Estados Unidos), proyectando la certificación formal del sistema durante el año 2026.

- **Recomendaciones**

Como recomendación para organizaciones del sector de tecnologías de la información y ciberseguridad que deseen implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2022, se sugiere desarrollar paralelamente un Sistema de Gestión de la Calidad bajo la norma ISO 9001:2015. La experiencia obtenida durante esta consultoría evidenció que la estructura basada en procesos, la definición de responsabilidades, el enfoque de riesgos, el control documental y los mecanismos de seguimiento promovidos por ISO 9001 proporcionan una base organizacional sólida que facilita la implementación y sostenibilidad de los requisitos de seguridad de la información. La integración de ambas normas permite construir sistemas de gestión más organizados, eficientes y alineados con los objetivos estratégicos del negocio, evitando que la implementación de controles de seguridad se realice de manera aislada o desarticulada de la gestión organizacional.

10. Referencias

- AENOR. (2005). Sistemas de gestión: Guía para la integración de los sistemas de gestión UNE_66177:2005. <https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0033847>
- Bakhtiar, A., Nugraha, A., Suliantoro, H., & Pujotomo, D. (2023). El efecto del sistema de gestión de calidad (ISO 9001) en el desempeño operativo de varias organizaciones en Indonesia. *Cogent Business & Management*, 10(2), Article 2203304. <https://doi.org/10.1080/23311975.2023.2203304>
- Benzaquen-de Las Casas, J., & Convers-Sorza, J. (2015). El ISO 9001 y TQM en las empresas de Colombia. *Journal of Globalization, Competitiveness & Governability*, 9(3), 107–128. <https://www.redalyc.org/pdf/5118/511851345005.pdf>
- Cabrera, H. R., Medina León, A., Abab Puente, J., Nogueira Rivera, D., & Núñez Chaviano, Q. (2015). La integración de sistemas de gestión empresariales, conceptos, enfoques y tendencias. *Ciencias de la Información*, 46(3), 3–8. <https://www.redalyc.org/pdf/1814/181443340001.pdf>
- Cámara Colombiana de Informática y Telecomunicaciones. (11 de agosto de 2022). Número de empresas de información y telecomunicaciones. <https://www.ccit.org.co/articulos-tictac/numero-de-empresas-de-informacion-y-telecomunicaciones/>
- Cámara Colombiana de Informática y Telecomunicaciones. (28 de junio de 2024). Fortaleciendo la ciberseguridad en Colombia: Educación y protección empresarial. <https://www.ccit.org.co/articulos-tictac/fortaleciendo-la-ciberseguridad-en-colombia-educacion-y-proteccion-empresarial/>
- Carro, R., & González, D. (2020). Administración de la Calidad Total. Administración de las operaciones.

Departamento Nacional de Planeación. (2016). *Política Nacional de Seguridad Digital (CONPES 3854)*. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

Departamento Nacional de Planeación. (2025). *Política Nacional de Inteligencia Artificial (CONPES 4144)*. <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf>

DANE. (2021). Encuesta de inversión en investigación y desarrollo I+D. <https://www.dane.gov.co/index.php/estadisticas-por-tema/tecnologia-e-innovacion/encuesta-de-inversion-en-investigacion-y-desarrollo-i-d>

Datacrédito Experian. (14 de mayo de 2024). Tecnología en Colombia: Una industria cada vez más importante dentro del crecimiento del país. <https://www.datacredito.com.co/blogs/datablog/tecnologia-en-colombia/>

De La Cruz Rodríguez, G., Méndez Fernández, R. A., & Méndez Fernández, A. C. (2023). Seguridad de la información en el comercio electrónico basado en ISO/IEC 27001: Una revisión sistemática. *Innovación y Software*, 4(1), 219–236. <https://www.redalyc.org/journal/6738/673874721015/673874721015.pdf>

Decreto 2364 de 2012. Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. 22 de noviembre de 2012. D.O. No. 48622. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=50583>

Decreto 338 de 2022. Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. 08 de marzo de 2022. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>

Fernández, J. S., Cipagauta, E. C., Wilches, A., & Fonseca, A. I. (2024). Integración de sistemas mediante metodología de “uso integrado de estándares de gestión”. *Revista de Ciencias*

Sociales, XXX(1), 154–165.
<https://produccioncientificaluz.org/index.php/rcs/article/view/41644/48135>

Fernández, J., Cipagauta, E., Wilches, A., & Fonseca, A. (2024). Principales metodologías para la integración de sistemas de gestión. *Revista I3+*, 5(1), 9–24.
<https://revistasdigitales.uniboyaca.edu.co/index.php/reiv3/article/view/1394/1025>

Herfried, K. (2020). A Comprehensive Guide to Content, Implementation Tools, and Certification Schemes. *Standards for Management Systems*. XXVIII, 800 (1).

Hernández, G., Jaramillo, J., & Hernández, Y. (2022). La relación entre la cultura organizacional y la gestión de la calidad total en las pymes. *Estudios de Administración*, 29(2), 79–104.
<https://doi.org/10.5354/0719-0816.2022.67726>

G-Certi. (2025). Colombia: #18 mundial con 10.231 certificados ISO.
<https://gcerti.org/en/paises/colombia>

Global Standards. (2025). Infografía ISO Survey 2024. https://www.globalstd.com/wp-content/uploads/2025/10/Infografia-ISO-Survey-2024_ES.pdf

Gutiérrez Gómez, J. D., & Playonero Ortiz, D. J. (2019). Importancia de la gestión de la calidad en el mejoramiento del servicio al cliente [Trabajo de grado, Ingeniería Industrial]. Universidad Santiago de Cali.
<https://repositorio.usc.edu.co/server/api/core/bitstreams/7d1a6046-9400-446c-a000-44efc2aaadf1/content>

ICONTEC. (2015). Compendio: Normas fundamentales sobre gestión de la calidad y documentos de orientación para su aplicación (6ª ed.). Icontec.

Integración de sistemas de gestión mediante PASS 99 – 2012. (s.f).
<https://es.scribd.com/document/337037811/Integracion-de-Sistemas-de-Gestion-Mediante-PAS-99-2012-QueAprendemosHoy>

Instituto de seguridad y bienestar laboral (2023) Encuesta ISO sobre certificaciones de normas de sistemas de gestión a nivel mundial.

<https://isbl.eu/2024/10/iso-survey-2023/>

ISO.org – Encuesta de la ISO (2023)

<https://www.iso.org/the-iso-survey.html>

Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2013). NTC-ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. ICONTEC. <https://tienda.icontec.org/gp-tecnologia-de-la-informacion-tecnicas-de-seguridad-sistemas-de-gestion-de-la-seguridad-de-la-informacion-requisitos-ntc-iso-iec27001-2013.html>

Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC]. (2023). Certificaciones ISO 9001 en Colombia: herramienta de competitividad e internacionalización. ICONTEC. <https://www.icontec.org/eval-conformidad/certificacion-iso-9001-sistema-de-gestion-de-calidad/>

ISO. (2024). ICONTEC – Instituto Colombiano de Normas Técnicas y Certificación [Perfil del organismo miembro]. Organización Internacional de Normalización. <https://www.iso.org/member/1644.html>

Karapetrovic, S., & Willborn, W. (1998). Integrated audit of management systems. International Journal of Quality & Reliability Management, 15(7), 694–711. <https://doi.org/10.1108/02656719810218220>

- Kirvan, P. (27 de octubre de 2023). Top 12 IT security frameworks and standards explained. TechTarget Security. <https://www.techtarget.com/searchsecurity/tip/IT-security-frameworks-and-standards-Choosing-the-right-one>
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 17 de octubre de 2012. D.O. No. 48587. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. 5 de enero de 2009. D.O. No. 47.223. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>
- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. 21 de agosto de 1999. D.O. No. 43.673. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276>
- Marcha Lagos, N., Gómez, L. F., Londoño, D. C., Moreno, I. C., & Camacho Camacho, H. (2023). Metodologías para la integración de sistemas de gestión: Revisión de literatura. Signos, Investigación en Sistemas de Gestión, 15(2). <https://doi.org/10.15332/24631140.8689>
- Martínez-Rojas, A. B., Laguado-Ramírez, R. I., & Flórez-Serrano, E. (2018). Factores de éxito de la certificación ISO 9001 en empresas de Cúcuta y su Área Metropolitana. Estudios Gerenciales, 34(147), 216–228. <https://doi.org/10.18046/j.estger.2018.147.2599>
- Montoya, A. (5 de enero de 2024). Valor y dinero, desafío y oportunidades: Perspectivas 2024 para el sector tecnológico en Colombia. Revista Valor y Dinero. <https://valorydinero.com/2024/01/05/desafios-y-oportunidades-perspectivas-2024-para-el-sector-tecnologico-en-colombia/>

Moreno, A., Restrepo, J., & Sánchez, L. (2021). Integración de las normas NTC ISO 14001:2015, NTC ISO 45001:2018 y NTC ISO 13485:2016 y su alineación a un sistema de gestión integral basado en la GTC 180:2008, en el sector de comercialización para dispositivos médicos en Colombia [Tesis de maestría, Universidad Santo Tomás]. Repositorio Institucional USTA. <https://repository.usta.edu.co/handle/11634/27994>

Ministerio de comercio, industria y turismo - millones invertidos para que mipymes adopten estándares de calidad global (2024)

<https://www.mincit.gov.co/prensa/noticias/industria/inversion-mipymes-adopten-estandares-de-calidad>

Ministerio de Comercio, Industria y Turismo [MINCIT]. (2024). Colombia Productiva – Programa de apoyo a MiPymes para certificaciones ISO 9001. <https://www.colombiaproductiva.com>

Mipymes.gov.co – Sistema nacional de apoyo a las Mipymes (2024)

<https://www.mipymes.gov.co/coordinacion-con-entidades-publico-privadas-para-a/sistema-nacional-de-apoyo-a-las-mipymes-1#:~:text=El%20Sistema%20Nacional%20de%20Apoyo%20a%20las%20Mipymes%20borda%20apoyo,que%20forman%20parte%20del%20mismo.>

OpenAI. (2024). ChatGPT [Modelo de lenguaje AI]. <https://chat.openai.com/>

Organización Internacional de Normalización (ISO). (2022). Sistema de gestión de seguridad de la información (ISO/IEC 27001). <https://ecollection-icontec-org.crai-ustadigital.usantotomas.edu.co/normavw.aspx?ID=102657>

Organización Internacional de Normalización (ISO). (s.f.). ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection. ISO. Recuperado el [30 octubre 2024], de <https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7emZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top>

Organización Internacional de Normalización. (2015). *Sistemas de gestión de la calidad — Requisitos* (ISO 9001:2015). <https://www.iso.org/standard/62085.html>

Organización Internacional de Normalización, & Comisión Electrotécnica Internacional. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos* (ISO/IEC 27001:2022). <https://www.iso.org/standard/27001>

Pupo Guisado, B., Cruz Garrido, Y., & Robert García, M. (2021). Formación y mejora del liderazgo para perfeccionar el sistema de gestión de la calidad en empresa cubana. *Dilemas Contemporáneos: Educación, Política y Valores*, 8(2), 1–31.

Pirani – Seguridad de la información – Casos de ciberataques a empresas en 2022

<https://www.piranirisk.com/es/blog/ciberataques-empresas-en-2022>

Ramírez Flores, C. I., Martínez Moctezuma, E., & Arroyo Grant, M. G. (2019). El líder como promotor de la gestión del cambio. *Revista Ciencia Administrativa*, 1, 38–42.

Sánchez, N. (30 de septiembre de 2024). Sector digital en Colombia creció 25,7% en 2023 y generó ventas por \$57,2 billones. *La República*. <https://n9.cl/t2fb9>

Tesis Maestría en ingeniería de sistemas con mención en tecnologías de la información – Universidad Cesar Vallejo - Edwin Samuel Arias, Edwin Alberto Martínez, 2020, Peru)

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1&isAllowed=y

Valencia Duque, F. (2021). Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. Centro Editorial de la Facultad de Administración. <https://repositorio.unal.edu.co/bitstream/handle/unal/80158/9789587946017.pdf?sequence=2&isAllowed=y>

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Cengage Learning. https://almuhammadi.com/sultan/sec_books/Whitman.pdf

Whitman, M. E., & Mattord, H. J. (2028). *Management of information security* (6.^a ed.). Cengage Learning. <https://www.cengage.com/c/management-of-information-security-6e-whitman/9781337405713/>

11. Anexos

Anexo A Instrumento Autodiagnóstico SGC Y SGSI INICIAL 2024

Anexo B Plan de implementación Berruit SAS

Anexo C SOA-SGI-01 DECLARACIÓN DE APLICABILIDAD (SoA)

Anexo D Resultado plan de implementación

Anexo E Integración de numerales y controles