Diseño de un Sistema Integrado de Gestión a partir de la integración de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013 para la empresa AMOVIL S.A.S

Clarien Selene Guerrero Vega, Natalia Niño Meza

Trabajo de grado para optar el título de Magíster en Calidad y Gestión Integral

Director

Omar Vivas Calderón

Magíster en E-Learning

Universidad Santo Tomas, Bucaramanga

División de Ingenierías y Arquitectura

Maestría en Calidad y Gestión Integral

2023

Dedicatoria

Clarien Selene Guerrero Vega

Dedico este trabajo a Dios quien a través de su bondad me dio la fuerza, perseverancia y esta valiosa oportunidad de crecimiento personal y profesional.

A mi esposo Juan Sebastian por haberme dado el impulso para retomar mis estudios y su consejo sabio y amoroso para perseverar todas las veces que pensé en renunciar.

A mi hermosa hija porque fue comprensiva y me concedió con amor, el tiempo necesario para cubrir mis compromisos académicos.

Natalia Niño Meza

Dedico primeramente este trabajo a Dios, quien me tomó en mis días malos y me levantó con nuevo aliento, y por darme la oportunidad de llegar hasta aquí.

A mi esposo, Daniel Quiroz por motivarme y apoyarme a continuar a pesar de toda adversidad, y por su amor siendo mi terapia emocional.

A mis padres, Argenis Meza y Ricardo Niño, por sembrar en mí el deseo de llegar más lejos y por enseñarme el valor del esfuerzo.

Agradecimientos

Expresamos nuestro agradecimiento a la Universidad Santo Tomás seccional Bucaramanga por ofrecernos un programa académico, docentes y espacios de formación que dejaron una huella en nuestras vidas personales y profesionales. Igualmente, agradecemos a la directora de la Maestría Vanessa Rivera y a los profesores Omar Vivas y Sandra Castillo, por su orientación y apoyo. Por último, agradecemos a la empresa Amovil S.A.S por ofrecernos la oportunidad de aplicar nuestros conocimientos en este proyecto tan retador.

Contenido

Lista de Tablas

Lista de Figuras

Apéndices

Apéndice *A*. *Hoja de vida experta – Ing. Alexandra Bibiana Cala Moreno*

Apéndice *B*. *Diagnóstico preliminar - consolidado de resultados de análisis de brechas – NTC ISO 9001:2015, NTC ISO/IEC 27001:2013 y Anexo A*

Apéndice *C*. *Contexto - 4.1 y 4.2 Comprensión contexto y partes interesadas*

Apéndice *D*. *Contexto - 4.3 y 4.4 Determinación del alcance SIG y sus procesos*

Apéndice *E*. *Liderazgo – 5.1, 5.2 y 5.3 Liderazgo, política y roles y responsabilidades*

Apéndice *F*. *Planificación – 6.2 Objetivos SIG y su planificación*

Apéndice *G*. *Apoyo – 7.1, 7.2, 7.4 y 7.5 Recursos, competencia, comunicación e información documentada*

Apéndice *H*. Evaluación desempeño – 9.1, 9.2 y 9.3 Seguimiento y medición, auditoría interna y revisión por la dirección

Apéndice *I*. *Mejora – 10.2 y 10.3 No conformidad, acción correctiva y mejora continua*

Apéndice *J*. *Apéndice J: Contexto – 4.4 SIG y sus procesos*

Apéndice *K*. *Planificación - 6.1 Acciones para abordar riesgos y oportunidades*

Apéndice *L*. *Liderazgo – 5.1.2 Enfoque al cliente*

Apéndice *M*. *Planificación – 6.3 Planificación de los cambios*

Apéndice *N*. *Apoyo – 7.1.2, 7.1.3, 7.1.4, 7.1.6 Personas, infraestructura, ambiente de operación y conocimientos de la organización*

Apéndice *O*. *Operación – 8.1 y 8.2 Planificación y control operacional y requisitos para los productos y servicios*

Apéndice *P*. *Operación – 8.3 Diseño y desarrollo*

Nota: los apéndices asociados a este trabajo corresponden a documentos externos, razón por la cual no se relacionan números de página en esta lista.

Resumen

Las organizaciones familiares realizan prácticas que muchas veces no facilitan su adaptación a la globalización. En este contexto, los sistemas de gestión ofrecen una ruta para lograr una gestión más eficiente. Además, que su estructura de alto nivel facilita su implementación e integración. Este estudio expone los resultados logrados en una organización de base familiar dedicada al diseño y desarrollo de software. La organización experimentó un rápido crecimiento en diez años, el cual no se enfocó en los procesos y puso en riesgo la eficacia de la gestión por la centralización de funciones en el equipo de alta gerencia y la pérdida del conocimiento por la inexistencia de prácticas de documentación. A través del presente trabajo se planteó el diseño de un sistema integrado de gestión (SIG) que integrara los requisitos de las normas NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013 y que ofreciera a la organización las bases para un funcionamiento organizado, pragmático y de mejora permanente a través de tres fases: el diagnóstico preliminar mediante el análisis de brechas, la fase de diseño basada en la metodología del ciclo Deming y la relación de requisitos, la fase de ejecución a través de la documentación e implementación del SIG, y la fase de validación a través de un informe de juicio de expertos. El proyecto resultó en un SIG que integró completamente los requisitos de ambos estándares, logró el aseguramiento de la gestión del conocimiento, la gestión basada en los procesos y dio mayor robustez organizacional a la empresa.

Palabras Claves: integración, NTC ISO 9001:2015, NTC ISO/IEC 27001:2013, empresa familiar

Abstract

Family organizations carry out practices that often do not facilitate their adaptation to globalization. In this context, management systems offer a route to achieve more efficient management. In addition, their high-level structure facilitates their implementation and integration. This study exposes the results achieved in a family-based organization dedicated to the design and development of software. The organization experienced rapid growth in ten years, which did not focus on processes and put management effectiveness at risk due to the centralization of functions in the senior management team and the loss of knowledge due to the lack of documentation practices. Through the present work, the design of an integrated management system (IMS) was proposed that would integrate the requirements of the NTC ISO 9001:2015 and NTC ISO/IEC 27001:2013 standards and that would offer the organization the bases for an organized operation, pragmatic and of permanent improvement through three phases: the preliminary diagnosis through the analysis of gaps, the design phase based on the Deming cycle methodology and the relationship of requirements, the execution phase through the documentation and implementation of the IMS, and the validation phase through an expert judgment report. The project resulted in an IMS that fully integrated the requirements of both standards, achieved knowledge management assurance, process-based management, and gave the company greater organizational robustness.

Key Word: integration, NTC ISO 9001:2015, NTC ISO/IEC 27001:2013, family company

Glosario

Análisis de brecha: un análisis de brechas (también conocido como análisis GAP o análisis de necesidades) es un proceso que se usa para comparar el desempeño real de la empresa con el desempeño deseado. La "brecha" se entiende como el espacio entre donde se encuentra tu negocio actualmente y donde te gustaría que esté. (ASANA, 2022)

Calidad: grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos. (ICONTEC, 2015, p. 2)

Ciclo Deming: el ciclo de Deming es un sistema que busca la optimización constante de las actividades empresariales a través de cuatro etapas. Una vez que se llega a la última etapa, la empresa debe volver a comenzar, promoviendo así una autoevaluación continua que le permita identificar oportunidades de mejora en cada proceso. (DispatchTrack, 2023)

Confidencialidad: la confidencialidad, cuando nos referimos a sistemas de información, permite a los usuarios autorizados acceder a datos confidenciales y protegidos. Existen mecanismos específicos garantizan la confidencialidad y salvaguardan los datos de intrusos no deseados o que van a causar daño. (ISO 27001, 2013)

Diagnóstico: como diagnóstico se denomina la acción y efecto de diagnosticar. Como tal, es el proceso de reconocimiento, análisis y evaluación de una cosa o situación para determinar sus tendencias, solucionar un problema o remediar un mal. La palabra proviene del griego διαγνωστικός (diagnōstikós). (Significados)

Disponibilidad: la disponibilidad, en el contexto de los sistemas de información se refiere a la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto. (ISO 27001, 2013)

Diseño: normalmente, por diseño se conoce el arte de proyectar el aspecto, la función y la producción de un objeto funcional por medio de signos gráficos, sea que se trate de un objeto bidimensional (carteles, logos, animaciones, portadas, etc.) o tridimensional (edificios, maquinarias, muebles, entre otros). (Significados)

Enfoque basado en procesos: implica la definición y gestión sistemática de los procesos y sus interacciones, con el fin de alcanzar los resultados previstos de acuerdo con la política de la calidad y la dirección estratégica de la organización. (ICONTEC, 2015, p. 7)

Integración: cualquier empresa u organización es considerado una forma de organismo social. Bajo esta definición, la integración constituye una función administrativa constante de inclusión, unión y actualización de los recursos humanos, recursos materiales y recursos informáticos en un solo sistema u organismo social. (Significados)

Integridad: la integridad de la información se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios. (ISO 27001, 2013)

NTC ISO 9001:2015: norma internacional que especifica los requisitos para un sistema de gestión de la calidad cuando una organización: a) necesita demostrar su capacidad para proporcionar regularmente productos y servicios que satisfagan los requisitos del clientes y los

legales y reglamentarios aplicables, y b) aspira a aumentar la satisfacción del cliente a través de la aplicación eficaz del sistema, incluidos los procesos para la mejora del sistema y el aseguramiento de la conformidad con los requisitos del cliente y los legales y reglamentarios aplicables. (ICONTEC, 2015, pp. i - v)

NTC ISO/IEC 27001:2013: esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. La presente Norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. (ICONTEC, 2013, p. 1)

Relación de requisitos: metodología propuesta por (Mesquida, 2012, pp. 92 - 94) en la que se establecen tres tipos de correspondencia para los requisitos comparativos de las normas a integrar en el marco de un Sistema Integrado de Gestión. Las correspondencias propuestas con el autor son: relación total (“F”), relación parcial (“P”) e inexistencia de relación (“ ”).

Riesgo: efecto de la incertidumbre. (ICONTEC, 2015, p. 23)

Seguridad de la información: la seguridad de la información como vemos tiene por objetivo la protección de la confidencialidad, integridad y disponibilidad de los datos de los sistemas de información de cualquier amenaza y de cualquiera que tenga intenciones maliciosas. (ISO 27001, 2013)

Sistema de Gestión: conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, objetivos y procesos para lograr estos objetivos. (ICONTEC, 2015, p. 18)

Sistema de Gestión de Calidad (SGC): parte de un sistema de gestión relacionada con la calidad. (ICONTEC, 2015, p. 18)

Sistema de Gestión de Seguridad de la Información (SGSI): un sistema de gestión para la seguridad de la información consta de una serie de políticas, procedimientos e instrucciones o directrices específicas para cada actividad o sistema de información que persiguen como objetivo la protección de los activos de información en una organización. (ISO 27001, 2013)

Sistema Integrado de Gestión: un sistema de gestión integrado es un sistema único diseñado para gestionar múltiples aspectos de las operaciones de una organización en consonancia con múltiples normas, como las relativas a la gestión de la calidad, el medioambiente y la salud y la seguridad laboral. (NQA Organismo de certificación global)

Software: el término software es un vocablo inglés que fue tomado por otros idiomas y designa a todo componente intangible (y no físico) que forma parte de dispositivos como computadoras, teléfonos móviles o tabletas y que permite su funcionamiento. (Editorial Etecé, 2022)

Validación: confirmación, mediante la aportación de evidencia objetiva, de que se han cumplido los requisitos para una utilización o aplicación especifica prevista. (ICONTEC, 2015, p. 25)

Introducción

En Colombia la investigación de empresas familiares comenzó alrededor de los años 1990 y 2000, a partir de la cual se ha identificado un patrón de que al menos el 70% al 75% de las organizaciones corresponden a empresas familiares, lo que constituye un importante aporte al desarrollo económico del país (Sandoval & Guerrero, 2010, p. 136); sin embargo, este tipo de organizaciones asumen diferentes retos entre los que se destaca la separación de decisiones gerenciales de los intereses familiares, lo que genera debilidades organizacionales causadas por la segregación de funciones o la asignación de nuevos roles y responsabilidades que no se desean asumir o se asumen en exceso (Rave & Moreno, 2023, p. 40).

El caso de estudio del presente trabajo de investigación, se enfoca en la empresa Asistencia Móvil S.A.S – AMOVIL, una empresa santandereana de base familiar dedicada al desarrollo de software, orientada a atender los requerimientos del sector logístico de empresas de productos de consumo masivo. En menos de diez años AMOVIL experimentó un crecimiento exponencial para el que no estaba preparada y que para cualquier organización genera varios impactos: a) caos a nivel organizacional, b) alta demanda de recursos, c) crecimiento instantáneo o inmediato, y d) necesidad de seguridad absoluta; dónde la primera direcciona las siguientes (Platero & Arias, 2019, p. 6).

Para éstos y otros escenarios organizacionales, los Sistemas de Gestión surgen como una herramienta que permite a las empresas atender dichas necesidades, con un aporte significativo en la toma de decisiones, competitividad y sostenibilidad (Murrieta, Ochoa, & Carballo, 2020, p. 117), a través de los enfoques de la gestión de la calidad: enfoque al cliente, liderazgo, compromiso de las personas, enfoque a procesos, mejora continua, toma de decisiones basada en la evidencia

y gestión de las relaciones (ICONTEC, 2015, p. ii). Cuando una empresa además decide consolidar diversos Sistemas de Gestión a través de su integración, obtiene beneficios adicionales tales como: dar cumplimiento normativo mediando un único proceso de gestión, mejorar la eficiencia general de la organización, definir adecuadamente sus funciones, roles y responsabilidades orientadas a los mismos objetivos, facilitar la verificación del mejoramiento a través de procesos integrados de auditoría y el desarrollo de estrategias y acciones de mejora continua. (Gisbert & Esengeldiev, 2014, p. 248).

Este fue el reto abordado con la empresa AMOVIL realizar la integración de un Sistema Integrado de Gestión -SIG, basado en los requisitos de la norma NTC-IEC 27001:2013 enfocada a la protección de la información del negocio y los requisitos de la norma NTC-ISO 9001:2015 enfocada al logro de la satisfacción de los clientes y partes interesadas. Desde esta perspectiva se desarrolló una metodología de integración que optimizara los recursos ya invertidos, apoyara el mantenimiento del surgente SIG y promoviera el establecimiento de una cultura de gestión que fuera cimiento para una fuerte base organizacional orientada al logro de los objetivos propuestos en la proyección institucional.

El presente documento está estructurado en cinco capítulos principales: el capítulo 1 en donde se realiza el planteamiento del problema y se precisa el árbol de problemas identificado a partir del diagnóstico de las necesidades y contexto de la organización. En el capítulo 2, se abordan los antecedentes internacionales, nacionales y locales y marcos conceptuales que dieron punto de partida para la comprensión de las alternativas de solución abordadas por otras organizaciones con problemas similares. En el capítulo 3 se detalla la metodología propuesta para realizar la integración del Sistema de Gestión de Seguridad de la Información - SGSI y el Sistema de Gestión

de la Calidad - SGC con el propósito de lograr un Sistema Integrado de Gestión robusto, enfocado en procesos y que capitalizara la gestión del conocimiento de AMOVIL. En el capítulo 4 se consolidan todos los resultados logrados durante el proceso de integración e implementación del proyecto y, por último, en el capítulo 5 se concretan las conclusiones derivadas del trabajo de investigación.

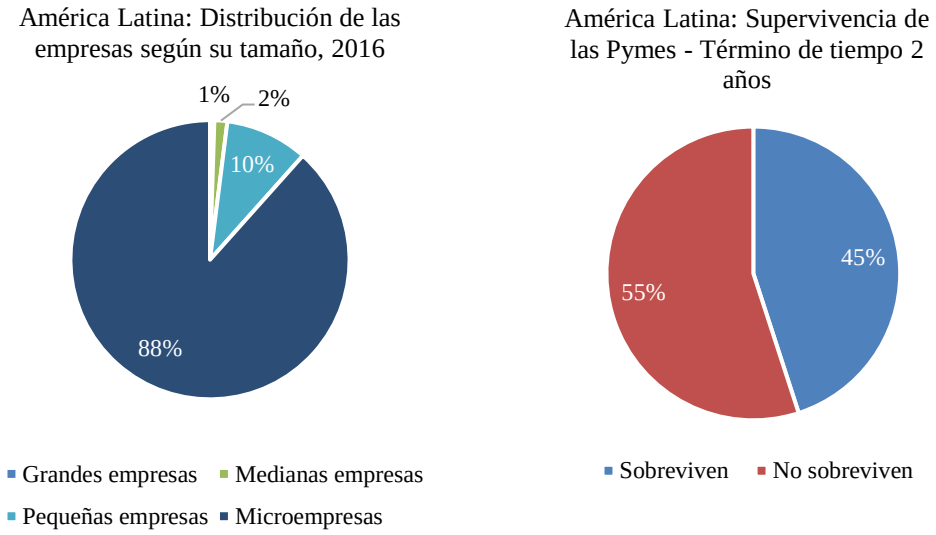
El proyecto supuso varios retos, entre ellos, motivar a la organización a un cambio de cultura fundamentado en la gestión por procesos, el fortalecimiento del liderazgo de la Alta Dirección para el logro del objetivo propuesto y el continuo entendimiento de las necesidades de AMOVIL para diseñar un SIG conveniente, adecuado y eficaz.

1. Diseño de un Sistema Integrado de Gestión a partir de la integración de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013 para la empresa AMOVIL S.A.S

1.1 Planteamiento del problema

En la actualidad la economía de los países se sostiene gracias a las MiPymes, especialmente en Latinoamérica, donde el desarrollo empresarial está ligado a núcleos familiares o sectores cuyo mercado es de fácil acceso, es decir, las barreras de entrada son mínimas lo que genera una amplia competencia con bajo valor diferenciador (Franco-Ángel, 2019, p. 82). La participación de las MiPymes en el número total de empresas en la región Latinoamericana, alcanza el 99.5%, siendo la gran mayoría microempresas con el 88.4%, los segmentos siguientes corresponden a medianas y grandes empresas con un 1.5% y 0.5% de participación, respectivamente (Dini & Stumpo, 2019, p. 13). Así mismo, se destaca que más del 60% del empleo es ofertado por las micro, pequeñas y medianas empresas (Dini & Stumpo, 2019, p. 16); sin embargo, en América Latina sólo el 45% de las Pymes logran sobrevivir los primeros dos (2) años, a diferencia de los países europeos dónde hay una supervivencia mayor al 80%, las causas de las bajas tasas de supervivencias son variadas y se requiere de su caracterización y compresión para implementar planes de acciones adecuados y eficaces (Ver Figura *1*). (Méndez, 2020)

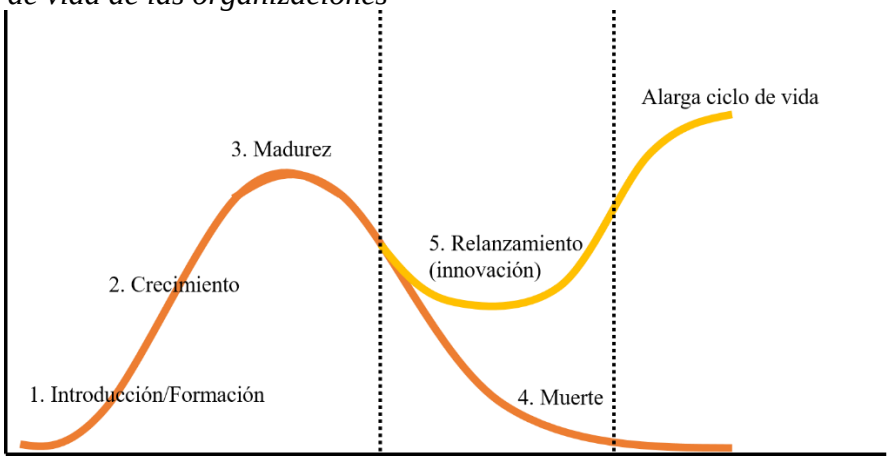
Figura 1. *Distribución de las empresas según su tamaño y tasa de supervivencia de las MiPymes en América Latina*



Adaptado de (Dini & Stumpo, 2019) (Méndez, 2020).

En países de la región como México, dentro de las causas asociadas a la prematura desaparición de las Pymes, se atribuyen las escasas medidas de apalancamiento y apoyo financiero gubernamental, pero con mayor peso, las debilidades propias de las organizaciones, entre ellas una mala gestión estratégica y administrativa. La debilidad organizacional se genera a raíz del inadecuado manejo del recurso financiero, humano y físico; la falta de asesoría administrativa y el difícil acceso al financiamiento por parte de los bancos (Lacayo & García, 2013, pp. 4 -10); estás situaciones conducen a la organización a un punto limitado de crecimiento, donde el caos estructural y las bases inestables dirigen a las empresas a su punto de quiebre y posteriormente a su muerte. Sin embargo, aquellas empresas que logran superar sus problemas organizacionales alargan su ciclo de vida (de Faveri, dos Santos, & Leandro, 2014, pp. 386 - 388). tal y como se muestra en la Figura *2*

Figura 2. *Ciclo de vida de las organizaciones*



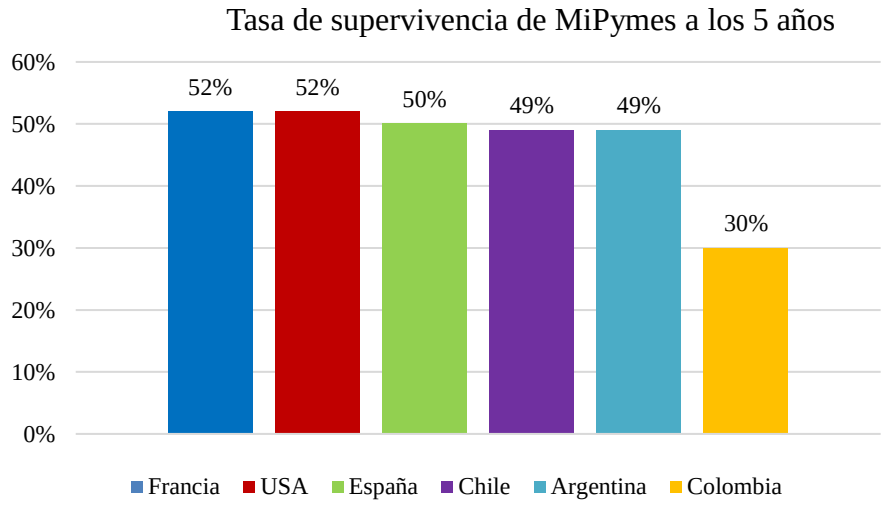
Adaptado de (de Faveri, dos Santos, & Leandro, 2014)

Así mismo, la debilidad organizacional dificulta la estructuración de los procesos causado por la preferencia al personal no calificado para evitar costos en capital humano, reflejado en el incumplimiento de las necesidades y expectativas de los clientes. Esto representa incrementos en los gastos de producción, ineficiencia de los procesos, centralización de las actividades, mal ambiente laboral, y principalmente conlleva a pérdidas económicas por problemas en ventas y mercadeo (Cruz, López, E., & Meneses, 2016, pp. 330 - 336). Esta situación se presentó en la organización argentina del sector de software y servicios informáticos TEMP, dónde la debilidad empresarial desarrolló la dependencia a un único cliente y se consideró como único factor diferenciador el costo bajo; lo que disminuyó sus ventas y utilidades y comprometió su supervivencia (D' Annunzio & Carattoli, 2014, p. 29).

En Colombia, las MiPymes representan alrededor del 90% del sector productivo nacional, generando el 35% del Producto Interno Bruto – PIB y el 80% del empleo en el país (Ministerio de Trabajo, 2019); sin embargo, más del 60% de las empresas no logran sobrevivir después de los 5 años, a comparación de países como Argentina o Chile, donde la cifra baja alrededor del 50% (Ver gráfica Figura *3*) (Confecámaras, 2017, p. 9). Esto se debe al desequilibrio en la gestión

empresarial reflejado en utilidades mínimas o nulas, posibilidad de expansión y permanencia limitada, desconocimiento en orden financiero, barreras de entidades financieras, impuestos (Trujillo, Gamba, & Arenas, 2016, pp. 13 - 17) ausencia de sistemas de información, ausencia de certificaciones de calidad, atraso y analfabetismo tecnológico, inadecuada gestión del riesgo, entre otras; conllevando a la reducción del flujo de caja sostenible, y posteriormente, a la muerte (Santana, 2017, pp. 51 - 52).

Figura 3.*Comparación de la tasa de supervivencia de MiPymes a los 5 años de edad*



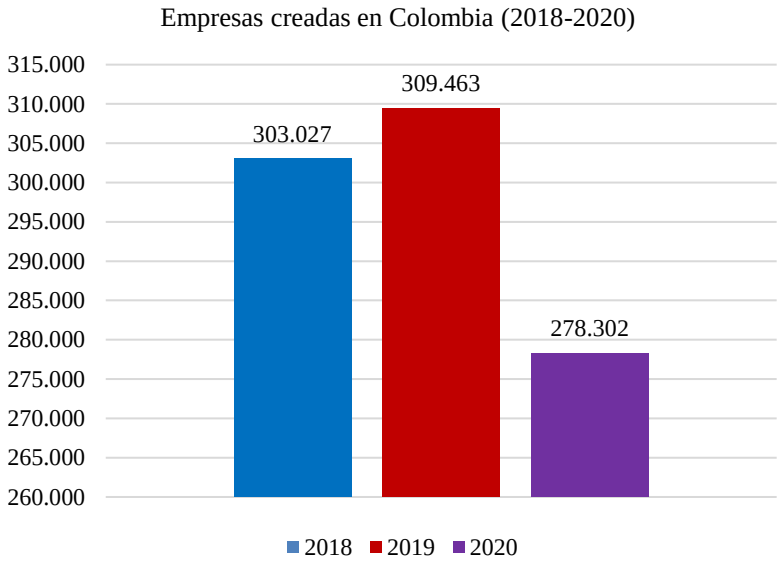
Adaptado de (Asobancaria, 2018).

De igual manera, estas debilidades organizaciones generan que alrededor del 83% de las MiPymes no tienen estandarizados sus procesos empresas; el 50% no poseen control de sus procesos y desconocen los costos asociados a reprocesos y/o salidas no conformes (Ministerio de Comercio, Industria y Turismo, 2022).

Por otra parte, la situación de emergencia dada por el SARS-CoV-2 influyó en la creación y sobrevivencia de empresas en Colombia, con una tendencia decreciente representada en la

muerte de varias organizaciones de agricultura, transporte, energía, construcción, servicios, entre otros, como se muestra en la Figura 4. Debido a las medidas tomadas a nivel nacional, las debilidades organizaciones dejaron expuestas a las MiPymes, sólo las empresas que lograron estructurarse ordenadamente lograron sobrevivir al día de hoy (Confecámaras, 2021, pp. 1 - 14).

Figura 4. *Número de empresas creadas en Colombia entre los años 2018 y 2020*

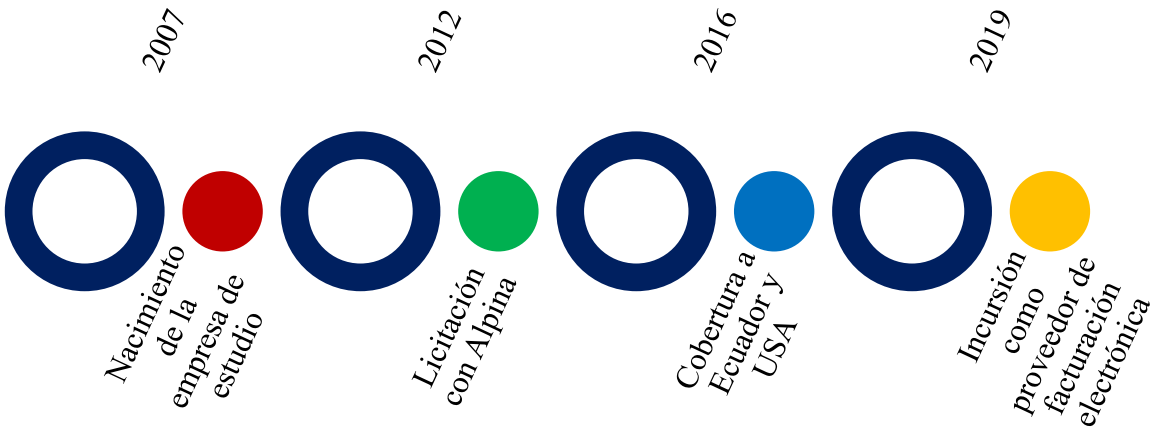


Nota: esta gráfica muestra el impacto en la generación de nuevas empresas en Colombia en el 2020 a causa de la pandemia por el SARS-CoV-2.
Adaptado de (Confecámaras, 2020) y (Confecámaras, 2019).

Asistencia Móvil S.AS. – AMOVIL, organización objeto de este estudio que nació en el 2007 como una empresa santandereana de base familiar, se dedica al desarrollo de aplicaciones móviles y web para la distribución logística de productos de consumo masivo, sus productos son utilizadas por más de 100 organizaciones a nivel nacional. Su oferta de valor se centra en la gestión integral del proceso de distribución logística, la generación de indicadores de desempeño del proceso que facilitan la toma de decisiones y la constante adaptación, mejora e innovación de sus

productos tecnológicos. A partir del lanzamiento de su primera aplicación orientada a la automatización de la fuerza de venta, mantuvo un radio de impacto local hasta su quinto año de funcionamiento cuando logró adjudicarse la licitación con una de las empresas líderes en ventas de productos lácteos a nivel nacional “Alpina”. A partir de ese hito el portafolio de clientes creció a otros países de la región latinoamericana y Estados Unidos. En el 2019, con el objetivo de ofrecer el servicio complementario como proveedor de facturación electrónica validado por la DIAN, la organización obtuvo la certificación de su Sistema de Gestión de Seguridad de la Información de acuerdo a los lineamientos de las NTC ISO/IEC 27001:2013. Para el 2022 AMOVIL logró otro importante hito de crecimiento, obtuvo la adjudicación de la licitación para el desarrollo de un producto para la automatización de los procesos logísticos de una de las empresas más importantes del sector de los alimentos el Grupo Nutresa a través de su distribuidora Comercial Nutresa. (Ver Figura 5) (AMOVIL S.A.S., 2020).

Figura 5. *Línea de tiempo de la empresa de estudio*



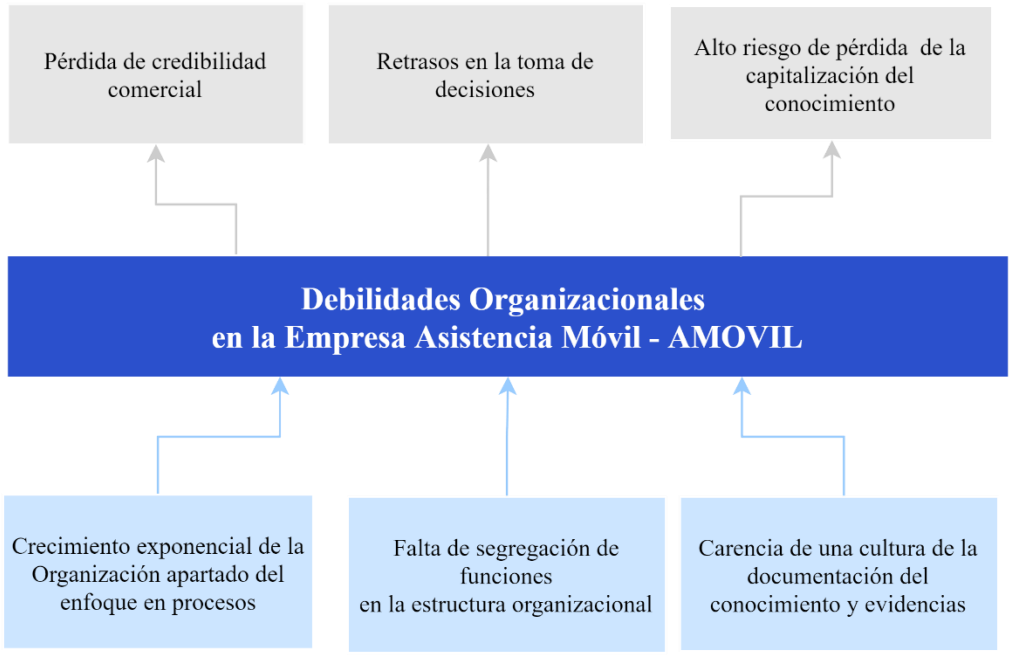
Adaptado de (AMOVIL S.A.S., 2020)

No obstante, tras un periodo de rápido crecimiento la organización ha experimentado los resultados de una débil estructura organizacional, que ha centralizado su direccionamiento en una alta dirección que posee poca formación y experiencia en la administración empresarial; lo que se ha reflejado en una centralización de funciones operativas por encima de las estratégicas, esta situación ha apartado a la organización de una gestión organizada, pragmática y con orientación a los procesos y ha acentuado la carencia de una cultura de la documentación que soporta la gestión del conocimiento y su capitalización (AMOVIL, 2021). Como fue descrito, la organización cuenta con un Sistema de Gestión de Seguridad de la Información que con su certificación viabilizó la participación de la empresa como proveedor tecnológico y también ha profundizado en la necesidad de incorporar elementos de gestión a través de un sistema integrado que aporte a mejorar el desempeño de la organización para el desarrollo de ideas e iniciativas para su desarrollo sostenible.

Dentro de la descriptiva de la problemática abordada, también se identifica que este contexto ha dado lugar o potencializado de manera conjunta y sinérgica, efectos indeseables para la organización como la pérdida de credibilidad comercial ante la falta de agilidad y cumplimientos de tiempos de entrega, reprocesos y falta de escenarios de pruebas de los productos; retrasos en la toma decisiones por la existencia de una estructura organización centralista y un altor riesgo de la pérdida del conocimiento ya que los procesos no han establecido unos lineamientos documentados, reproducibles y revisados de forma periódica.

La problemática descrita en sus elementos más destacados se muestra en la Figura 6.

Figura 6. *Árbol del problema*



Nota: esta imagen muestra el árbol de problemas esquematizado a partir del diagnóstico de la empresa AMOVIL. Se muestran las causas y consecuencias principales.

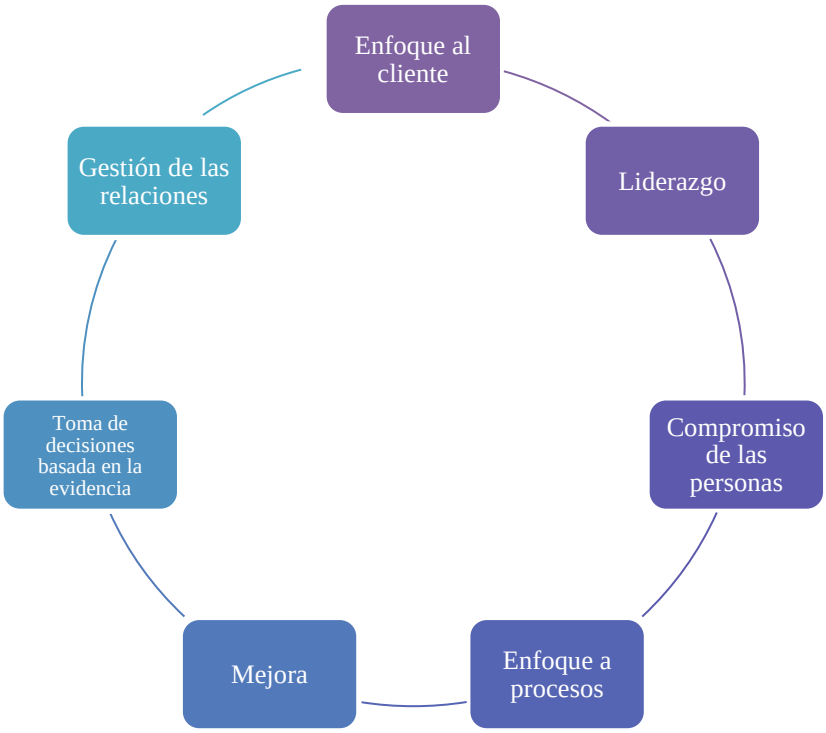
1.2 Justificación

El problema a atender correspondió a la debilidad organizacional producida a raíz de una administración empírica basada en las experiencias de los propietarios de la organización objeto de estudio; por esta razón, se planteó aportar a la solución a través del diseño de un Sistema Integrado de Gestión -SIG que incorporara los requisitos de la norma NTC ISO 9001:2015 que fundamenta el Sistema de Gestión de la Calidad y de esta forma apalancar las bases organizacionales en los principios de gestión basada en procesos, gestión basada en riesgos y una clara definición de los procesos y sus actividades de transformación y por otra parte, la integración de los requisitos de la norma NTC ISO/IEC 27001:2013 del Sistema de Gestión de Seguridad de la Información, implementado previamente por la organización, a través de los cuales se continue

con el aseguramiento de la integridad, confiabilidad y disponibilidad de la información como activo valioso para la organización. De esta forma se propone un SIG que corresponda a una herramienta organizacional que permita correlacionar y coordinar los procesos y recursos y ofrezca una estructura sólida en pro de la calidad de los productos y servicios ofertados (Quintero, 2014).

El alcance del presente estudio correspondió al diseño de este Sistema Integrado de Gestión, el cual incorpora los principios que esquematizan en la Figura *7* y que permiten lograr la satisfacción de las necesidades y expectativas de todas las partes involucradas (ICONTEC, 2015, p. ii).

Figura 7. *Principios de la calidad*



Adaptado de (ICONTEC, 2015)

De esta manera el SIG se convierte en una herramienta que promueve la planificación estratégica mediante el desarrollo de objetivos y estrategias claras para establecer a las organizaciones en su escenario deseado; esto suscita una estructuración de todos los recursos de la organización para el trabajo conjunto en el corto, mediano y largo plazo (Mora, Vera, & Melgarejo, 2013, pp. 80 - 81). Lo anterior, permite la consolidación de una nueva cultura organizacional, desarrollando una gestión sistemática de cada proceso orientado al fortalecimiento y protagonización de los clientes internos y externos generando valor (Hernández, Barrios, & Martínez, 2018, pp. 186, 189) al asegurar un ciclo de mejora continua constituida en la planificación de los procesos, la implementación de los planes propuestos, la verificación y análisis de los resultados obtenidos para una posterior actuación con medidas correspondientes (Ortega, Bustamante, Gutiérrez, & Correa, 2015, pp. 152 - 156). En la Figura 8, se esquematiza el ciclo de mejora continua o ciclo PHVA (Ciclo Planificar-Hacer-Verificar-Actuar) el cual es empleado como elemento relevante para el diseño del Sistema Integrado de Gestión.

Figura 8. *Esquema del ciclo de mejora continua PHVA*

Adaptado de (ICONTEC, 2015)

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un Sistema Integrado de Gestión a través de la integración de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013, que permita el fortalecimiento organizacional de la empresa AMOVIL S.A.S.

1.3.2 Objetivos específicos

- Determinar el nivel de cumplimiento de los requisitos de las normas NTC-ISO 9001:2015 y NTC-IEC 27001:2013 a través de un análisis de brecha, que establezca el nivel de madurez de la implementación.
- Definir los elementos para el diseño del Sistema Integrado de Gestión a través de la metodología del análisis de relación de los requisitos de las normas técnicas, de modo que se asegure la integración.
- Validar el diseño del Sistema Integrado de Gestión a través de un informe de validación bajo criterio técnico de un experto auditor de las normas NTC-ISO 9001:2015 y NTC-IEC 27001:2013, que determine elementos de mejora continua.

2. Marco referencial

2.1 Reseña histórica y caracterización de la empresa

La empresa de estudio Asistencia Móvil S.A.S. conocida comercialmente como AMOVIL, posee una amplia trayectoria como aliado tecnológico de empresas de distribución masiva y ofrece aplicaciones móviles y web con más de 2.500 usuarios activos, 75.000 pedidos y $5.000 millones en transacciones diarias. AMOVIL ofrece productos tecnológicos en los procesos de preventa,

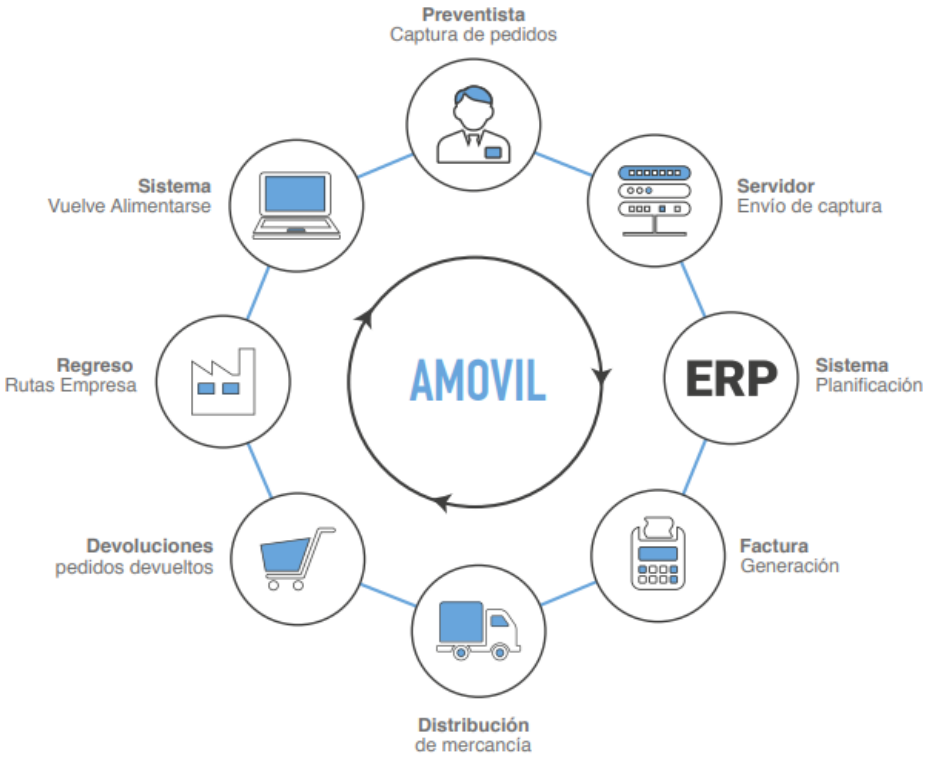
autoventa, supervisión comercial y facturación electrónica, con esta oferta integra de forma completa las actividades del ciclo de gestión de la distribución logística. Adicionalmente, AMOVIL posee un compromiso con sus clientes en la satisfacción total y mejoramiento continuo de los productos o servicios, mediante el contacto directo con servicio al cliente las 24 horas del día los 7 días de la semana (AMOVIL S.A.S., 2020). Dentro de sus 105 clientes, se encuentran los mostrados en la Figura *9*.

Figura 9. *Principales clientes de AMOVIL S.A.S*

Adaptado de (AMOVIL S.A.S., 2020)

Así mismo, AMOVIL brinda apoyo a aquellas empresas que desean mejorar continuamente sus procesos y sus relaciones con sus clientes, acompañándolos y apoyándolos en todo el ciclo transaccional desde sus capturas de pedidos hasta la retroalimentación del sistema con la llegada de las rutas a la empresa, tal y como se muestra en la Figura *10*.

Figura 10. *Participación de AMOVIL en el ciclo transaccional empresarial*



Adaptado de: (AMOVIL S.A.S., 2020)

La historia de AMOVIL comienza en el año 2007 como pionera en la creación de software móvil y web mediante Amovil Preventa como una solución automatizada para ventas. Tres años después, Amovil Preventa emigró a dispositivos móviles, lo que le permitió obtener la licitación con la mayor empresa de ventas de lácteos a nivel nacional “Alpina” en el 2012. Al año siguiente, Asistencia Móvil lanzó al mercado Amovil Autoventa, y Amovil Supervisores para el año 2014; estos progresos proyectaron a AMOVIL como una alternativa de aplicaciones de captura según la revista Enter.co y como aliado del MINTIC con el inicio del programa Apps.co en el año 2015. Este recorrido le permitió a la empresa extender sus operaciones en otras geografías en el 2016, año en el que incursionó con sus productos en Ecuador, ese mismo año añadió un nuevo producto llamado Amovil Distribución; y en el 2017 llegó a Estados Unidos con un modelo 4G. Con los

nuevos requisitos para las empresas dadas por la normatividad colombiana para la facturación electrónica, AMOVIL incursionó como proveedor de esta herramienta con Amovil FELAM en el año 2018, este hecho supuso un nuevo reto: obtener la certificación en el estándar ISO 27001:2013 para la seguridad de la información, cuya implementación comenzó en el 2019; proceso que dio lugar a las mejoras de la herramienta Amovil FELAM 2.0. Finalmente, en ese mismo año desarrolló la nueva aplicación para automatización de pedidos A'pedir. Actualmente, AMOVIL ha movilizado sus esfuerzos a ofrecer un sistema de información tipo ERP que se integra con todas las soluciones tecnológicas de sus productos llamado SIDIS, a través de este producto AMOVIL ofrece un portafolio que completa todas las necesidades de sus clientes desde la toma de pedido hasta el procesamiento y generación de la facturación y manejo de sus inventarios. (AMOVIL S.A.S., 2020).

2.2 Antecedentes

2.2.1 Antecedentes en el ámbito internacional

En España un estudio tomado como referente fue el titulado "Un modelo para facilitar la integración de estándares de gestión de TI en entornos maduros" (Mesquida, 2012, pp. 79 - 108), detalla la relación que tienen las normas ISO 9001:2008, ISO/IEC 20000-1:2005, e ISO/IEC27001:2005 y realiza una guía para la alineación e integración de los sistemas de gestión. A pesar de que la guía se basa en una versión anterior de las normas actuales, permite analizar la metodología usada para el desarrollo de la propuesta en el presente proyecto.

Como primera actividad, en el estudio dirigido para optar por su título de doctorado el autor identificó las estructuras de las normas y destacó que la ISO 9001:2008 posee un apartado de compatibilidad con otros sistemas de gestión y normas de la familia de calidad en campos

específicos tales como: ISO/IEC 90003:2004 dedicada al proceso de desarrollo con calidad del software e ISO/IEC TR 90005:2008 que brinda directrices para la aplicación de la ISO 9001 a los procesos de ciclo de vida del sistema orientada a la ingeniería de sistemas. La ISO 20000-1:2005 posee un enfoque de procesos integrados, permitiendo satisfacer los requisitos del negocio y de los clientes. Finalmente, la norma ISO/IEC 27001:2005 posee un apartado que permite la compatibilidad con las normas ISO 9001:2000 y 14001:2004. Una vez analizadas las posibles compatibilidades, el autor procedió al estudio de las relaciones entre las normas 9001:2008 e ISO/IEC 20000-1 y entre las normas 9001:2008 e ISO/IEC 27001, para lo que estableció 3 tipos de relaciones: relación total, relación parcial e inexistencia de la relación. Con ello, sugirió realizar la recolección de requisitos similares, adaptar los requisitos parciales y resaltar los requisitos específicos para concluir en la elaboración de la guía como herramienta para el cumplimiento de los estándares (Mesquida, 2012, pp. 79 - 108).

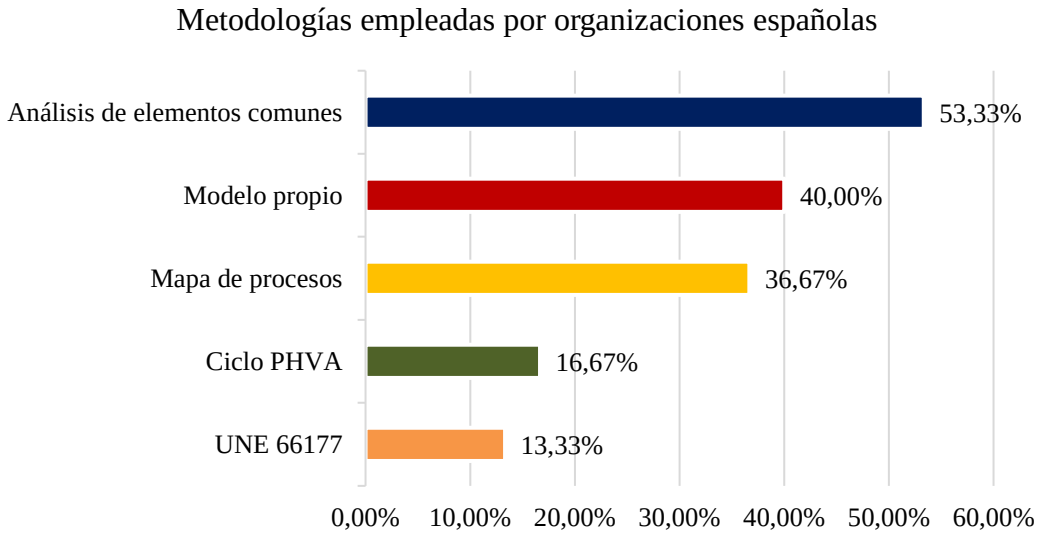
De otra parte, otros referentes como la Agencia de Calidad para el Sistema Universitario de Cataluña (AQU Catalunya – *Agència per a la Qualitat del Sistema Universitari de Catalunya)* resalta que la integración de los sistemas de la seguridad de la información ISO 27001 y de la calidad ISO 9001 permiten garantizar la disponibilidad, integridad y confidencialidad de la información de una organización. Debido a su alta importancia en la formación de las personas, la AQU optó por su certificación en calidad y la certificación en seguridad de la información, con el propósito de llevar a cabo sus procesos de manera ordenada y satisfactoria, mejorando significativamente su imagen corporativa. Este proceso inició alineado la visión estratégica con los procesos y la gestión, para lograr la unanimidad en su mapa de procesos, políticas sinérgicas; la integración de la seguridad de la información en el comité de la calidad, así como sus requisitos en las actividades diarias; y la incorporación en el equipo de auditoría interna de una persona del

área informática. Como resultado se obtuvo la sensibilización del personal sobre la seguridad de la información, la incorporación de nuevos hábitos laborales, la adopción de criterios y normativas para la gestión de la información, un plan de continuidad abarcando todo tipo de riesgos, y sus respectivos controles y medidas de acción. Esto les ha permitió organizar la información de 12 universidades (7 públicas y 5 privadas), 1245 titulaciones (475 pregrados, 570 maestrías y 200 doctorados), 21500 docentes de educación superior, y 51 evaluaciones institucionales (AENOR, 2018, p. 1).

En la región de Latinoamérica, en Ecuador, se desarrolló un estudio para el diseño de un Sistema Integrado de Gestión basado en las normas ISO 9001:2015 e ISO 27001:2013, con énfasis en la emisión de documentos de identificación militar de las Fuerzas Armadas. En primer lugar, el autor realizó una evaluación de cumplimiento de requisitos de ambas normas, para lo que se consideró los apartados de contexto de la organización, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora, y obtuvo un balance general de cumplimiento. Este balance fue el insumo para el diseño de la propuesta de integración de los sistemas de gestión; el análisis de los procesos, aspectos legales y lineamientos para la sinergia adecuada entre la calidad y la seguridad de la información. Dentro del diseño se destacó el cambio del enfoque de la estrategia, la estructuración de los procesos, el establecimiento de la tecnología requerida, la participación del personal, la determinación de los activos de la información y la creación del mapa de riesgos de los activos de la información. Como resultado, el autor obtuvo un manual que brinda herramientas para el establecimiento de los sistemas, sus interrelaciones, formatos, registros y lineamientos para el control de cumplimiento de requisitos (García, 2020, pp. 1 - 241).

Finalmente, en España se realizó un estudio titulado “Nueva metodología desarrollada para la integración de *Lean Manufacturing*, *Kaizen* e ISO 31000:2009 basados en la ISO 9001:2015” el cual sondeó las diferentes metodologías usadas por las organizaciones para la integración de dos o más sistemas de gestión, y el desarrollo de una nueva guía que permitiera facilitar el proceso. En el estudio los autores destacan el enfoque de la norma australiana y neozelandesa AS/NZS 4581:1999 orientada a integrar los sistemas de gestión a partir de la identificación de los elementos comunes para evitar la duplicidad; por su parte la norma danesa *Dansk Standard* DK 8001:2005 que resalta la Excelencia Empresarial como el desarrollo de todos los elementos de la organización en una misma dirección, seguido del abordaje de los elementos similares y diferenciadores de cada sistema para su posterior integración; así como, la norma española UNE 66177:2005 que constituye una guía metodológica para la integración de los sistemas de gestión de calidad, ambiental y seguridad y salud en el trabajo, basado en el ciclo Deming; en el marco del estado del arte destaca además la norma británica PAS 99:2006 que ofrece un marco genérico de requisitos comunes entre los estándares ISO para los sistemas de gestión de la calidad, ambiental y seguridad y salud en el trabajo; finalmente, concluye por resaltar que la ISO a través de su publicación “*The integrated use of management system standards*” que en español corresponde a “El uso integrado de los sistemas de gestión”, detalla metodologías, herramientas y prácticas específicas para integrar los sistemas de gestión de la calidad, ambiental, cadena de suministro, seguridad alimentaria, seguridad de la información y seguridad y salud en el trabajo (Palacios, 2019, pp. 12 - 43)

Figura 11. *Metodologías empleadas por organizaciones españolas*



Nota: esta figura muestra las principales metodologías utilizadas para realizar la integración de sistemas de gestión por parte de organizaciones españolas.
Adaptado de (Palacios, 2019)

De acuerdo a lo se muestra en la Figura *11*, el estudio observó que la metodología más usada es la de análisis de elementos comunes, seguido de la adopción de un modelo propio. Esto ocurre debido a que estas metodologías proponen medidas simples y fáciles de entender. Por esta razón, la metodología creada se basó en el Análisis de Elementos Comunes y en el Ciclo Deming de la siguiente manera (Palacios, 2019, pp. 12 - 43)

2.2.2 Antecedentes en el ámbito nacional

Desde el ámbito nacional, se tomó como referente el trabajo titulado “Guía para la implementación de un Sistema de Gestión Integrado ISO 9001:2015 E ISO/IEC 27001:2013” en el que el autor desarrolló una guía para la implementación de un Sistema de Gestión Integrado ISO 9001 e ISO 27001. Esta guía se planteó para ser aplicada por cualquier organización sin importar tamaño, actividad económica o antigüedad. El investigador determinó los elementos similares y

diferenciadores de cada norma, identificó los beneficios de cada norma de manera integral y por separado; desarrolló una lista de requisitos de ambas normas para su respectivo cumplimiento. Así mismo, estableció herramientas ofimáticas que le permitieron el planteamiento, desarrollo, revisión y actuación del Sistema Integrado de Gestión. Esta guía de implementación permitió a las organizaciones obtener beneficios tales como: aplicar el concepto de calidad a la seguridad, reducir los riesgos, mejorar la competitividad, fortalecer el compromiso y la concientización, y la mejora continua. La primera guía correspondió a la aplicación de la norma ISO 27001, estableciendo un nuevo proceso relacionado a la información, donde la norma ISO 9001 abarcó un enfoque a todos los procesos de la organización. Además, permitió establecer controles para reducir los riesgos de gestión debido al manejo de la información, una mejora en la imagen y un aumento su competitividad frente a las demás organizaciones, así como establecer estándares para la toma de conciencia y formación del compromiso del recurso humano, el cual, es fundamental para lograr el éxito de la organización y su mejoramiento continuo (Pineda, 2017, pp. 14 - 68).

Otro estudio también tomado como referente, llevado a cabo en la ciudad de Bogotá y titulado “Estructuración del Sistema Integrado de Gestión en F1 TOP POINT con base en las normas ISO 9001:2015, ISO 27001:2013, ISO 45001:2018 e ISO 14001:2015” documenta la estructuración de un Sistema Integrado de Gestión para una empresa de actividades de desarrollo de sistemas informáticos. Debido a que la empresa objeto del presente estudio pertenece a esta misma actividad económica y maneja las versiones más actualizadas de las normas, este referente brindó información fundamental para el desarrollo de la consultoría propuesta. En el estudio referenciado el autor implementó 6 fases: fase 1 diagnóstico del estado actual del Sistema de Gestión Integrado, fase 2 actualización del SGC, fase 3 actualización del SGSI, fase 4 estructuración del Sistema de Gestión de Seguridad y Salud en el Trabajo, fase 5 diseño del

Sistema de Gestión Ambiental, y fase 6 finalización del proyecto correspondiente a la socialización de los resultados. La fase diagnóstica se realizó mediante un análisis de fortalezas y debilidad para cada apartado de las normas ISO 9001:2015, ISO 27001:2013, ISO 45001:2018 e ISO 14001:2015; de esta manera, logró resumir las no conformidades y las conformidades. Con base al diagnóstico, determinó los controles orientados al mejoramiento de los Sistemas analizados, lo que permitió mejorar los sistemas de calidad y seguridad de la información, y estructurar y diseñar los sistemas de ambiente y seguridad y salud en el trabajo. Finalmente, el documento ofrece los lineamientos a seguir por la empresa para la integración de los sistemas de gestión en cumplimiento con las normas ISO 9001:2015, ISO 27001:2013, ISO 45001:2018 e ISO 14001:2015; y optimizar los procesos de la organización (Rincón, 2019, pp. 12 - 89).

Finalmente, en la misma ciudad se desarrolló una guía para la armonización de la gestión documental para los sistemas de gestión de la calidad y de la seguridad de la información. En primera instancia, se realizó un diagnóstico para concretar la situación actual y el grado de cumplimiento de la gestión documental conforme al Decreto 1080 de 2015, los procesos y controles según la norma ISO 30301, ISO 27001 e ISO 9001, principalmente el numeral 7.5. “Información documentada”. Esto permitió elaborar la guía de armonización teniendo en cuenta los requisitos similares y diferenciadores de cada norma para su posterior validación. Esta fase se realizó mediante un cuestionario a un grupo de expertos, a través de la cual se confirmó su claridad, pertinencia y aplicabilidad (Triana, 2020).

2.3 Marco teórico

Los conceptos calidad, seguridad de la información e integración son sin duda referentes claves para la comprensión y adecuada aproximación al presente trabajo. A continuación, se

aborda su comprensión conceptual, así como, la de otros términos asociados que en conjunto aportan a la contextualización de la problemática objeto de estudio.

2.3.1 Calidad

Es el resultado cultural dada por la gestión de comportamientos, actitudes, actividades y procesos, orientadas al cumplimiento de las necesidades y expectativas de todas las partes interesadas (ICONTEC, 2015, p. 2).

2.3.2 Seguridad de la información

Corresponde a la confidencialidad, integridad y disponibilidad de la información que posee una organización (ISO 27001, 2013). Así mismo, se considera como el conjunto de medidas técnicas, organizativas y legales que llevan a cabo las organizaciones para salvaguarda su información y de las partes interesadas. Se tiene en cuenta que la confidencialidad permite ocultar o mantener en secreto para evitar perjuicios al dueño de la información; la integridad evita la modificación o alteración de la información, garantizar su veracidad e impacto; finalmente, la disponibilidad garantiza el acceso a las personas autorizadas, facilitando su manejo y gestión (Calderón, 2015, p. 2).

2.3.3 Sistema de gestión

Es una herramienta organizacional conformada por políticas, objetivos y procesos, debidamente interrelacionados o con interacción constante. Este modelo se orienta a diferentes necesidades de las empresas con el fin de dar respuesta conforme a buenas prácticas implementadas y perfeccionadas (ICONTEC, 2015, p. 18), dónde se profundizarán principalmente en dos: calidad y seguridad de la información.

2.3.4 Sistema de Gestión de la Calidad NTC-ISO 9001:2015

Este sistema de gestión provee una dirección estratégica a una organización, orientada a mejorar su desempeño global y proporcionar una base sólida para el desarrollo sostenible. Algunos beneficios son: generar la capacidad de proporcionar regularmente productos y servicios que permitan satisfacer los requisitos de los clientes y los requisitos legales y reglamentarios, incrementar las oportunidades de satisfacer al cliente, abordar riesgos y oportunidades y la capacidad de generar conformidades con requisitos del sistema de gestión de la calidad especificados. Con la norma ISO 9001:2015, se posee una estructura Deming: Planificar, Hacer, Verificar y Actuar (PHVA) y pensamiento basado en riesgos. Así mismo, se basa en los principios como enfoque al cliente, liderazgo, compromiso con las personas, enfoque a procesos, mejora, toma de decisiones basado en la evidencia y gestión de las relaciones (ICONTEC, 2015, pp. ii - iv).

2.3.5 Sistema de Gestión de la Seguridad de la Información

Este sistema de gestión busca preservar la confidencialidad, la integridad y la disponibilidad de la información mediante la gestión adecuada de los riesgos, lo que brinda confianza a las partes interesadas. Así mismo, la organización debe considerar la seguridad de la información como parte de los procesos y estructura de la misma para permitir la gestión total de la información interna y de las partes interesadas. Adicionalmente, la norma NTC-ISO/IEC 27001 es compatible con las directivas ISO/IEC, parte 1, Suplemento ISO consolidado y con otras normas de sistemas de gestión. Por esta razón, es posible establecer una integración con el Sistema de Gestión de la Calidad NTC-ISO 9001:2015 (ICONTEC, 2013, p. 1).

2.3.6 Integración de Sistemas de Gestión

La integración de sistemas de gestión corresponde a la unificación de requisitos iguales, complementar los requisitos similares y gestionar los requisitos específicos para consolidar un único sistema bajo una misma estructura (Heras, Bernando, & Casadesús, 2007, pp. 155-174).

Así mismo, cuando se realiza la integración de dos más sistemas de gestión surge un Sistema Integrado de Gestión, correspondiente a un sistema interdisciplinario, conformado por la estructura de la organización, sus recursos y responsabilidades, direccionados hacia un mismo fin, lo que evita la duplicidad de procesos e información y optimiza los procesos. Por esta razón, el presente trabajo se desarrolló mediante una metodología de integración de normas ISO, teniendo en cuenta que estas normas de estandarización poseen una misma estructura.

De igual manera, se menciona a continuación las metodologías de integración de sistemas de gestión más comunes entre las organizaciones:

2.3.6.1 Integración por Ciclo PHVA. Este modelo resalta las fases del ciclo Deming o PHVA como lineamientos para realizar la integración de varios sistemas de gestión. Esto quiere decir, que se realiza la panificación de los elementos estratégicos y la distribución de los recursos de la organización, bajo los criterios establecidos por las normas a adoptar. Seguido, se implementa lo planificado mediante la interrelación de los recursos, evitando reprocesos y cubriendo cada una de las normas establecidas. Luego, se realizar una verificación mediante auditorías internas combinadas o complementarias, que permitan comprender el estado en el que se encuentran de manera conjunta. Finalmente, se toman acciones que permitan el mejoramiento sinérgico de los sistemas, permitiendo cumplir con el ciclo (Forbes, 2011, pp. 1 - 5).

Este modelo permite ahorrar tiempo, debido a que se desarrolla por etapas, permite trabajar en todos los sistemas al mismo tiempo, unificando las actividades y tiempos. Sin embargo, se debe complementar con otros modelos para relacionar los diversos requisitos de las normas (Duque, 2017, pp. 115 - 130).

2.3.6.2 Integración por Elementos Comunes. La integración por elementos comunes permite revisar y clasificar los requisitos de las normas teniendo en cuenta los siguientes criterios (Antúnez, 2016, pp. 1-28):

- Requisitos con relación total: son aquellos que permiten unificarse en un solo documento, procedimiento, actividad, recursos, etc.
- Requisitos con relación parcial: son aquellos que permiten combinarse manteniendo las características propias de cada norma, o realizarse de manera conjunta bajo un estándar.
- Requisitos con relación nula: son aquellos que no permiten unificarse debido a su naturaleza propia de la norma; es decir, que no se comparte con las demás.

Esta metodología facilita y complementa al ciclo PHVA, ya que permite definir la ruta de integración del sistema de manera ágil y ordenada, optimizando los procesos (Parra, Hernández, & y Rodríguez, pp. 1-17).

2.3.6.3 Norma PAS 99. Esta norma internacional surge de la necesidad de facilitar la implementación de los sistemas de gestión en las organizaciones mediante la integración de criterios y requisitos. Por esta razón, esta norma considera seis requisitos comunes fundamentales, incluye el modelo PHVA, y promueve el desarrollo de Sistemas de Gestión de forma holística, mediante la siguiente estructura (Miguel, 2013, pp. 8-12):

- Contexto de la organización
- Liderazgo
- Planificación
- Soporte
- Operación
- Evaluación del desempeño
- Mejora

Esta norma aconseja la integración mediante los 7 elementos comunes mencionados anteriormente, y los requisitos específicos de cada norma a adoptar. Así mismo, conlleva beneficios estratégicos mediante la unificación de objetivos, metas y rutas; direccionando todos los procesos de la organización (Miguel, 2013, pp. 8-12).

2.4 Marco conceptual

Con el propósito de comprender los términos específicos relacionados al tema de Sistemas de Gestión, se exponen los siguientes conceptos:

2.4.1 Contexto de la organización

Permite exponer y comprender los factores internos y externos que influyen en la organización en todos sus aspectos. De igual manera, los factores internos son aquellos que la

misma organización puede controlar o gestionar tal como la cultura organizacional, valores, desempeño, infraestructura, etc. Por otro lado, los factores externos son aquellos que no son controlados y manejados por la organización, pero sí pueden ser gestionados como oportunidades o representar riesgos en el cumplimiento de sus objetivos; entre ellos se destaca el entorno legal, tecnológico, mercado, cultura social, etc. (ICONTEC, 2015, p. 2).

2.4.2 Partes interesadas

Anteriormente se poseía el enfoque de gestionar únicamente las necesidades y expectativas de los clientes; sin embargo, a lo largo del tiempo se ha evidenciado el requerimiento de considerar a todas las partes pertinentes, ya que no sólo los clientes pueden llegar a influir al momento de gestionar un sistema. Por esta razón, se considera una parte interesada aquella persona natural o jurídica que puede generar un riesgo significativo en la sostenibilidad organizacional, es decir, en el desarrollo de los objetivos (ICONTEC, 2015, p. 2).

2.4.3 No conformidad

Es un posible resultado en la verificación del sistema de gestión, y se presenta cuando existe un incumplimiento total o parcial de un requisito, es decir, de una necesidad o expectativa obligatoria (ICONTEC, 2015, p. 20). Estas representan una oportunidad de mejora del sistema para alcanzar el cumplimiento del requisito y su sostenimiento en el tiempo; donde dependiendo de su impacto, puede clasificarse en una No conformidad mayor o menor (ICONTEC, 2018, p. 32).

2.4.4 Acción correctiva

Una vez identificada la no conformidad, se desarrollan una serie de actividades encaminadas a eliminar su causa y prevenir su recurrencia (ICONTEC, 2015, p. 30). Es decir, estas acciones permiten el mejoramiento del sistema de gestión.

2.4.5 Verificación

Esta actividad permite conocer el estado de cumplimiento de requisitos específicos teniendo en cuenta información objetiva del sistema (ICONTEC, 2015, p. 25), es decir, recolecta toda la información posible para comprobar el cumplimiento de lo establecido por la norma, la organización y la legislación.

2.4.6 Validación

Esta actividad es similar a la anterior, ya que se desarrolla una comprobación frente a requisitos establecidos, pero ésta se realiza con el fin de garantizar que lo implementado y ejecutado funcione para cumplir los requerimientos establecidos (ICONTEC, 2015, p. 25).

2.5 Marco legal

En la Tabla *1* se expone la normatividad vigente aplicable:

Tabla 1. *Marco normativo*

Nombre	Año	Entidad	Descripción
Ley 0590	2000	Congreso de Colombia	Por la cual se dicta disposiciones para promover el desarrollo de las micro, pequeñas y medianas empresas.
Ley 1581	2012	Congreso de Colombia	Por la cual se dicta disposiciones generales para la protección de datos personales.
Decreto 1595	2015	MinComercio	Por la cual se regulan los entes de certificación y acreditación.
Ley 1032	2006	Congreso de la República	Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Protección de la información y de los datos (delitos informáticos)

Nombre	Año	Entidad	Descripción
Ley 1273	2009	Congreso de la República	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.
Decreto 2242	2015	DIAN	Por la cual se reglamentan las condiciones de expedición e Inter portabilidad de la factura electrónica con fines de masificación y control fiscal.
Resolución 0019	2016	DIAN	Mediante la cual se prescribe un sistema técnico de control para la factura electrónica acorde con el Decreto 2242 de 2015, se señalan los procedimientos que deben agotar y los requisitos que deben cumplir los sujetos del ámbito de este decreto y se disponen otros aspectos en relación con la factura electrónica.
Resolución 00639	2019	DIAN	Por medio de la cual se otorga una autorización para prestar los servicios como proveedor tecnológico de Factura Electrónica Asistencia Móvil SAS
Resolución 0030	2019	DIAN	Por lo cual se señalan los requisitos de la Factura Electrónica de venta con validación previa a su expedición, así como, las condiciones, términos y mecanismos técnicos y tecnológicos para su implementación.
Resolución 0042	2020	DIAN	Por la cual se desarrollan los sistemas de facturación electrónica, proveedores tecnológicos, registro de factura electrónica, y otras disposiciones.
Resolución 0094	2020	DIAN	Por la cual se desarrollan los sistemas de facturación, los proveedores tecnológicos, el registro de la factura electrónica de venta como título valor, se expide el anexo técnico de factura electrónica de venta y se dictan otras disposiciones en materia de sistemas de facturación.
Ley 1581	2012	Congreso de la República	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 1377	2013	Congreso de la República	"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
Decreto 886	2014	Congreso de la República	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Ley 1266	2008	Congreso de la República	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Nombre	Año	Entidad	Descripción
Sentencia C-748	2011	Corte Constitucional	La Corte Constitucional declaró la constitucionalidad del articulado del proyecto de ley estatutaria que regula el tratamiento de datos diferentes a los financieros y comerciales con fines de cálculo de riesgo, que ya fueron regulados en otra Ley estatutaria 1266 de 2008
Ley 1221	2008	Congreso de la República	Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones. ARTÍCULO 7o. GARANTÍA LEGAL. Es la obligación, en los términos de esta ley, a cargo de todo productor y/o proveedor de responder por la calidad, idoneidad, seguridad y el buen estado y funcionamiento de los productos.
NTC ISO 9001	2015	ICONTEC	Norma Técnica Colombia de Sistemas de Gestión de la Calidad. Requisitos.
NTC ISO/IEC 27001	2013	ICONTEC	Norma Técnica Colombiana de Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
GTC ISO 19001	2018	ICONTEC	Guía Técnica Colombiana. Directrices para la auditoría de los sistemas de gestión.
GTC ISO 10014	2021	ICONTEC	Guía Técnica Colombiana. Gestión de una organización para resultados de calidad. Orientación para obtener beneficios financieros y económicos

Nota: esta tabla muestra los requisitos legales y normativos más significativas para el desarrollo del trabajo.

3. Método

Para el desarrollo del presente estudio se optó por implementar la metodología de análisis de elementos comunes con la articulación de las actividades basadas en el ciclo Deming o ciclo PHVA propuesta por (Palacios, 2019, pp. 12-43), en la consideración de que ambas perspectivas aportan elementos complementarios para asegurar una integración eficaz, a la vez que se asegura la incorporación de los elementos normativos a lo largo de todo el ciclo de gestión. Pese a que en el estudio realizado por los investigadores la metodología no fue aplicada directamente en la integración de un sistema de gestión basado en las normas NTC-ISO 9001:2015 y NTC-ISO/IEC

27001:2013, la transversalidad con estos sistemas de gestión habilita su aplicación para este caso de estudio.

La metodología conserva un enfoque mixto, ya que se incluye la recolección y análisis de información cuantitativa, tal como las valoraciones y cuantificación del nivel de cumplimiento de los requisitos; y cualitativa, como los aspectos y descripciones de los procesos, actividades y criterios de control. Toda esta información se articuló a lo largo del proceso resolutivo de la pregunta de investigación.

El planteamiento metodológico se basó en tres (3) fases, en las que a su vez se incluyeron las siguientes actividades específicas:

3.1 Fase de planificación

La primera fase metodológica corresponde a la planeación del diseño del Sistema Integrado de Gestión. Esta fase está integrada por las siguientes actividades principales:

3.1.1 Compromiso de la Alta Dirección

Como decisión estratégica, la planeación inició con la toma de decisión por parte de la Alta Dirección de AMOVIL S.A.S de comprometer los recursos y tiempos asociados al logro del objetivo de diseñar un Sistema Integrado de Gestión que asegure el cumplimiento de los requisitos normativos de calidad y seguridad de la información. Asociada a esta actividad se consolidó el equipo de trabajo encargado de liderar y asegurar el proceso de diseño, así como, el nombramiento de los mandos medios correspondientes a los responsables de proceso.

3.1.2 Diagnóstico preliminar

Se realizó el diagnóstico del estado inicial frente al cumplimiento de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013 (considerando los requisitos desde el capítulo 4 hasta el capítulo 10, incluyendo el Anexo A de la NTC ISO/IEC 27001:2013). Para ello, se ejecutó un análisis de brecha con la estructura sugerida por plantillas de uso gratuito disponibles en la red, a las cuales se articularon las preguntas de evaluación sugeridas en el (Cuestionario para la realización de auditoría interna de un sistema de gestión de la calidad. Norma ISO 9001:2015), que permitieron la identificación del nivel de cumplimiento de cada requisito y la verificación de las evidencias disponibles, integrando una valoración porcentual del nivel de cumplimiento que toma como referencia los niveles de madurez sugeridos en (ICONTEC, 2021, p. 18). Para cada norma se desarrolló una hoja de cálculo y análisis de brecha a través de la interpretación gráfica de los resultados en un esquema tipo radar. En la Tabla *2* se muestra la estructura de la hoja de cálculo del análisis de brecha.

Tabla 2. *Estructura del análisis de brecha de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013*

Numeral	Requisito	Estado[a]	Preguntas	Documento Asociado	Comentarios
Sección de la norma evaluada	Requisito evaluado	Valoración del estado de implementación	Preguntas sugeridas para la verificación	Soporte de implementación	Observaciones y comentarios

Nota: esta tabla muestra la estructura utilizada para identificar las brechas de implementación de las normas.
a El Estado se determina a partir de la verificación de la evidencia o soporte de implementación y su valoración respecto a los criterios de calificación.
Adaptado de (Cuestionario para la realización de auditoría interna de un sistema de gestión de la calidad. Norma ISO 9001:2015)

Ejecutado el diagnóstico del estado de cumplimiento de cada numeral de ambas normas, se revisó y analizó el porcentaje de cumplimiento según los siguientes criterios que se muestran en la Tabla 3.

Tabla 3. *Niveles de la madurez de implementación de los sistemas de gestión de acuerdo con la NTC-ISO 10014:2021*

Calificación	Criterio
Desconocido	No ha sido verificado.
Sin implementación	No hay un enfoque sistemático evidente, no hay métricas u objetivos
Poca implementación	Enfoque reactivo, principalmente para corregir problemas
Implementación parcial	Más proactivo que reactivo. Información disponible sobre los objetivos y el desempeño
Prácticamente implementado como rutina	El proceso de mejora continua está bien integrado en la organización
Implementado totalmente como rutina y efectivo	Evidencia sostenida a lo largo de un largo periodo
No aplicable	Requisito no aplicable de acuerdo con el alcance del SIG.

Nota: esta tabla muestra los criterios cualitativos para determinación de los niveles de madurez de la implementación de los sistemas de gestión.
Adaptado de (ICONTEC, 2021)

Para el caso particular de los controles de seguridad de la información sugeridos en el Anexo A de la norma NTC-ISO/IEC 27001:2013, se ejecutó también un análisis de brecha, pero el comparativo del nivel implementación se realizó respecto con la escala de madurez propuesta por el Modelo de Madurez de COBIT® (Gorgona, 2021, pp. 1-3) que se muestra en la Tabla *4*.

Tabla 4. *Niveles de madurez de los sistemas de tecnologías de la información de acuerdo con el modelo COBIT*

Calificación	Criterio
Desconocido	No ha sido verificado.
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de alta calidad.

Calificación	Criterio
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay información.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni por el Comité de dirección.
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo con un procedimiento documenta aprobado y formalizado, y su eficiencia se mide periódicame mediante indicadores.
No Aplicable	El control no es aplicable y se justifica su exclusión del alcance del sistema de seguridad de la información.

Nota: esta tabla muestra los criterios cualitativos para la determinación del nivel de madurez en la implementación de los sistemas de gestión de tecnologías de la información.
Adaptado de (Gorgona, 2021)

3.2 Fase de ejecución

3.2.1 Diseño del Sistema Integrado de Gestión

Posteriormente se realizó el análisis de relación uno a uno de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013, siguiendo para ello la siguiente categorización de los niveles de correspondencia o relación sugeridos por (Mesquida, 2012, pp. 92-105)

- Relación total (T): para este caso el requisito de la norma NTC-ISO/IEC 27001:2013, ya está contemplado por algún requisito de la norma NTC-ISO 9001:2015. Para este escenario no se necesita la implementación de ningún elemento específico de una u otra norma.
- Relación parcial (P): para este caso el requisito de la norma NTC-ISO/IEC 27001:2013, detalla o específica alguna medida particular respecto a lo que establece el requisito para la norma NTC-ISO 9001:2015 o viceversa.
- Inexistencia de relación (X): para este particular los requisitos corresponden a aquellos específicos del objeto y campo de aplicación de las normas respectivas.

Una vez realizado el análisis de relación, se estructuró un plan de integración con el propósito de asegurar el cumplimiento global de los requisitos, orientado al cierre de brechas y al aseguramiento de la integración. En la Tabla *5.* se describe la estructura del análisis de relación de los requisitos de ambas normas.

Tabla 5. *Estructura del análisis de relación de los requisitos de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013*

Requisito Norma NTC ISO 9001:2015		**Tipo de Relación**	**Requisito Norma NTC ISO/IEC 27001:2013**	
Sección de la norma evaluada	Requisito evaluado	Relación total (T) Relación parcial (P) Relación inexistente (X)	Sección de la norma evaluada	Requisito evaluado

Nota: esta tabla muestra la estructura del análisis de relación de requisitos entre las normas. Adaptado de (Mesquida, 2012)

El plan de integración se estructuró basado en un plan de trabajo detallado conformado por los siguientes aspectos: ID o ítem consecutivo de planeación, descripción de la actividad de integración a realizar siguiendo las etapas del ciclo PHVA, fecha inicial y fecha final, responsable de la implementación, observación asociada a la ejecución y el título del documento o registro evidencia del cierre. Las actividades de integración, a su vez fueron planteadas siguiendo la clasificación del nivel de relación de los requisitos de las normas, iniciando por aquellos con relación total, seguidamente por los requisitos de relación parcial y finalizando con los requisitos con inexistencia de relación. Se consideró en todo caso, la facilidad y agilidad en el proceso de implementación para aquellos requisitos que son comunes para ambas normas. En la integración.

Tabla 6. se muestra la estructura del plan de integración.

Tabla 6. *Estructura del plan de integración de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013.*

ID	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Observación	Evidencia
Numeración ítem de planeación.	Requisito de las normas NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013	Actividad de integración a realizar.	Fecha de cierre de la actividad propuesta.	Responsable de avance en la ejecución de la actividad.	Observaciones asociadas el proceso de implementación.	Registro o evidencia del cierre de la actividad.

Nota: esta tabla muestra la estructura del plan de trabajo del presente proyecto.

3.2.2 Implementación del Sistema Integrado de Gestión

Esta fase abarcó todas las actividades de implementación del plan de integración. Incluye la documentación de los lineamientos del nuevo Sistema Integrado de Gestión (manuales, políticas, programas, planes, procedimientos, instructivos, anexos, documentos externos, etc.); surte las respectivas etapas de revisión, aprobación y publicación. Esta actividad fue ejecutada de modo paralelo a la implementación efectiva de una parte importante de los lineamientos del SIG.

Sin embargo, pese a lo antes expuesto no se logró desarrollar la implementación de la totalidad de los lineamientos del diseño del SIG. Las razones de este imprevisto investigativo se deben al desistimiento por parte de la organización quien optó en la no implementación de los lineamientos del sistema de calidad justo en la fase en la que ya habíamos avanzado en un 90% del plan de integración. Esta circunstancia hizo que optáramos por la modificación del título y alcance de este proyecto. A pesar de esta circunstancia de aparente adversidad, nosotras como investigadoras recogimos la información recopilada hasta el momento para fortalecer el rumbo del trabajo. De ahí que la fase nombrada como “implementación” continúa vigente en el diseño metodológico.

Además, se mantuvo un acompañamiento permanente que permitió realizar el aseguramiento de la implementación a través de la revisión periódica de las evidencias del control operacional, el control de riesgos y el cumplimiento de requisitos normativos y legales, con la que se generó la información documentada de la ejecución del SIG.

3.3 Fase de validación

La misma norma NTC ISO 9001 en su versión 2015 define a la validación como "las actividades para asegurarse de que los productos y servicios resultantes satisfacen los requisitos para su aplicación o uso específico" (ICONTEC, 2015). Por su parte como herramienta de validación en numerosos ejercicios de diseño de herramientas o modelos se ha implementado la metodología de validación de contenido a partir de criterio de experto. Esta metodología "consiste, básicamente, en solicitar a una serie de personas la demanda de un juicio hacia un objeto, un instrumento, un material de enseñanza, o su opinión respecto a un aspecto concreto" (Escobar & Cuervo, 2008, pp. 27-36)

Como actividad clave de validación se realizó una valoración del diseño a partir del juicio de una experta en el diseño e implementación de sistemas integrados de gestión que articulan los requisitos de las normas objeto de este estudio. La experticia y formación de la experta se soportan a través de su hoja de vida y los soportes asociados, los cuales pueden verificarse en el Apéndice *A*.

La estructura del informe de validación por criterio de experto incluyó la exploración uno a uno de los requisitos de las normas NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013, en orientación con el ciclo PHVA, se priorizó la revisión a partir de la metodología de correlación de los mismos (relación total, relación parcial e inexistencia de relación), además, el informe acotó el

título del documento evidencia del desarrollo documental del requisito, la valoración cualitativa de cumplimiento (Si o No) y finalmente, las observaciones por parte del evaluador.

4. Resultados

4.1 Fase de planificación

4.1.1 Compromiso de la Alta Dirección

La ejecución del plan de implementación del Sistema Integrado de Gestión, dio inicio con la formalización del compromiso de la Alta Dirección y la conformación del equipo de implementación. El equipo fue integrado por las personas asignadas a los cargos de: director administrativo, director de gestión de proyectos y desarrollo, director comercial y el gerente general de Amovil S.A.S, así como, por un profesional consultor certificado como auditor ISO 27001 y las autoras del presente proyecto de grado en la modalidad de consultoría, con formación como auditores internas ISO 9001. Se realizó, además, la asignación de las responsabilidades respectivas dentro del Equipo SIG, como se indica en la Tabla *7*.

Tabla 7. *Integrantes y responsabilidades del equipo de implementación*

Partes	Integrantes	Responsabilidades
Asistencia Móvil S.A.S - AMOVIL	Gerente General Directora Administrativa Director Comercial Director Gestión de Proyectos y Desarrollo	•Aprobar los elementos de diseño del SIG •Generar los documentos asociados al SIG •Implementar los lineamientos del SIG en el marco de sus procesos •Realizar seguimiento al plan de integración del SIG •Atender el proceso de auditoría interna del SIG
Apoyo SIG	Asesora INNOVIC S.A.S Gestora SIG	•Ofrecer asesoría en la implementación de los lineamientos técnicos de la NTC ISO/IEC 27001:2013 •Realizar aseguramiento de la implementación del Anexo A. Objetivos de control y controles de

Partes	Integrantes	Responsabilidades
		referencia de la NTC ISO/IEC 27001:2013 •Realizar el proceso de auditoría interna del SIG
	Estudiantes Maestría Calidad y Gestión Integral USTA	•Proponer los elementos de diseño del SIG •Generar el plan de integración del SIG •Ofrecer asesoría en la implementación de los lineamientos técnicos de la NTC ISO 9001:2015 •Apoyar la generación de documentos asociados al SIG •Realizar aseguramiento periódico de la implementación de lineamientos del SIG

Nota: esta tabla muestra los miembros y responsables del equipo de implementación del sistema integrado de gestión.

En el marco de la misma actividad la Gerencia General de AMOVIL definió los responsables de los procesos estratégicos, misionales y de apoyo, elementos claves para la implementación de los lineamientos del SIG. La asignación de responsables se muestra en la Tabla *8*.

Tabla 8. *Responsables de procesos estratégicos, misionales y de apoyo*

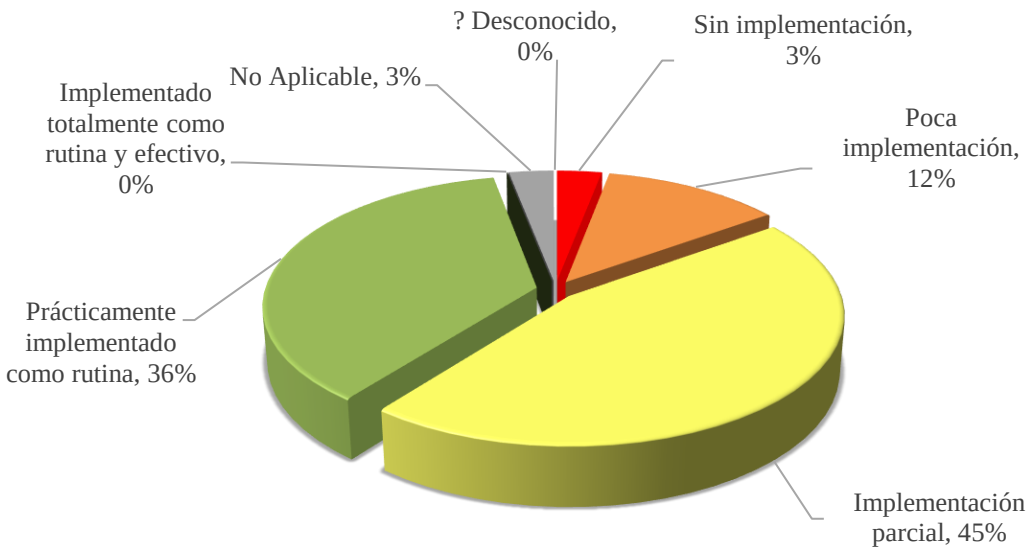
Tipo de Proceso	Proceso	Responsable Asignado
Estratégico	Direccionamiento Estratégico - DE	Gerente General
	Sistema Integrado de Gestión - SIG	Gestor SIG
Misionales	Gestión Comercial - GC	Director Comercial
	Gestión de Proyectos y Desarrollo - GPD	Director de Proyectos y Desarrollo
	Implementación y Soporte - IMS	Líder de Implementación
		Líder de Mesa de Ayuda
	Operaciones de Tecnologías de la Información - OTI	Director de Operaciones
Apoyo	Gestión Administrativa, Financiera y de Talento Humano - GAF	Directora Administrativa

Nota: esta tabla muestra los procesos organizacionales de AMOVIL y los cargos responsables asignados.

4.1.2 Diagnóstico preliminar

El diagnóstico preliminar del estado de cumplimiento de los requisitos de las NTC ISO 9001:2015 y NTC ISO 27001:2013 se realizó a través de un análisis de brecha. Las herramientas aplicadas para realizar la medición se muestran en el Apéndice *B*. La medición fue realizada a través de entrevistas con el personal operativo y administrativo, y la revisión de la información documentada. Posteriormente, cada requisito fue valorado cualitativamente frente a los criterios sugeridos por la NTC-ISO 10014:2021. Gestión de la Calidad. Directrices para obtener beneficios financieros y económicos. En la Figura *12* se esquematizan los resultados derivados del análisis de brecha para la norma de calidad.

Figura 12. *Resultados del diagnóstico de implementación de la NTC ISO 9001:2015*

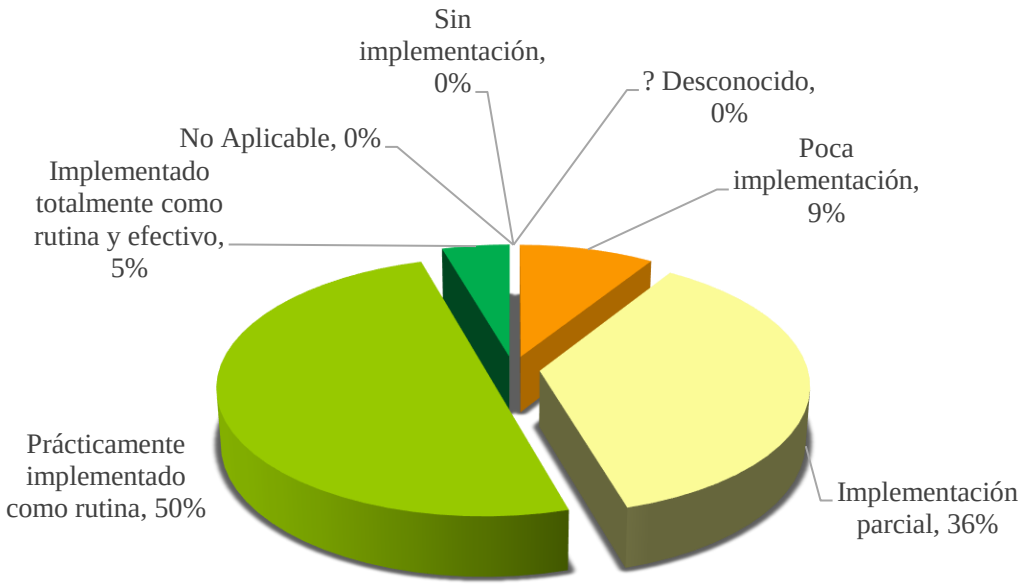


De acuerdo a los resultados consolidados, ninguno de los requisitos de la norma NTC ISO 9001:2015 se valoró en un estado de implementación total, siendo que en todos los casos se identificaron aspectos susceptibles a la mejora, en relación a su documentación y/o

implementación. Un 36% de los requisitos se valoraron prácticamente implementados como rutina, lo que corresponde a una práctica típica, solo con algunas excepciones. El 45% de los requisitos obtuvo una valoración de implementación parcial, lo que corresponde a prácticas comunes, pero no en la mayoría de las áreas. El 12% de los requisitos se categorización en un nivel de poca implementación, es decir que la práctica sólo se ve en algunas áreas. Y, por último, el 3% de los requisitos se evidenciaron sin implementación. En lo relacionado a las no aplicabilidades, el 3% de los requisitos de la norma NTC ISO 9001:2015 no son aplicables al alcance del Sistema de Gestión de Calidad y corresponde al numeral 7.1.5 Recursos de seguimiento y medición. Todos los requisitos fueron validados, por tanto, ningún requisito fue categorizado con estado desconocido.

En la Figura *13* se muestran los resultados del diagnóstico de la NTC ISO/IEC 27001:2013. Los resultados, aunque comparables en algunos numerales con los obtenidos para la implementación de la NTC ISO 9001:2015, difirieron para algunos de los requisitos, siendo que la empresa había previamente adelantado la implementación de un Sistema de Gestión de la Seguridad de la Información y a que en aspectos particulares los mismos requisitos para NTC ISO 9001:2015 incluyen un mayor grado de especificidad o detalle.

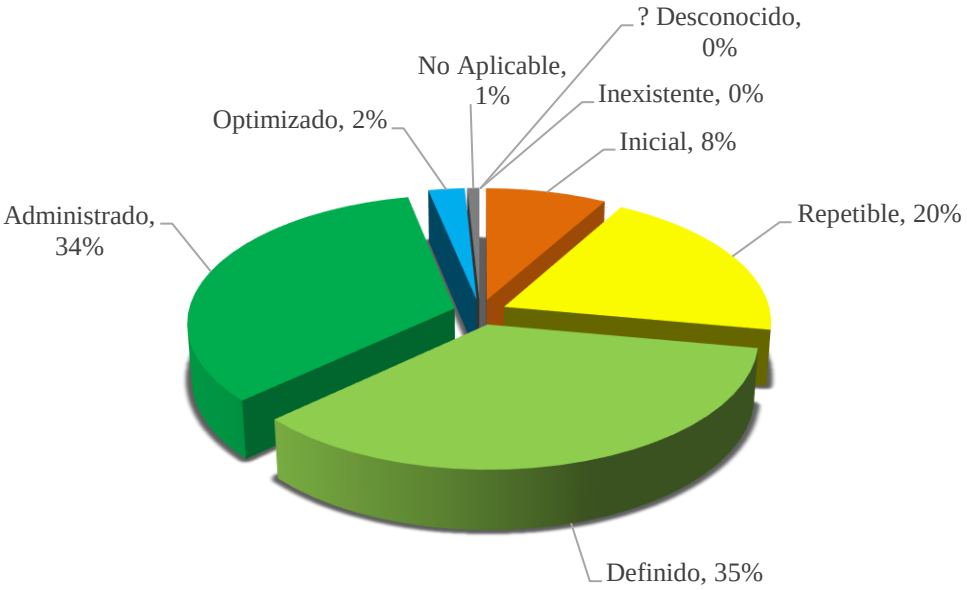
Figura 13. *Resultados del diagnóstico de la implementación de la NTC ISO 27001:2013*



De esta forma a la luz de las evidencias de documentación e implementación, el 5% de los requisitos se categorizaron con una implementación total, al ser verificables como práctica en toda la organización. Por su parte, el 50% se categorizó como prácticamente implementado como rutina, el 36% de los requisitos tuvo un cumplimiento parcial y el 9% una categorización de poca implementación, es decir, una ocurrencia como práctica sólo en algunas áreas de la organización. Ningún requisito mostró incumplimiento total o fue considerado como no aplicable. Por último, siendo que todos los requisitos fueron revisados no se categorizó ninguno con estado desconocido.

Por su parte, la verificación del nivel de cumplimiento de los controles del Anexo A de la norma NTC ISO/IEC 27001:2013, dio lugar a los resultados que se esquematizan en la Figura 14.

Figura 14. *Resultados del diagnóstico de la implementación de la NTC ISO/IEC 27001:2013 - Anexo A*



De una naturaleza más técnica, el diagnóstico preliminar de la implementación de los controles específicos indicados en el anexo A de la NTC ISO/IEC 27001:2013, mostró los siguientes resultados: Un 2% de los controles mostró el nivel máximo de madurez correspondiente al nivel Optimizado, en el cual además de documentado, el control se encuentra aprobado, formalizado y con medición de eficacia por la organización. El 34% de los controles se valoraron como Administrados, es decir, documentados, aprobados y formalizados. El 35% se ubicaron en la categoría de Definidos, habiendo sido documentados. Por su parte, los controles que se evaluaron con un nivel de madurez correspondiente a Repetible constituyeron el 20%, mientras que aquellos en estado Inicial constituyeron un 8%, la diferencia entre estas dos categorías radica en, la implementación de manera informal de los primeros muy sujeto a las actividades de una persona, y la gestión apenas incipiente de los últimos. Finalmente, no fue valorado ningún requisito en la categoría de inexistente toda vez que se pudo validar su implementación en alguno de los

niveles anteriores. Como una no aplicabilidad para la organización se identificó el control A.14.2.7 Externalización del desarrollo de software, el cual constituye una exclusión del alcance del Sistema de Gestión de Seguridad de la Información.

4.2 Fase de ejecución

4.2.1 Diseño del Sistema Integrado de Gestión

A partir de los resultados diagnósticos y los lineamientos de relación de requisitos de las normas objeto de estudio, se procedió a realizar su análisis de relación el cual se muestra en la Tabla 9. Seguidamente, identificados los niveles de relación de los requisitos se procedió a la estructuración del plan de trabajo detallado, para lo cual se tuvo en cuenta la secuencia del ciclo PHVA y las categorías de relación los requisitos así: en primer lugar los requisitos de Relación Total (T), seguidamente por los de Relación Parcial (P), para terminar por aquellos de Inexistencia de Relación (X), con objetivo de facilitar su ejecución metodológica. El plan de trabajo que se muestra en la Tabla 10. fue ejecutado por el equipo de trabajo de implementación y referencia de forma general los documentos que se derivaron de la fase de implementación, la cual se describe en detalle en la fase correspondiente.

Tabla 9. *Resultados del análisis de relación de requisitos de las NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013*

NTC - ISO 9001:2015		Tipo de Relación	NTC - ISO/IEC 27001:2013	
Capítulo	**Requisitos**		**Capítulo**	**Requisito**
4	**Contexto de la organización**		**4**	**Contexto de la organización**
4,1	Comprensión de la organización y de su contexto	T	4,1	Conocimiento de la organización y de su contexto
4,2	Comprensión de las necesidades y expectativas de las partes interesadas	T	4,2	Comprensión de las necesidades y expectativas de las partes interesadas
4,3	Determinación del alcance del SGC	T	4,3	Determinación del alcance del SGSI
4,4	SGC y sus procesos	P	4,4	SGSI
5	**Liderazgo**		**5**	**Liderazgo**
5,1	Liderazgo y compromiso	P	5,1	Liderazgo y compromiso
5,1,1	Generalidades	T	-	-
5,1,2	Enfoque al cliente	X	-	-
5,2	Política	T	5,2	Política
5,2,1	Establecimiento de la política de la calidad	T	-	-
5,2,2	Comunicación de la política de la calidad	T	-	-
5,3	Roles, responsabilidades y autoridades en la organización	T	5,3	Roles, responsabilidades y autoridades en la organización
6	**Planificación**		**6**	**Planificación**
6,1	Acciones para abordar los riesgos y oportunidades	P	6,1	Acciones para tratar riesgos y oportunidades
6,1,1	Determinar los riesgos y oportunidades que es necesario abordar	P	6,1,1	Generalidades
6,1,2	Establecer acciones que sean proporcionales a los riesgos y oportunidades	P		
-	-	X	6,1,2	Valoración de los riesgos de la seguridad de la información
-	-	X	6,1,3	Tratamiento de riesgos de la seguridad de la información
6,2	Objetivos de la calidad y planificación para lograrlos	T		
6,2,1	Establecer los objetivos de calidad para las funciones y niveles pertinentes y los procesos necesarios para el SGC	T	6,2	Objetivos de seguridad de la información y planes para lograrlos

NTC - ISO 9001:2015		Tipo de Relación	NTC - ISO/IEC 27001:2013	
Capítulo	**Requisitos**		**Capítulo**	**Requisito**
6,2,2	Planificar el logro de los objetivos	T		
6,3	Planificación de los cambios en el SGC	X		
7	**Apoyo**		**7**	**Soporte**
7,1	Recursos	T	7,1	Recursos
7,1,1	Generalidades	T	-	-
7,1,2	Personas	X	-	-
7,1,3	Infraestructura	X	-	-
7,1,4	Ambiente para la operación de los procesos	X	-	-
7,1,5	Recursos de seguimiento y medición	X	-	-
7,1,6	Conocimientos de la organización	X	-	-
7,2	Competencia	T	7,2	Competencia
7,3	Toma de conciencia	T	7,3	Toma de conciencia
7,4	Comunicación	T	7,4	Comunicación
7,5	Información documentada	T	7,5	Información documentada
7,5,1	Generalidades	T	7,5,1	Generalidades
7,5,2	Creación y actualización	T	7,5,2	Creación y actualización
7,5,3	Control de la información documentada	T	7,5,3	Control de la información documentada
8	**Operación**		**8**	**Operación**
8,1	Planificación y control operacional	X	8,1	Planificación y control operacional
8,2	Requisitos para los productos y servicios	X	8,2	Valoración de los riesgos de la seguridad de la información
8,2,1	Comunicación con el cliente	X	-	-
8,2,2	Determinación de los requisitos para los productos y servicios	X	-	-
8,2,3	Revisión de los requisitos para los productos y servicios	X	-	-
8,2,4	Cambios en los requisitos para los productos y servicios	X	-	-

NTC - ISO 9001:2015		Tipo de Relación	NTC - ISO/IEC 27001:2013	
Capítulo	**Requisitos**		**Capítulo**	**Requisito**
8,3	Diseño y desarrollo de los productos y servicios	X	8,3	Tratamiento de riesgos de la seguridad de la información
8,3,1	Generalidades	X	-	-
8,3,2	Planificación del diseño y desarrollo	X	-	-
8,3,3	Entradas para el diseño y desarrollo	X	-	-
8,3,4	Controles del diseño y desarrollo	X	-	-
8,3,5	Salidas del diseño y desarrollo	X	-	-
8,3,6	Cambios del diseño y desarrollo	X	-	-
8,4	Control de los procesos, productos y servicios suministrados externamente	X	-	-
8,4,1	Generalidades	X	-	-
8,4,2	Tipo y alcance del control	X	-	-
8,4,3	Información para los proveedores externos	X	-	-
8,5	Producción y provisión del servicio	X	-	-
8,5,1	Control de la producción y de la provisión del servicio	X	-	-
8,5,2	Identificación y trazabilidad	X	-	-
8,5,3	Propiedad perteneciente a los clientes o proveedores externos	X	-	-
8,5,4	Preservación	X	-	-
8,5,5	Actividades posteriores a la entrega	X	-	-
8,5,6	Control de los cambios	X	-	-
8,6	Liberación de los productos y servicios	X	-	-
8,7	Control de las salidas no conformes	X	-	-
8,7,1	Identificación y control de las salidas no conformes	X	-	-
9	**Evaluación del desempeño**		**9**	**Evaluación del desempeño**
9,1	Seguimiento, medición, análisis y evaluación	T	9,1	Seguimiento, medición, análisis y evaluación
9,1,1	Generalidades	T		

NTC - ISO 9001:2015		Tipo de Relación	NTC - ISO/IEC 27001:2013	
Capítulo	**Requisitos**		**Capítulo**	**Requisito**
9,1,2	Satisfacción del cliente	X	-	-
9,1,3	Análisis y evaluación	X	-	-
9,2	Auditoría interna	T	9,2	Auditoría interna
9,3	Revisión por la dirección	T	9,3	Revisión por la dirección
9,3,1	Generalidades	T	-	-
9,3,2	Entradas de la revisión por la dirección	T	-	-
9,3,3	Salidas de la revisión por la dirección	T	-	-
10	**Mejora**		**10**	**Mejora**
10,1	Generalidades	T	-	-
10,2	No conformidad y acción correctiva	T	10,1	No conformidades y acciones correctivas
10,3	Mejora continua	T	10,2	Mejora continua

Nota: esta tabla muestra los resultados del análisis de relación entre los requisitos de las normas NTC ISO 9001:2015 y NTC-ISO/IEC 27001:2013.

Tabla 10. *Plan de integración de las normas NTC-ISO 9001:2015 y NTC-ISO/IEC 27001:2013*

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
0	**Actividades Preliminares**			-	
0.3	Presentación del Equipo	14-abr-21	14-abr-21	Amovil-Innovinc-Clarien Guerrero-Natalia Niño	N/A
0.4	Acceso a la Información	12-abr-21	12-abr-21	Amovil	N/A
0.5	Revisión y ajuste de cronograma de trabajo	19-abr-21	21-abr-21	Innovinc-Clarien Guerrero-Natalia Niño	Plan de Trabajo - Integración NTC ISO 9001 y NTC 27001
1	**Diagnóstico del SGSI-SGC**			-	
0.1	Entrega y Empalme del SGSI	15-mar-21	06-abr-21	Amovil-Innovinc-Clarien Guerrero	N/A
1.1	Entrega de Informe - GAP Análisis	12-abr-21	13-abr-21	Innovinc-Clarien Guerrero-Natalia Niño	Informe Diagnóstico - GAP Análisis
1.2	Validación de Informe	13-abr-21	26-abr-21	Innovic	N/A
2	**Requisitos de Relación Total**			-	
Planear	**Contexto: SIG**				
2.1	Revisión Mapa de Procesos	05-abr-21	05-abr-21	Amovil-Innovinc-Clarien Guerrero	A SIG 02 Mapa de Procesos AMOVIL [i]
2.2	Documentación Alcance	12-abr-21	22-abr-21	Amovil-Innovinc-Clarien Guerrero	A SIG 01 Alcance Sistema Integrado de Gestión [i]
2.3	Revisión y Ajuste Política General SIG	22-abr-21	03-may-21	Amovil-Innovinc-Clarien Guerrero	P SIG 01 Política Sistema Integrado de Gestión [i]
2.4	Revisión y Ajuste Objetivos SIG	06-may-21	20-may-21	Amovil-Innovinc-Clarien Guerrero	F SIG 08 Matriz de Objetivos e Indicadores SIG [i]
Planear	**Contexto: despliegue estratégico**				
2.5	Ajuste del Contexto Externo e Interno (FODA y PESTEL)	21-abr-21	28-jul-21	Amovil-Innovinc-Clarien Guerrero	F DE 01 FODA [i], F DE 02 PESTEL [i]

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
2.6	Ajuste de Matriz de Partes Interesadas	21-abr-21	20-ago-21	Amovil-Innovinc-Clarien Guerrero	F DE 03 Matriz Partes Interesadas [i]
2.7	Revisar Planeación Estratégica (vigencia 2021-2025)	05-may-21	30-nov-21	Amovil-Innovinc-Clarien Guerrero	MN DE 01 Manual Direccionamiento Estratégico [i]
2.8	Indicadores Estratégicos (derivados de la Planeación Estratégica)	20-may-21	16-nov-21	Amovil-Innovinc-Clarien Guerrero	PLN DE 01 Estrategias y Planes Operativos [i]
Planear	**Liderazgo**				
2.9	Realizar Presupuesto Anual del SIG	10-may-21	16-nov-21	Amovil-Innovinc-Clarien Guerrero	F SIG 02 Presupuesto SIG 2022 [i]
2.10	Definir Roles y Responsabilidades del SIG	03-may-21	16-nov-21	Clarien Guerrero - Natalia Niño - Gestor SIG	MN GAF 01 Manual de Funciones [i], A GAF 02 Estructura Organizacional AMOVIL [i], F GAF 39 Matriz Roles y Responsabilidades [i]
2.11	Revisar Segregación de Funciones	03-may-21	16-nov-21	Amovil-Innovinc-Clarien Guerrero	
Planear	**Planeación: competencia / comunicación / información documentada**				
2.12	Plan de Capacitaciones	13-may-21	12-nov-21	Amovil-Clarien Guerrero	PC GAF 05 Capacitación y Entrenamiento [i], PLN GAF 01 Plan Capacitación [i]
2.12.1	*Capacitación Riesgos*	17-jul-21	14-ago-21	Innovic	
2.12.2	*Capacitación Indicadores*	25-sep-21	25-sep-21	Gestor SIG	
2.12.3	*Capacitación Auditores Internos*	05-feb-22	26-mar-22	Innovic	
2.12.4	*Campañas Sensibilización SGI*	01-may-21	01-may-22	Gestor SIG - Asistente TI	
2.12.5	*Revisión de Eficacia de las Capacitaciones*	Mensual	-	Amovil - Gestor SIG	
2.13	Revisión y Ajuste Matriz de Comunicaciones	20-may-21	30-nov-21	Gestor SIG	F SIG 26 Matriz Comunicación Interna y Externa [i]
2.14	Revisar Listado Contactos con Autoridades y Grupos de Interés Especial	19-may-21	30-nov-21	Gestor SIG	A SIG 06 Directorio Contactos Autoridades - Emergencias y Grupos de Interés [i]

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
2.15	Revisión y Ajuste de Sharepoint	17-ago-21	17-ago-21	Innovic - Amovil	PC SIG 02 Control Información Documentada [i], F SIG 05 Listado Maestro Información Documentada [i], F SIG 06 Listado Maestro de Registros [i]
2.16	Migración de documentos al Sharepoint	06-sep-21	10-sep-21	Innovic - Asistente TI	
2.17	Revisión y Ajuste Procedimiento Gestión Documental	22-abr-21	28-may-21	Amovil - Clarien Guerrero	
2.18	Revisión y Ajuste Listado Maestro de Documentos	26-abr-21	27-ago-22	Gestor SIG - Clarien Guerrero - Natalia Niño	
2.19	Revisión y Ajuste Documentación SIG	28-abr-21	27-ago-22	Gestor SIG - Clarien Guerrero - Natalia Niño	
2.20	Revisión y Ajuste Listado Maestro de Registros	01-feb-21	27-ago-22	Gestor SIG - Clarien Guerrero - Natalia Niño	
Verificar	**Evaluación de Desempeño**				
2.21	Consolidación de indicadores de gestión	Mensual	-	Amovil - Gestor SIG - Clarien Guerrero	F SIG 03 rer [i] por Procesos
2.22	Acompañamiento en la revisión por la Dirección	30-jun-22	30-jun-22	Amovil - Gestor SIG	PC DE 02 Revisión por la Dirección [i], F DE 05 Informe Revisión por la Dirección [i] 2022
2.23	Revisión Procedimiento, Programa y documentos anexos de auditoría interna	19-oct-21	30-nov-21	Natalia Niño	PC SIG 05 Auditoría Interna [i], PR SIG 01 Programa de auditorías [i], PLN SIG 01 Plan de auditoría [i], F SIG 16 Validación de Competencias Auditores Internos [i], F SIG 16 Validación de Competencias Auditores Internos [i], F SIG 17 Lista de Chequeo [i], F SIG 18 Informe de Auditoría [i], F SIG 19 Evaluación Desempeño Auditor Interno [i]
Actuar	**Mejora**				
2.24	Revisar las NC de la auditoría anterior	03-may-21	30-jun-21	Amovil-Gestor SIG-Clarien Guerrero	PC SIG 03 Acciones Correctivas y de Mejora [i]; F SIG 07 Matriz

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
2.25	Gestión de cierre de Acciones Correctivas y de Mejora	03-may-21	30-nov-21	Amovil-Gestor SIG-Clarien Guerrero	Acciones Correctivas y de Mejora [i]; A SIG 05 Análisis Causa Raíz - Metodología Cinco Por qué [i]
3	**Requisitos de Relación Parcial**			-	
Planear	**Contexto: procesos del SIG**				
3.1	Revisión de Caracterizaciones Procesos	13-may-21	30-nov-21	Clarien Guerrero	CA XXX 01 Caracterización Por Procesos [i]
Planear	**Planeación: riesgos**				
3.2	Revisión Metodología de Riesgos	17-jul-21	14-ago-21	Innovic - Gestor SIG	PC SIG 01 Gestión de Riesgos [i], F SIG 12 Matriz Riesgos y Oportunidades [i] Por Procesos, F SIG 13 Acta Aceptación Riesgo Residual y Tratamiento [i] Por Procesos
3.3	Revisión y Ajuste de Matriz para Identificación, Valoración y Tratamiento de Riesgos	21-sep-21	22-sep-21	Innovic - Gestor SIG	
3.4	Revisión y Ajuste de Riesgos de cada Proceso	14-sep-21	30-nov-21	Amovil-Gestor SIG-Clarien Guerrero	
3.5	Levantamiento de Actas de Riesgos	14-sep-21	30-nov-21	Gestor SIG	
4	**Requisitos de Relación Inexistente**				
Planear	**Planeación: planificación de los cambios**				
4.1	Revisión y Actualización de Lineamientos Procedimiento de Gestión del Cambio	21-jun-21	09-nov-21	Gestor SIG	PC SIG 06 Gestión del Cambio [i], PC GPD 02 Gestión de Cambios a Nivel de Desarrollo [i], F SIG 04 Gestión del Cambio [i] Por cambio
4.2	Revisión Planes de Gestión del Cambio en curso	15-jun-21	15-dic-21	Gestor SIG	
Planear	**Planeación: ambiente de trabajo**				
4.3	Plan de bienestar laboral (Plan - evidencias de cumplimiento)	22-sep-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	Políticas, procedimientos, instructivos y formatos - SG SST
Planear	**Planeación: requisitos legales**				

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
4.4	Revisión y Ajuste Matriz Legal	19-may-21	30-nov-21	Gestor SIG	SIG-P-05 Requisitos Legales [i], F SIG 11 Matriz de Requisitos Legales [i]
Verificar	**Evaluación de Desempeño: satisfacción del cliente**				
4.5	Encuestas de Satisfacción del Cliente	09-oct-21	30-oct-21	Gestor SIG - Director Comercial	Formularios Google - Encuesta de Satisfacción
Hacer	**Operación: procesos misionales**				
4.6	Procedimientos - Proceso Gestión de Gestión Comercial	Director 06-jul-21	03-nov-21	Amovil - Gestor SIG - Clarien Guerrero	-Políticas, procedimientos, instructivos y formatos - Procesos
4.7	Procedimientos - Proceso Gestión Proyectos y Desarrollo	24-may-21	19-nov-21	Amovil - Gestor SIG - Clarien Guerrero	-misionales
4.8	Procedimientos - Proceso Soporte	15-jun-21	24-nov-21	Amovil - Gestor SIG - Clarien Guerrero	-
4.9	Procedimientos - Proceso Implementación	06-jul-21	30-nov-21	Amovil - Gestor SIG - Clarien Guerrero	-
4.10	Procedimiento, Instructivo o Formato Control de Salidas no Conformes	27-sep-21	14-oct-21	Gestor SIG	PC SIG 04 Salidas no Conformes [i], F SIG 14 Matriz Salidas No Conformes [i]
Hacer	**Operación: control de los procesos/servicios suministrados externamente**				
4.11	Identificación de Proveedores (Listado Maestro Proveedores/Contratistas)	02-ago-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	-P GAF 01 Política de Proveedores y Contratistas [i], PC GAF 01
4.12	Selección Proveedores / Contratistas	04-ago-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	-Selección y Registro de Proveedores-Contratistas [i], PC
4.13	Identificación de Políticas y Riesgos para proveedores	11-ago-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	-GAF 03 Compras y Subcontrataciones [i], PC GAF 08
4.14	Evaluación de Proveedores	15-jun-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	Evaluación de Proveedores y Contratistas, F GAF 02 Listado Maestro Proveedores y Contratistas [i], F GAF 03 Informe de Auditoría a Proveedores [i], F GAF 04 Selección Proveedores y Contratistas [i], F GAF 05

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
					Evaluación de Proveedores [i], F GAF 07 Evaluación de Contratistas [i], F GAF 33 Orden de Compra, F GAF 34 Orden de Servicio
Hacer	**ANEXO A - Objetivos de Control y Controles de Referencia**				
Hacer	**Políticas de Seguridad de la Información**				
4.15	Políticas y lineamientos de seguridad de la información	26-ago-21	12-nov-21	Gestor SIG - Asistente TI	P OTI 01 Compendio de Políticas Seguridad Información [i]
Hacer	**Organización interna**				
4.16	Seguridad de Recursos Humanos	26-ago-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	-Políticas, procedimientos, instructivos y formatos - Procesos de Apoyo (Gestión Administrativa, Financiera y del Talento Humano)
4.17	Revisión de Proceso Disciplinario	02-sep-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	
4.18	Acuerdos de Confidencialidad o no Divulgación	06-sep-21	06-sep-21	Amovil - Natalia Niño - Clarien Guerrero	
4.19	Revisión de Perfiles	08-sep-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	-
4.20	Revisión hojas de vida y soportes	15-sep-21	12-nov-21	Amovil - Natalia Niño - Clarien Guerrero	-
Hacer	**Dispositivos móviles y teletrabajo**				
4.21	Dispositivos Móviles	19-oct-21	30-nov-21	Gestor SIG	P OTI 01 Compendio de Políticas Seguridad Información [i]
4.22	Trabajo en Casa (Home office)	04-oct-21	30-nov-21	Gestor SIG	
Hacer	**Responsabilidad por los activos**				
4.23	Gestión de Activos	08-sep-21	30-nov-21	Gestor SIG - Asistente TI	PC OTI 05 Gestión de Inventarios [i], F OTI 01 Inventario de Activos [i]
4.24	Inventario de Activos (incluye propietarios de activos)	18-may-21	30-nov-21	Asistente TI	

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
Hacer	**Clasificación de la Información**				
4.25	Clasificación de la Información	13-sep-21	30-nov-21	Clarien Guerrero	P OTI 01 Compendio de Políticas Seguridad Información [i] Ver documentos - Información Documentada
4.26	Etiquetado Información (acorde a la clasificación)	18-may-21	30-nov-21	Gestor SIG - Asistente TI	
Hacer	**Manejo de medios**				
4.27	Manejo de Medios (información en medio removibles)	20-sep-21	30-nov-21	Asistente TI	P OTI 01 Compendio de Políticas [i], PC OTI 15 Borrado Seguro [i], PC OTI 14 Transferencia de Información [i]
Hacer	**Requisitos del negocio para control de acceso**				
4.28	Control de Acceso (red, servicios y aplicaciones)	21-jul-21	30-nov-21	Asistente TI	PC OTI 06 Asignación de Usuarios [i], F OTI 02 Inventario de Accesos Físicos y Digitales [i], F OTI 10 Credenciales de Acceso [i]
Hacer	**Gestión de acceso de usuarios**				
4.29	Gestión de Usuarios	30-jul-21	30-nov-21	Asistente TI	PC OTI 06 Asignación de Usuarios [i]
Hacer	**Control de acceso a sistemas y aplicaciones**				
4.30	Gestión de Contraseñas	28-jul-21	30-nov-21	Asistente TI	F OTI 02 Inventario de Accesos Físicos y Digitales [i] F OTI 10 Credenciales de Acceso [i]
4.31	Acceso a Código Fuente de Programas	11-ago-21	30-nov-21	Gestor SIG	
4.32	Matriz de Permisos y Accesos	18-may-21	30-nov-21	Gestor SIG - Asistente TI	
Hacer	**Controles criptográficos**				
4.33	Criptografía (incluye gestión de llaves)	08-jul-21	30-nov-21	Asistente TI	P OTI 01 Compendio de Políticas [i]

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
Hacer	**Áreas seguras**				
4.34	Seguridad Física	02-jul-21	30-nov-21	Asistente TI	P OTI 01 Compendio de Políticas [i]
4.35	Control de Acceso Físico	07-jul-21	30-nov-21	Gestor SIG - Asistente TI	INS OTI 04 Instructivo de Seguridad Física y del Entorno [i]
Hacer	**Equipos**				
4.36	Disposición Segura o Reutilización de Equipos (borrado seguro)	27-sep-21	30-nov-21	Asistente TI	PC OTI 04 Mantenimiento Correctivo y Preventivo [i], PLN OTI 02 Plan de Mantenimiento de Equipos [i], F OTI 08 Cronograma de Mantenimiento de Equipos [i], F OTI 09 Bitácora de Mantenimiento [i]
4.37	Mantenimiento de Equipos	29-sep-21	30-nov-21	Asistente TI	
Hacer	**Procedimientos operacionales y responsabilidades**				
4.38	Separación Ambientes de Desarrollo, Prueba y Operación	07-oct-21	15-dic-21	Asistente TI	PC GDP 01 Desarrollo Seguro [i]
Hacer	**Protección contra códigos maliciosos**				
4.39	Protección Contra Código Malicioso	19-oct-21	30-nov-21	Amovil	P OTI 01 Compendio de Políticas Seguridad Información [i]
Hacer	**Copias de respaldo**				
4.40	Copias de Seguridad (Backups) y Plan de Restauración	24-jun-21	30-nov-21	Asistente TI	PC OTI 09 Gestión Copias Seguridad [i], PC OTI 01 Restauración de Copias Seguridad [i], INS OTI 01 Restauración Copias de Seguridad [i]
Hacer	**Control de software operacional**				
4.41	Instalación de Software (incluye restricciones)	16-jul-21	30-nov-21	Asistente TI	PC OTI 07 Instalación y Actualización de Software [i]

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
Hacer	**Gestión de la vulnerabilidad técnica**				
4.42	Planes de Remediación Vulnerabilidades (Pentesting)	18-may-21	30-nov-21	Amovil-Innovic	PC OTI 03 Gestión Vulnerabilidades Técnicas [i], F OTI 04 Plan Pruebas Plan de Contingencia [i], F OTI 07 Plan de Acción Cierre Vulnerabilidades Técnicas [i]
Hacer	**Gestión de la seguridad de las redes**				
4.43	Diagrama de Red (Elaborar diagrama de red)	18-may-21	30-nov-21	Asistente TI	PC OTI 13 Gestión Equipos de Red [i]
Hacer	**Transferencia de información**				
4.44	Transferencia de Información	18-may-21	30-nov-21	Asistente TI	P OTI 01 Compendio de Políticas Seguridad Información [i]
Hacer	**Seguridad de los procesos de desarrollo y de soporte**				
4.45	Requerimientos para Desarrollo nuevo Modificación o Ajuste de Software	23-jun-21	19-nov-21	Gestor SIG - Director Proyectos y Desarrollo	PC GDP 01 Desarrollo Seguro [i], F GPD 09 Formato de Pruebas de Desarrollo y Funcionales [i], F IMS 25 Plan Pruebas de Aceptación [i] Por Producto/Servicio
4.46	Desarrollo Seguro (políticas, procedimientos, principios)	11-oct-21	19-nov-21	Gestor SIG - Director Proyectos y Desarrollo	
4.47	Pruebas (seguridad, funcionales, aceptación)	13-oct-21	19-nov-21	Gestor SIG - Director Proyectos y Desarrollo	
Hacer	**Gestión de incidentes y mejoras en la seguridad de la información**				
4.48	Gestión de Incidentes de Seguridad	31-ago-21	30-nov-21	Gestor SIG - Asistente TI	AmovilDesk / Cervello, PC IMS 01 Gestión de Incidencias y Requerimientos [i], PC OTI 11 Gestión de Incidentes [i] PC OTI 12 Gestión de Requerimientos [i]
4.49	Reporte de Eventos de Seguridad	25-ago-21	30-nov-21	Gestor SIG - Asistente TI	
4.50	Aprendizaje sobre Eventos de Seguridad	30-ago-21	30-nov-21	Gestor SIG - Asistente TI	
4.51	Recolección de Evidencia	30-ago-21	30-nov-21	Gestor SIG - Asistente TI	
Hacer	**Continuidad de seguridad de la información**				

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
4.52	Revisión Plan de Continuidad y ajustes al SGSI	27-oct-21	30-nov-21	Asistente TI	PLN OTI 01 Plan Continuidad del Negocio [i], F OTI 03 Análisis Impacto Negocio (BIA) [i], F OTI 04 Plan Pruebas Plan de Contingencia [i], F OTI 05 Evaluación Plan de Contingencia [i], F OTI 07 Plan de Acción Cierre Vulnerabilidades Técnicas [i], F OTI 11 Riesgos Plan de Contingencia [i]
4.53	Revisión Pruebas de Continuidad	08-nov-21	10-ene-22	Innovinc - Asistente TI	
4.54	Revisión Plan de Recuperación de Desastres	10-nov-21	10-ene-22	Innovinc - Asistente TI	
4.55	Revisión Pruebas de Recuperación de Desastres	12-nov-21	10-ene-22	Innovinc - Asistente TI	
Hacer	**Redundancias**				
4.56	Documentación Redundancia	21-oct-21	10-ene-22	Asistente TI	PLN OTI 01 Plan Continuidad del Negocio [i]
4.57	Pruebas Redundancia y Ajustes	25-oct-21	10-ene-22	Innovinc - Asistente TI	
Hacer	**Cumplimiento de requisitos legales y contractuales**				
4.58	Datos Personales	18-ago-21	30-nov-21	Innovinc - Asistente TI	F SIG 11 Matriz de requisitos Legales [i], P SIG 02 Política Tratamiento Datos Personales [i], A GAF 04 Acuerdo Confidencialidad (Trabajadores) [i] A GAF 16 Acuerdo de Confidencialidad (Clientes, Contratista y Proveedores) [i]
4.59	Consola de Antivirus	18-may-21	30-nov-21	Asistente TI	
Hacer	**Revisión de Implementación de Procesos TI**				
4.60	Primera Revisión de Implementación de Procesos TI	24-ene-22	29-ene-22	Gestor SIG - Clarien Guerrero - Natalia Niño	Verificación - F OTI 06 Declaración de Aplicabilidad [i]
4.61	Segunda Revisión de Implementación de Procesos TI	21-mar-22	25-mar-22	Gestor SIG - Clarien Guerrero - Natalia Niño	
4.62	Tercera Revisión de Implementación de Procesos TI	23-may-22	27-may-22	Gestor SIG - Clarien Guerrero - Natalia Niño	

Id	Descripción de la Actividad	Fecha Inicial	Fecha Final	Responsable	Evidencia
4.63	Cuarta Revisión de Implementación de Procesos TI	25-jul-22	29-jul-22	Gestor SIG - Clarien Guerrero - Natalia Niño	

Nota: esta tabla muestra el plan de trabajo detallado ejecutado en el marco del presente proyecto.

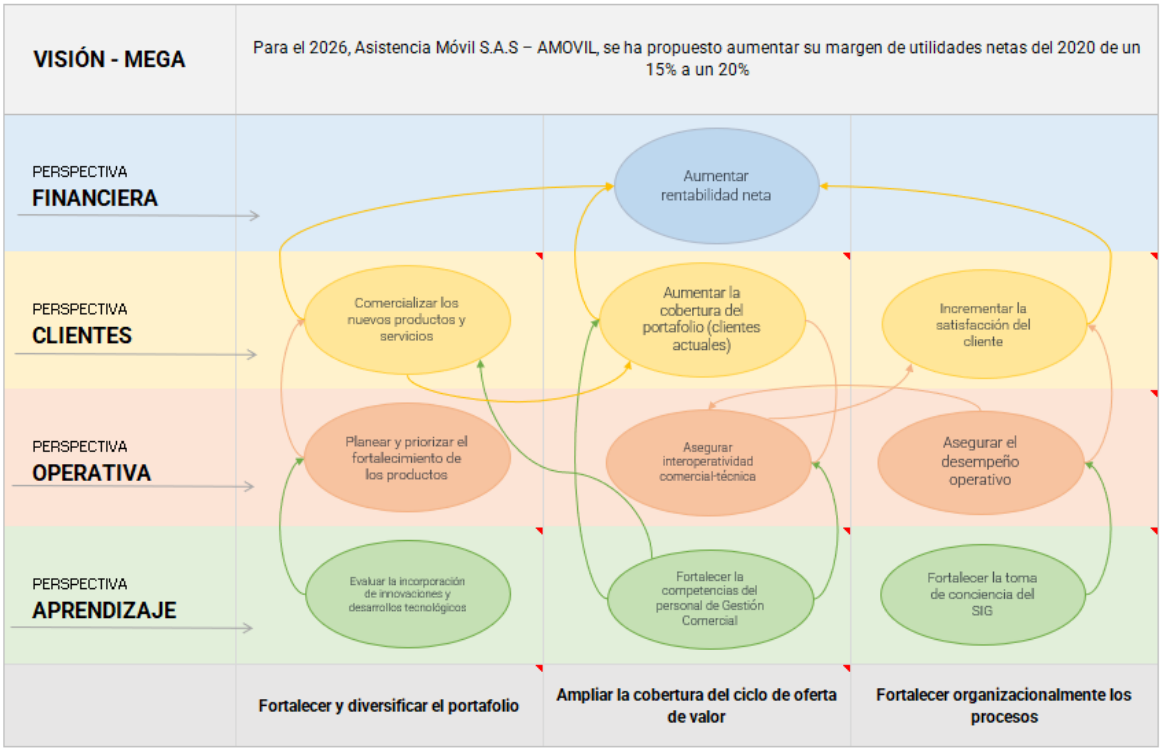
4.2.2 Implementación del Sistema Integrado de Gestión

La fase de ejecución se realizó conforme a lo estructurado en el plan de trabajo de integración, se desarrolló de forma conjunta la documentación e implementación con una importante cobertura de requisitos de ambas normas en la práctica diaria de la organización. Cabe resaltar que, si bien la intención original de la organización fue realizar la implementación conjunta de las ambas normas en el marco del SIG, por razones estratégicas priorizó la total implementación y auditoría de los requisitos de la norma NTC ISO/IEC 27001:2013, por lo que para algunos de los requisitos de la NTC ISO 9001:2015 no se dispone de evidencias de implementación, pero si en todos los casos, la base documental.

Requisitos de Relación Total (T). Se inició con la integración de los requisitos con Relación Total, se abordaron en primera instancia los requisitos asociados a los capítulos 4. Contexto, 5. Liderazgo y 6. Planificación. En el marco del capítulo 4 correspondiente al Contexto de la Organización, se realizó el despliegue estratégico a la cabeza de la Alta Dirección, para ello fueron evaluados y definidos los contextos internos y externos, se aplicó para tal fin la metodología de las matrices FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) y PESTAL (Factores Políticos, Económicos, Sociales, Tecnológicos, Ambientales y Legales), a través de las cuales se realizó un ejercicio de lluvia de ideas y deliberaciones para concretar los aspectos más relevantes. Los resultados de estos ejercicios se documentaron en las matrices respectivas.

A partir del diagnóstico del contexto interno y externo, se realizó el despliegue estratégico para la que se usó la metodología *Balance Score Card* - BSC (por sus siglas en inglés), a partir de la cual se definieron los tres principales enfoques estratégicos, como se muestra en la Figura 15.

Figura 15. *Mapa Estratégico - AMOVIL S.A.S*



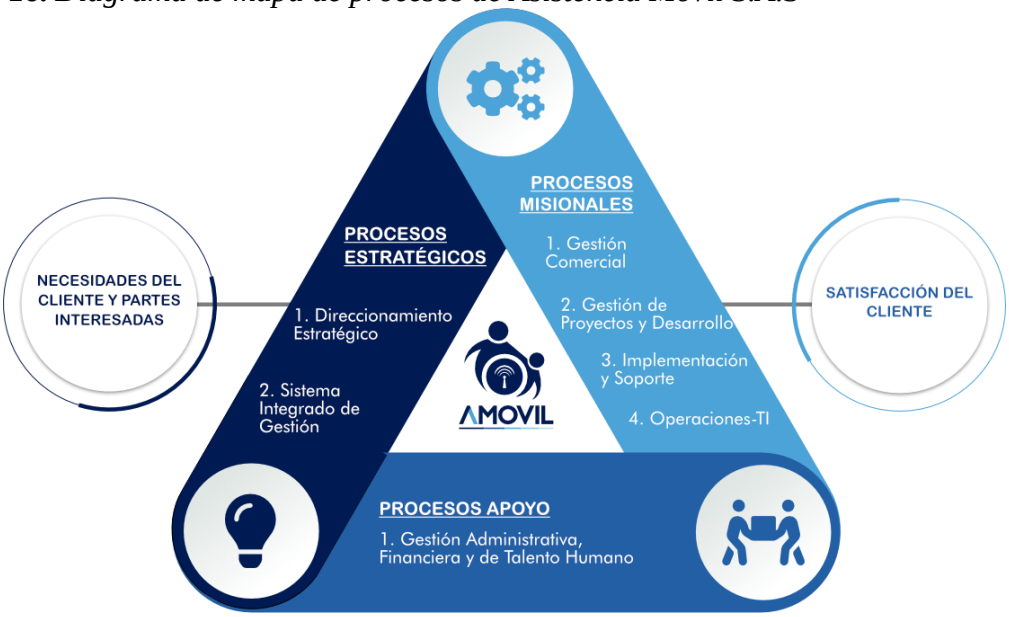
Adaptado de (AMOVIL S.A.S, 2021)

Para cada uno de los enfoques estratégicos identificados se definieron los planes de acción a ejecutar. Las matrices FODA, PESTAL y los Planes Operativos, así como, el contenido de los requisitos asociados al contexto y despliegue estratégico, se documentaron en el marco de un Manual del Direccionamiento Estratégico, donde además se incluyen otros lineamientos de la identidad de organizacional, tales como: la visión, misión y valores.

En el marco del despliegue estratégico, fue realizada también la identificación de las partes interesadas de la organización, se mapearon sus expectativas y necesidades. Finalmente, toda la metodología estructurada para la ejecución de la planeación estratégica se documentó a través del PC DE 01 Planeación Estratégica. Todos los documentos asociados a la comprensión del contexto y las partes interesadas y su respectiva implementación puede verificarse en el Apéndice *C*.

Posteriormente, se abordó la definición del mapa de procesos de la organización, con el fin de precisar ajustes de forma y fondo que permitieran la esquematización gráfica de los procesos del SIG y sus interacciones, derivando en el esquema que se muestra en la Figura 16.

Figura 16. *Diagrama de mapa de procesos de Asistencia Móvil S.A.S*



Adaptado de (AMOVIL S.A.S, 201)

Se procedió a establecer con la Alta Dirección y el Equipo de Implementación el alcance del SIG, se precisaron los requerimientos de las normas para tal fin: límites, aplicabilidad, cuestiones internas y externas, requisitos de las partes interesadas, productos, servicios y dependencias. Igualmente, se enunciaron las exclusiones y sus justificaciones respectivas. Este mismo alcance se incorporó como información documentada en el marco del manual del sistema integrado de gestión MN SIG 01 Manual SIG.

Los documentos asociados a la implementación de los requisitos comunes relativos al alcance del SIG y sus procesos están asociados al Apéndice *D*.

Posteriormente, se abordaron los requisitos de los capítulos de 5 Liderazgo y 6 Planificación que comparten ambas normas. Relativo a las intenciones de la Alta Dirección respecto al SIG y como marco referencial para el establecimiento de sus objetivos, se estructuró como información documentada la política del sistema integrado de gestión, dando respuesta a los requerimientos de ambas normas.

Se estructuró el presupuesto anual para asegurar la implementación del SIG, con la designación de los rubros correspondientes y el seguimiento de su ejecución mensual. De igual forma y vinculado a requisitos del Liderazgo, se trabajó en la estructura organizacional detallando los cargos, niveles jerárquicos, perfiles de cargo y responsabilidades asociadas al SIG y al cargo, todo esto en el marco del manual de funciones. Estos documentos asociados al capítulo 5 de Liderazgo pueden verificarse en el Apéndice *E* y Apéndice *F*.

En relación a los recursos tales como: competencia, comunicación e información documentada, se estructuraron los procedimientos con los lineamientos asociados en cada caso, así como, el plan de formación continua del personal en temas de interés del SIG y de acuerdo a las necesidades de los procesos. En relación a los recursos de comunicación se estructuró la matriz de comunicaciones internas y externas en las que se detallan los elementos de comunicación referenciados por ambas normas (qué se comunica, quién comunica, a quién comunica y a través de qué medios). Por su parte, en relación a la información documentada el procedimiento estableció los lineamientos para la creación, revisión y modificación de documentos, la suspensión y anulación de los mismos, así como, los lineamientos para el control de la documentación propia y externa y de los registros asociados al SIG. El procedimiento además incluyó los lineamientos para el etiquetado y clasificación de la información y el nombramiento de los documentos en el

aplicativo GitLab, el cual funciona como repositorio de los códigos de desarrollo. Asociados a este procedimiento se estructuraron y documentaron los listados maestros para el control de la información documentada y los registros del SIG, así como, los formatos de las plantillas para la elaboración de los documentos del SIG que pueden ser usadas en caso de requerir la creación de cualquier documento dentro del SIG. Los documentos referenciados a los requisitos comunes del capítulo 7 Apoyo pueden verse en el Apéndice *G*.

Finalmente, se realizó la implementación de los requisitos de relación total asociados a los capítulos 9 Evaluación de desempeño y 10 Mejora, para ello se trabajó de forma integrada y se estructuraron los siguientes documentos: ficha de indicadores a través de la cual se documentó el cálculo de los indicadores de los procesos con el objetivo de medir su eficacia. Se establecieron los lineamientos generales para la ejecución de auditorías internas del SIG, se incorporó en el procedimiento correspondiente los requerimientos de cada norma, así como, los documentos asociados tales como: programa, plan de auditoría, validación de competencias de auditores internos, lista de chequeo, informe de auditoría y evaluación de desempeño de auditores internos, de los cuales se disponen de los registros de implementación. Por último, en el requisito asociado a la revisión por la dirección, se encontró conveniente la documentación de un procedimiento y de esta forma asegurar la cobertura completa de las entradas requeridas por cada norma, así como, la estructuración del informe correspondiente a la revisión, de estos requerimientos además se disponen los registros de implementación que pueden verificarse en el Apéndice *H*.

Por su parte, a nivel de los requisitos de la mejora, se documentó el procedimiento para la gestión de acciones correctivas y de mejora, así como, la matriz correspondiente para el registro y gestión de las acciones, en la cual que se incluye: el análisis de causas, el plan de acción, fechas y

responsables de cierre, el seguimiento del cierre, el estado de las actividades, las evidencias de cierre de acciones y la evaluación de la eficacia. Todos estos documentos están asociados al Apéndice *I*.

4.2.2.1 Requisitos de Relación Parcial. Siguiendo la metodología de integración, se prosiguió con la documentación e implementación de los requisitos con relación parcial, es decir, aquellos que, si bien son contemplados por ambas normas, alguna de ellas incorpora detalles particulares. Dentro de esta categoría se incluyen: a nivel del capítulo 5 Contexto, el requisito del sistema de gestión y sus procesos, para el cual la NTC ISO 9001:2015 establece de forma más detallada la estructura a la que deben responder los procesos de un sistema de gestión. Por esta razón, para este requisito se estructuraron las caracterizaciones de los procesos que dan respuesta a: los requisitos de entradas y salidas, secuencia de interacción, criterios, métodos e indicadores de gestión, recursos asociados, responsabilidades y autoridades, riesgos y oportunidades, gestión de cambios y actividades de mejora. Los documentos asociados a este requisito de relación parcial están disponibles en el Apéndice *J*.

Por su parte, en lo referido al capítulo 6 Planificación, el requisito asociado a la metodología para abordar riesgos y oportunidades es considerado en ambas normas, no obstante, para la norma NTC ISO/IEC 27001:2013 es requerido además de la determinación de riesgos y oportunidades, su valoración y especificación de tratamiento. De esta forma, se documentó un procedimiento que incorpora una metodología que aborda los requisitos globales de ambas normas, así como, la matriz correspondiente para la identificación del riesgo/oportunidad, el aspecto de seguridad de la información afectado, las causas y controles al riesgo/oportunidad, el plan de tratamiento, el responsable de su ejecución, la fecha estimada de cierre, el seguimiento del plan y la evaluación de la eficacia del plan de tratamiento. Además, se estructuró y firmó por cada responsable del riesgo el acta de aceptación del riesgo residual y su tratamiento. La implementación de los requisitos asociados a este numeral está disponible en el Apéndice *K*.

4.2.2.2 Requisitos de Relación Inexistente. Por último, se realizó el proceso de integración de los requisitos específicos a cada norma y entre los cuales no existe relación. Estos están asociados a: el capítulo 5 Liderazgo al requisito 5.1.2 Enfoque al cliente asociado solo a la norma NTC ISO 9001:2015, para el cual se optó por la documentación de un instructivo que refiere los lineamientos paso a paso para la medición de la satisfacción del cliente a través de la aplicación de encuestas a través de formularios digitales, que evalúen el grado de conformidad a nivel de calidad y la seguridad de la información. Las evidencias de implementación de este requisito se contemplan en el Apéndice *L*.

Por su parte, si bien los numerales de valoración y tratamiento de riesgos resultan ser específicos para la norma NTC ISO/IEC 27001:2013, se optó por contemplar estos requerimientos desde el requisito de gestión de riegos y oportunidades, sin dar lugar a procedimientos o metodologías independientes para cada norma.

Dentro de estos mismos requisitos también fue incluida la planificación de los cambios, contemplado en el marco de la gestión de calidad para la gestión de cambios transversales y por la seguridad de la información a nivel de los desarrollos, para ello, se estructuraron dos procedimientos uno con los lineamientos generales para la gestión transversal de cambios del SIG y su respectivo formato de implementación, y otro, con los lineamientos la gestión de cambios técnicos a nivel del desarrollo de software, con los formatos específicos a su implementación. De ambos requisitos se dispone de evidencias de implementación, las cuales están disponibles en el Apéndice *M*.

A nivel del capítulo 7 Recursos, la norma NTC ISO 9001:2015 compila varios requisitos específicos en torno a los recursos: personas, infraestructura, ambiente de operación y

conocimientos de la organización, los cuales fueron documentados e implementados a través de: La documentación de procedimientos para la selección, vinculación y evaluación del desempeño del recurso personas, así como, los lineamientos para su desvinculación laboral, los cuales están asociados al proceso de Gestión Administrativa, Financiera y del Talento Humano – GAF. Para cada uno de estos procedimientos se estructuraron los formatos asociados correspondientes. A nivel del requisito infraestructura, se documentaron los siguientes lineamientos: procedimiento de mantenimiento correctivo y preventivo, plan de mantenimiento de equipos junto con los formatos asociados al cronograma de mantenimiento de equipos y bitácora de mantenimiento. Se estructuró además un formato de inventario que compila la identificación, descripción y detalle de ubicación de los diferentes activos de la organización. Por su parte, en todo lo relacionado al ambiente de trabajo, se vinculó toda la información desarrollada en torno al Sistema de Gestión de Seguridad y Salud en el Trabajo, que además de dar respuesta a requerimientos legales en la materia, incluye elementos de gestión de ambientes sanos y seguros desde el punto de vista psicológico, social y físico, estos elementos incluyen políticas, procedimientos, instructivos, planes y formatos y anexos asociados al SG SST. Por último, lo correspondiente al conocimiento de la organización, requisito que está incluido en la norma de calidad, esta validado a través de la misma documentación vinculada a toda la implementación del SIG, así como, a la definición del aplicativo GitLab que corresponden al repositorio de los códigos de desarrollo de software y cuya gestión fue documentada a través de un anexo. Todos los documentos asociados a estos requisitos están asociados al Apéndice *N*.

Finalmente, como requisitos de relación inexistente se incluyen todos los asociados al numeral 8 Operación, que para ambas normas corresponden al corazón de su operatividad. Para estos particulares en relación a la norma NTC ISO/IEC 27001:2013 la cual únicamente referencia

la implementación de la metodología de identificación, valoración y tratamientos de riesgos, como ya fue descrito, estas actividades se englobaron y ejecutaron dentro de las actividades de identificación de riesgos y oportunidades asociadas también a la norma de calidad.

Por su parte, en relación a los requisitos específicos de la norma de calidad, los mismos fueron documentados e implementados en el marco de la operatividad de los procesos de la organización así: para la planificación y control operacional está asociada la documentación del proceso de Gestión Comercial, correspondiente a un procedimiento que describe todas la actividades asociadas al proceso desde la identificación de los requerimientos del cliente, la estructuración de la oferta técnico económica, su legalización y finalización oficial. En este procedimiento se describen además los lineamientos de comunicación con el cliente, la especificación del portafolio de bienes y productos ofrecidos por la organización, revisión de los requisitos de los mismo y la gestión de sus cambios. Desde este entendimiento y gestión de los requisitos de los clientes el proceso de Gestión Comercial determina la información de entrada para los demás procesos misionales orientados al ofrecimiento de los bienes y servicios. Los documentos que dan respuesta a estos requisitos están referenciados en el Apéndice *O*.

El *core* del negocio de la organización corresponde al diseño y desarrollo de software, cuyas actividades están documentadas e implementadas a través de los lineamientos del proceso de Gestión de Proyectos y Desarrollo – GPD, el cual engloba las directrices para el desarrollo seguro de los productos software el análisis y documentación de los requerimientos de seguridad y funcionalidad, la definición del equipo y plan de trabajo, el desarrollo de plan de trabajo y las pruebas de desarrollo, el despliegue en el ambiente de desarrollo y la ejecución de las pruebas de funcionalidad y seguridad, el ajuste a los hallazgos derivados de las pruebas, el despliegue en el

ambiente de producción y la ejecución de las pruebas de aceptación, el almacenamiento del código fuente y al realización de mantenimiento y actualizaciones. A través de este documento, se da respuesta a los requerimientos de identificación de requerimientos de entrada, revisión, verificación y validación requeridos por la norma de calidad a nivel de su numeral de 8.3 Diseño y desarrollo. En este mismo numeral, también se incluye el procedimiento de gestión de proyectos, el cual documenta los lineamientos para recibir, tramitar y gestionar el desarrollo de proyectos para la organización. Todos los documentos que soportan la documentación e implementación de este requisito de referencian en el Apéndice *P*.

En relación a los requisitos asociados al numeral 8.4 Control de los procesos, productos y servicios suministrados externamente, estos se documentaron e implementaron en el marco de los procedimientos del proceso de Gestión Administrativa, Financiera y del Talento Humano – GAF, el cual realiza la gestión para la selección, registro y evaluación de proveedores y contratistas, así como, la ejecución de las compras y subcontrataciones. Estos documentos se encuentran disponibles en el Apéndice *Q*.

Los lineamientos para el control de la producción y provisión del servicio, se documentaron a través de los procesos misionales de Gestión Comercial, en el cual se dan las especificaciones de los productos y servicios ofrecidos por la organización, el control operacional más destacado gestionado por este proceso es la identificación y análisis de los requisitos del cliente y el aseguramiento que los productos y servicios ofrecidos darán respuesta a las necesidades y expectativas de los mismos, así como, todos los procesos de legalización de las relaciones contractuales; por su parte, desde el proceso de Gestión de Proyectos y Desarrollo se realiza la estructura técnica y el desarrollo del portafolio de productos y servicios de la organización, que

corresponde a productos software móviles y web, dentro de los controles operacionales ejercidos por este proceso están: la valoración de capacidad técnica para el desarrollo de los requisitos del cliente, la evaluación de la funcionalidad y la seguridad de los productos y servicios y su respectiva documentación, la preservación de las pruebas correspondientes, el despliegue en los ambientes productos y el levantamiento de las pruebas de aceptación por parte del *producto owner* para los nuevos desarrollos; seguidamente se encuentran los procedimientos del proceso de Implementación y Soporte, a través de los cuales se realizan los procesos de implantación de los productos y servicios desarrollados en la infraestructura de los clientes, ejecutando los siguientes controles: asegurar la funcionalidad de los sistemas de integración entre los ERP de los clientes y la organización, la ejecución de las pruebas en ambiente de pruebas y posteriormente, los procesos de capacitación funcional de los usuarios y las respectivas pruebas de aceptación, siendo el soporte para la liberación de los productos. Finalmente, el subproceso de Soporte brinda, como su nombre lo indica, el soporte de la funcionalidad de los productos y servicios ofrecidos por la organización, se realiza atención de los casos de usuario de acuerdo a su categoría, siendo el principal control operacional del proceso el aseguramiento de la funcionalidad de los productos con un monitoreo permanente y la atención de los clientes post entrega. Como fue mencionado anteriormente, la liberación de los productos y servicios está controlado a nivel del subproceso de Implementación, a partir de las pruebas de aceptación por parte de los usuarios, esta entrega se acompaña de un tiempo de estabilización, posterior al cual, el soporte de los requerimientos de usuario es asumido por el subproceso de Soporte. El compendio de los documentos y soportes de implementación de estos controles se encuentra asociado al Apéndice *R*.

Por su parte, para el control de salidas no conformes se documentó y estableció un procedimiento con los lineamientos para la identificación y tratamiento de salidas no conformes.

De este control no se dispone de evidencias de implementación. El documento asociado se encuentra disponible en el Apéndice *S*.

El control específico de realizar la medición de la satisfacción del cliente, para el cual se documentó un instructivo para la medición de la satisfacción fue mencionado para el requisito de enfoque al cliente.

Finalmente, todos los controles específicos asociados a la seguridad de la información del anexo A de la norma NTC ISO/IEC 27001:2013se encuentran vinculados al Apéndice *T* y fueron estructurados de la siguiente manera: a nivel del control A.5 Políticas de seguridad de la información se documentó el P OTI 01 Compendio de Políticas Seguridad Información [i], en el cual se compilan todas las políticas que especifican los lineamientos de control de seguridad de la información. Para el control A.6 Organización de la seguridad de la información se respalda en el MN GAF 01 Manual de Funciones [i] ya mencionado a nivel de la definición de roles y responsabilidades, desde este documento se asegura la definición de responsabilidades de cara a la seguridad de la información para cada cargo, así como, la separación de los deberes. Este control se complementa con F OTI 01 Inventario de Activos [i] desde donde se especifica la asignación de la responsabilidad y custodia sobre los activos de información. Para este mismo control se vincula el A SIG 06 Directorio Contactos Autoridades - Emergencias y Grupos de Interés [i], donde se establecen los contactos con las principales autoridades y grupos de interés para asegurar el blindaje de los recursos de información. Por su parte, la seguridad de la información a nivel de los proyectos, se blinda a través de los lineamientos del PC GPD 03 Gestión de Proyectos [i]. Finalmente, en la misma categoría de controles y en relación a los dispositivos móviles se establece la política con el mismo nombre la cual se encuentra dentro del mismo documento del compendio

de políticas, adicionalmente, para regular la modalidad de trabajo de teletrabajo se dispone de una política con el mismo nombre y la especificación de la asignación de los activos de información a través del inventario como fue mencionado anteriormente.

Para el control A.7 Seguridad relativa a los recursos humanos se dispone de todos los lineamientos para la selección y vinculación a través del PC GAF 07 Selección, Vinculación y Evaluación de Desempeño [i], en donde se mencionan los controles para la contratación correspondientes a la verificación de antecedentes ante entes de control como la Procuraduría, Policía y Fiscalía. Adicionalmente, todos los términos de contratación están regidos por los tipos de contratación manejadas y las políticas y acuerdos de confidencialidad. Durante el empleo, los controles están regulados por el A GAF 01 Reglamento Interno de Trabajo [i], así como los acuerdos firmados para la cesión de derechos de autor y la autorización de tratamiento de datos personales. La toma de conciencia del personal de trabajo desde los procedimientos de inducción y reinducción, capacitación y entrenamiento, así como, del plan de capacitación. Por su parte, los procesos disciplinarios están orientados a través del INS GAF 02 Proceso disciplinario y los documentos asociados. Finalmente, la desvinculación laboral está reglamentada de acuerdo a los términos del PC GAF 06 Desvinculación Personal [i], así como, del F GAF 13 Acta Entrega de Cargo [i] donde se deja evidencia de la entrega de los activos asociados al cargo. Seguidamente en el control A.8 Gestión de activos, se tienen como herramientas para operativizar los controles el PC OTI 05 Gestión de Activos [i] y los inventarios correspondientes. Por su parte, una vez se da la desvinculación laboral se oficializa la devolución de los activos a través del acta de entrega de cargo, como fue mencionado anteriormente. En la misma categoría de los controles, el control A.8.2 respecto a la clasificación de la información se dispone de los lineamientos para su clasificación, etiquetado y manejo a través del PC SIG 02 Control Información Documentada [i],

así como, de la política para tal fin dispuesta en el compendio de políticas. Reconociendo a la información como un activo, a nivel del procedimiento gestión de activos y los inventarios respectivos también se dan lineamientos para su adecuado manejo. En relación al control A.8.3 del manejo de medios, se reglamente a través de la política de control de medios extraíbles, el procedimiento de borrado seguro y su respectivo informe de ejecución y el procedimiento de transferencia de información.

Para el control A.9.1 Requisitos de negocio para el control de acceso, se dispone de la política de control de accesos, redes y contraseñas en el marco del compendio de políticas, adicionalmente, se dispone del procedimiento PC OTI 06 Asignación de Usuarios [i] y los inventarios de accesos y credenciales de acceso, a través de los cuales se regula el registro y cancelación de usuarios, el suministro de accesos, los derechos de accesos privilegiados y el retiro y ajuste de los derechos de acceso. Por último, en relación al control de acceso al código fuente, este se regula de acuerdo a lo establecido en el PC GPD 01 Desarrollo Seguro [i], siendo que código fuente se encuentra en repositorio GitLab, siendo el líder y equipo de desarrollo sus custodios.

En lo relacionado al control A.10 Criptografía y controles asociados, éstos se encuentran regulados por la política de uso de controles criptográficos, principalmente. Respecto al control A.11 Seguridad física y del entorno se dispone de la política de control de accesos, redes y contraseñas, así como, del INS OTI 04 Instructivo de Seguridad Física y del Entorno [i] que ofrecen los principales lineamientos en la materia. Para lo relacionado a la respuesta a amenazas externas y ambientales, la organización estructuró el procedimiento de continuidad del negocio y su respectivo plan, para estar preparados a dar respuesta a condiciones de contingencia.

En relación a la seguridad de los equipos de acuerdo al control A.11.2 se tienen los siguientes controles: la política de control de accesos, redes y contraseñas, el procedimiento de mantenimiento correctivo y preventivo y su plan respectivo, así como, el cronograma de ejecución y la bitácora de registro de mantenimientos realizados. A estos controles se suman, el plan de emergencias del parque empresarial donde quedan ubicadas las instalaciones principales y el mismo procedimiento y plan de continuidad del negocio. En relación a la seguridad del cableado se dispone del A OTI 01 Diagrama de Red Amovil [i] en el que se valida conectividad inalámbrica para colaboradores y visitantes, por lo que no hay vulnerabilidad de cableado expuesto. En lo que respecta al retiro de activos, este se reglamente a través de la F GAF 37 Autorización Salida Equipos [i]. Se dispone además de las políticas de escritorio y pantalla limpia por la cual se da establece control al equipo desatendido y el escritorio de acceso principal de los equipos portátiles.

El control A.12 de seguridad de las operaciones se regula a través de todos los procedimientos técnicos que establecen los controles respectivos en los procesos y que están disponibles en el Repositorio Sharepoint. Las gestiones del cambio como ya fue mencionado se regulan por el procedimiento para cambios transversales del SIG y los específicos para el equipo de desarrollo. La gestión de capacidad se gestiona a través del procedimiento de seguimiento y monitoreo de la infraestructura tecnológica por el cual se realiza la monitorización del rendimiento de carga de los servidores y el mapeo de necesidades respectivas. Por su parte, la gestión del requerimiento de personal se gestiona a través del proceso GAF. La separación de los ambientes de desarrollo (pruebas y producción) se establece en el procedimiento de desarrollo seguro. A nivel de las protecciones de código malicioso se dispone de la política de desarrollo seguro, el acceso restringido al contenido web a través del firewall (Fortinet) y la consola antivirus. Las copias de respaldo se realizan de acuerdo a la política de *backups*, el procedimiento para tal fin, así como, la

restauración de las copias de seguridad. En lo que respecta al registro de eventos de seguridad, se estableció el PC OTI 12 Gestión de Requerimientos [i] y el PC OTI 11 Gestión de Incidentes [i] a través de los cuales se ofrecen los lineamientos para el registro y tratamiento de incidentes, a los cuales se les hace manejo y trazabilidad a través de las herramientas Amovildesk y Cervello. El control de acceso a los registros se regula a través del control de accesos físicos y digitales. Como implementación de la sincronización de relojes se estableció la política que establece la sincronización a la hora legal colombiana (http://horalegal.inm.gov.co/), sin excepción a ningún servidor, enrutador, equipo de cómputo, etc. Para el control de software operacional se documentó el PC OTI 07 Instalación y Actualización de Software [i] a través del cual se dan lineamientos para esta actividad y las respectivas restricciones de permisos de usuarios. A nivel de la gestión de vulnerabilidades técnicas se documentó el PC OTI 03 Gestión Vulnerabilidades Técnicas [i], F OTI 04 Plan Pruebas Plan de Contingencia [i] y F OTI 07 Plan de Acción Cierre Vulnerabilidades Técnicas [i] a través de los cuales se es establecen los lineamientos para las pruebas de vulnerabilidad y el establecimiento de los planes de acción para su atención prioritaria. Por último, las auditorías del sistema de información se ejecutan a través de los lineamientos del PC SIG 05 Auditoría Interna [i].

En lo que respecta al control A.13 asociado a la Seguridad de las Comunicaciones, se establecieron los lineamientos desde la política de control de acceso a las redes, adicionalmente se evidencian las políticas de seguridad del proveedor tecnológico de la organización (BTEC), con este proveedor se tienen contratado todos los procesos de monitoreo y control de los recursos de red. Adicionalmente, se documentó la política de control de acceso a las redes, en la cual se establece su respectiva separación. A nivel de la transferencia de información, se estableció la política para tal fin, así como el PC OTI 14 Transferencia de Información [i]. En este

procedimiento se detalla la transmisión de información a través de correo electrónico con aplicación de etiquetado como confidencial. Finalmente, en lo que respecta a los acuerdos de confidencialidad, los mismos se documentan y aplican para las diferentes partes interesadas así: A GAF 04 Acuerdo de Confidencialidad (Trabajadores)[i], A GAF 16 Acuerdo de Confidencialidad (Clientes, Contratista y Proveedores) [i].

En el control A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas, se documentó e implementó así: la gestión de seguridad del desarrollo se establece a través de los lineamientos del PC GPD 01 Desarrollo Seguro y la política del mismo nombre. En este mismo procedimiento, se establecen las pruebas de seguridad y de aceptación como controles de cumplimiento de los productos y servicios. Por su parte, en el PC GPD 02 Gestión de Cambios a Nivel de Desarrollo, se establecieron los lineamientos para los cambios en los ámbitos de desarrollo. A nivel de estos controles, también se detalla la no aplicabilidad del control A.14.2.7 Desarrollo contratado externamente, ya que corresponde a una exclusión de alcance para la organización, siendo que todos los desarrollos se ejecutan por personal directo. En lo relacionado a la relación con proveedores se dispone de la P GAF 01 Política de Proveedores y Contratistas[i] a través de ésta y de los documentos contractuales, autorizaciones y acuerdos se realiza la gestión con proveedores y contratistas.

Finalmente para los controles A 16 Gestión de incidentes de seguridad de la información, A 17 Aspectos de seguridad de la información para la continuidad del negocio y A 18 Cumplimiento de los requisitos legales y contractuales, la organización documento e implementó lineamientos como PC OTI Gestión Incidentes a Nivel de Servicio [i] a través del cual se da lineamientos para el reporte de incidentes a través de las plataformas establecidas por la

organización, indicando responsables de la recepción, evaluación, diagnóstico y ejecución de la corrección. A nivel de la continuidad, la organización estableció el PLN OTI 01 Plan Continuidad del Negocio [i], así como sus pruebas, plan de acción derivado y análisis de riesgo. A nivel legal, la organización realiza una identificación y gestión de los requisitos legales a través de la F SIG 11 Matriz de requisitos legales [i], asegurando la gestión de su implementación, la aplicación de otros requisitos legales como la protección de datos personales se gestiona a través de la P SIG 02 Política de tratamiento de datos personales y los acuerdos de confidencialidad con las partes interesadas. Finalmente, las revisiones de la seguridad de la información se establecieron a través de las auditorías internas y externas.

4.3 Fase de Validación

Como fue mencionado a nivel metodológico, la fase de validación fue ejecutada a través de un informe de validación por concepto de experto, en este particular, de la Ingeniera Alexandra Bibiana Cala, Auditor Líder y Auditor Certificado de Calidad y Especialista en Aseguramiento de la Calidad y en Alta Gerencia, con más de 22 años de experiencia laboral en la implementación y Auditoria de Sistemas de Gestión de Calidad, con una destacada experiencia en el manejo de las normas ISO 9000, ISO 31000, ISO 22301, ISO 27001 e ISO 37001.

Como conclusiones del informe de validación, la experta acotó las siguientes (Cala, 2023, pág. 84): a nivel de fortalezas resaltó la evidencia de un SIG bien estructurado, dando respuesta a la integración de manera adecuada y eficiente. Una destacada robustez documental que respalda a la gestión del conocimiento de la organización. Un importante volumen de evidencias de implementación para ambas normas, así como, una integración importante también de la documentación del SG SST.

A nivel de oportunidades desde el diseño y la implementación del SIG indicó: la sugerencia de vincular la información documentada de forma total e integrada del SG SST dentro del SIG, así como, la conveniencia de descentralizar la gestión del proceso GAF de acuerdo al crecimiento de la organización.

El concepto final del informe de validación (Cala, 2023, pág. 84) concluyó:

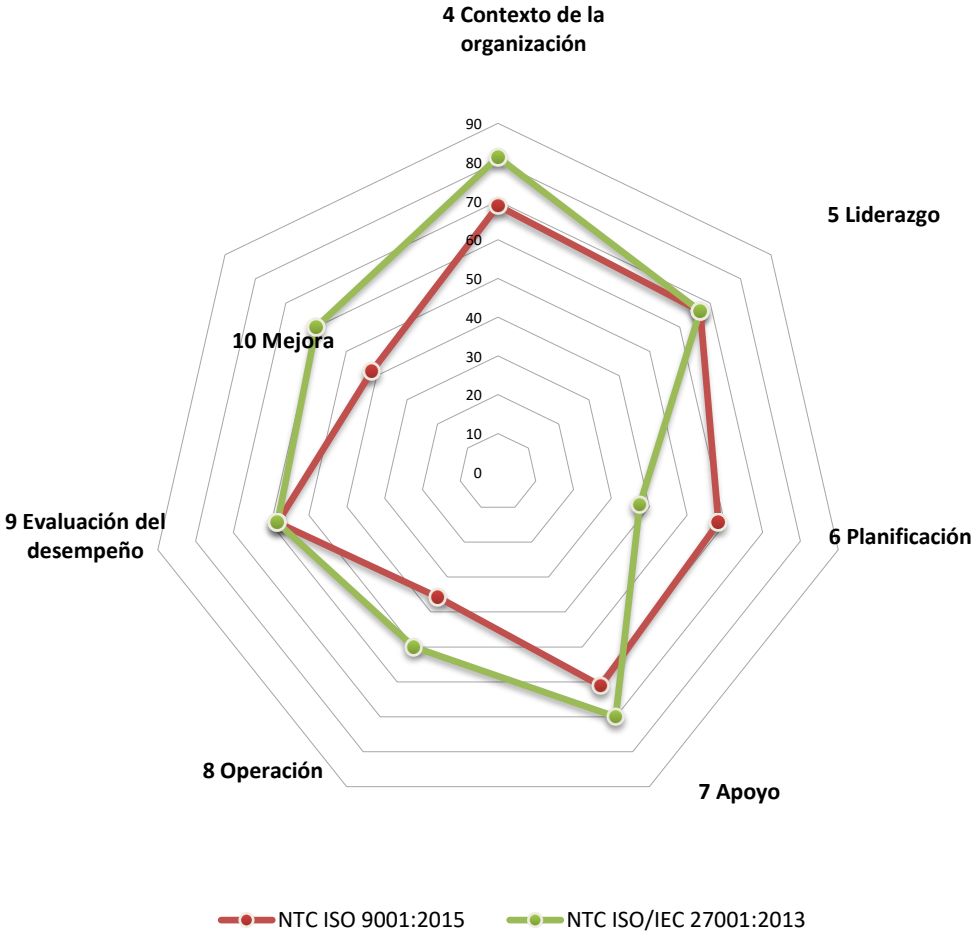
> Una vez validada la estructura y ejecución del diseño del Sistema Integrado de Gestión basado en los requisitos de las normas NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013 (incluyendo en el Anexo A), para todos los procesos de la empresa Asistencia Móvil S.A.S – AMOVIL, se concluye que el diseño asegura la adecuación, integración y en un importante porcentaje, la implementación de los requisitos, sin que se identifiquen hallazgos importantes que pudieran derivar en incumplimientos normativos y/o legales desde la evidencia documental.

El cuerpo completo del informe de validación está disponible y asociado al Apéndice U.

5. Conclusiones

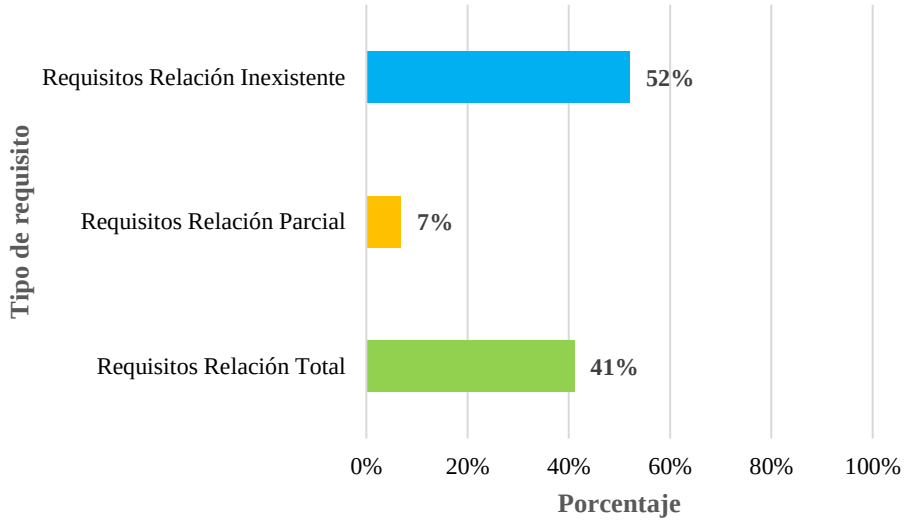
El desarrollo metodológico del diseño del Sistema Integrado de Gestión basado en las normas de calidad y seguridad de la información, dio lugar a importantes resultados, entre las cuales es posible destacar las siguientes: de la fase planificación y en particular en la etapa de diagnóstico preliminar, fue posible realizar un comparativo en el nivel de implementación logrado para cada uno de los capítulos principales de ambas normas, se identificó un apalancamiento del nivel de implementación de la norma NTC ISO 9001:2015 por el trabajo inicial realizado a nivel de la NTC ISO/IEC 27001:2013, también las mayores brechas en relación a la norma de calidad. Lo anterior, atribuible a que pese a la estructura de alta nivel que comparten ambas normas, la NTC ISO 9001 sigue siendo más específica en relación a los requisitos de gestión. Por tanto, para los numerales contexto, apoyo, operación y mejora se exhibieron niveles de implementación por debajo a los logrados para la NTC ISO 27001. Pese a ello, los resultados respaldaron la necesidad de la organización por abordar las brechas identificadas a nivel de la norma de calidad y su potencial impacto sobre sus bases organizacionales, así como, una valiosa oportunidad para realizar un robustecimiento de la madurez ya lograda a nivel de la gestión de la seguridad de la información. Lo anterior, se esquematiza con claridad en la Figura 17.

Figura 17. *Comparación del análisis de brecha de implementación de las normas NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013*



En lo que respecta a la etapa de diseño, el análisis de relación de requisitos de las normas NTC ISO 9001:2015 y la NTC ISO/IEC 27001:2013 se tomó como referente para la priorización del diseño e implementación a partir de la categorización de los requisitos basados en tres tipos: relación total (T), relación parcial (P) e inexistencia de relación (X), esto dio lugar a los porcentajes para cada tipo de requisito que se muestran en la Figura 18.

Figura 18. *Porcentajes de requisitos de las normas NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013 de acuerdo a su tipo de relación*

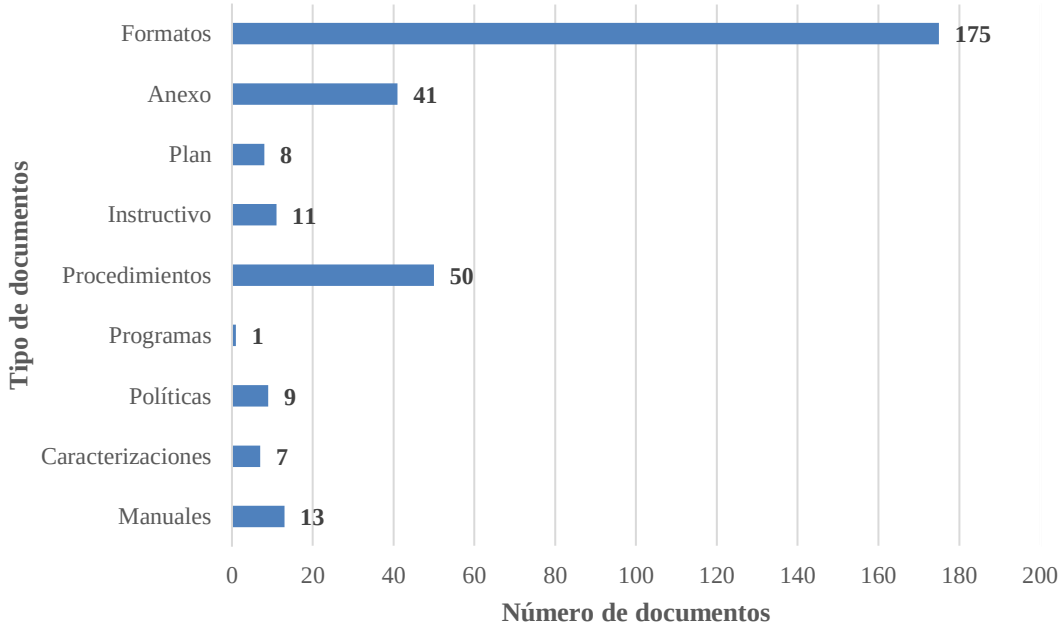


De acuerdo al análisis de tipo de relación se identificó que el 41% de los requisitos correspondieron a requisitos de relación total, requisitos sobre los cuales pudo aplicarse una gestión efectiva de integración abordando de forma global los requerimientos de ambas normas. Por su parte, el 7% de los requisitos fueron clasificados como requisitos de relación parcial, sobre los cuales, dando precisión a detalles específicos de una u otra norma se logró la integración completa. Por último y pese a ser el porcentaje mayoritario, el 52% de los requisitos fueron clasificados como requisitos de relación inexistente, en su mayoría correspondientes a los capítulos de operación que centralizan los objetos de estudio de ambas normas. En general, la estructura de alto nivel de las normas favorece en gran medida los procesos de integración, esto se suma al enfoque en procesos, en conjunto con el ciclo PHVA y el pensamiento basado en riesgos que corresponden a facilitadores integrativos.

Además en la etapa de diseño se documentaron las evidencias de implementación para un importante número de los requisitos de las normas del SIG, este trabajo no solo derivó en una

herramienta de capitalización y aseguramiento de la gestión del conocimiento de la organización, sino también en una oportunidad para complementar la integración con requisitos de otras normas dependiente del crecimiento y madurez de la organización, de forma más inmediata sobre los requisitos del Sistema de Gestión de Salud y Seguridad en el Trabajo, en donde se identifica la oportunidad de armonización con los requisitos legales del decreto 1072 del 2015.

Figura 19. *Tipos y números de documentos generados en el marco de la implementación del SIG*



En la Figura 19 se muestran los tipos y cantidades de documentos generados en el marco del proyecto, de acuerdo a la categoría de los mismos designados en el PC SIG 02 Control Información Documentada [i] de la organización. Toda esta documentación al término del proyecto quedó alojada en repositorio organizacional correspondiente al sitio Sharepoint del SIG de la empresa.

Por último, los resultados derivados del trabajo de diseño del SIG pese al no estar orientados en su objetivo al logro de la certificación combinada en las NTC ISO 9001:2015 y NTC ISO/IEC 27001:2013, si apalancaron de forma significativa el mantenimiento de la certificación en esta última norma, que logró la organización a través del proceso de auditoría externa con el ente de certificación SGS, tal como se muestra en el Apéndice V. Igualmente, ofreció herramientas valiosas para una próxima certificación combinada y robusteció las bases organizacionales de la empresa de estudio. Con esto puede concluirse, que al cierre del proceso el proyecto ha dado respuesta a las necesidades de la organización y ha aportado madurez al sistema de integrado de gestión.

Referencias

AENOR. (2018, abril). *La integración como aspecto clave de gestión*. Retrieved from https://revista.aenor.com/downloads/revistas/336.pdf?output=cb89826045209be82d30372af257f10e&output=66e1ddedd6842b680dd2b13c3cadcb2a

AMOVIL. (2021, Marzo 16). Conocimiento general de la organización. (C. Guerrero, Interviewer)

AMOVIL S.A.S. (201). A SIG 02 Mapa de Procesos AMOVIL [i]. 1-2. Colombia.

AMOVIL S.A.S. (2021). MN DE 01 Manual Direccionamiento Estratégico [i]. 1-16. Colombia.

AMOVIL S.A.S. (2020). Presentación Comercial Corporativa. 1. Bucaramanga, Santander, Colombia: AMOVIL.

Antúnez, V. (2016). Sistemas integrados de gestión: de la teoría a la práctica empresarial en Cuba. *Centro de Estudios de Técnicas de Dirección, 10*, 1-28. Cuba: Universidad de La Habana. Retrieved from http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2073-60612016000200001

ASANA. (2022, noviembre 12). *Cómo implementar el análisis de brechas para alcanzar los objetivos de negocios*. Retrieved julio 19, 2023, from https://asana.com/es/resources/gap-analysis

Asobancaria. (2018). *Supervivencia de las Mypime: un problema por resolver.* Cálculos Asobancaria. Retrieved from https://www.asobancaria.com/wp-content/uploads/1145.pdf

Cala, A. B. (2023). Informe de Validación - Diseño del Sistema Integrado de Gestión (NTC IOS 9001:2015 y NTC ISO/IEC 27001:2013) para la empresa AMOVIL. 1-84.

Calderón, L. (2015, septiembre 10). Seguridad informática y seguridad de la información. 1 - 7. Colombia: Universidad Piloto de Colombia. Retrieved from http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Confecámaras. (2017, agosto). Determinantes de la supervivencia empresarial en Colombia. 5 -25. Colombia: Confecámaras - Red de cámaras de comercio. Retrieved from https://confecamaras.org.co/phocadownload/Cuadernos_de_analisis_economico/Cuaderno_de_An%D0%B0lisis_Economico_N_14.pdf

Confecámaras. (2019). *Dinámica de creación de empresas en Colombia.* Bogotá: Confecámaras. Retrieved from https://confecamaras.org.co/analisis-economico

Confecámaras. (2020). *Dinámica de creación de empresas en Colombia.* Bogotá: Confecámaras. Retrieved from hhttps://confecamaras.org.co/analisis-economico

Confecámaras. (2021). *Resultados encuesta de las cámaras de comercio de seguimiento y monitoreo del impacto de la COVID-19 en el sector empresarial.* Bogotá: Confecámaras. Retrieved from

https://www.incp.org.co/Site/publicaciones/info/archivos/Encuesta-de-las-Camaras-de-Comercio.pdf

Cruz, M., López, E., C. R., & Meneses, G. (2016). ¿Por qué no crecen las micro y pequeñas empresas en México? *La micro y pequeña empresa: un análisis desde la perspectiva económico-adminsitrativa*, 329-339. México: ECORFAN y Universidad Tecnológica de Tecámac. Retrieved from https://gc.scalahed.com/recursos/files/r161r/w25506w/D1FZ102_S3_CRUZ.pdf

Cuestionario para la realización de auditoría interna de un sistema de gestión de la calidad. Norma ISO 9001:2015. (n.d.). 2-36. Hedera Consultores. Retrieved julio 19, 2023, from http://hederaconsultores.com/docs/Check-list-auditoria-ISO-9001-2015.pdf

D' Annunzio, M. C., & Carattoli, M. (2014). Proceso de crecimiento empresarial en pymes: Análisis de casos en el sector de Software y Servicios Informáticos. *2(2)*, 20-45. Revista Pymes, Innovación y Desarrollo. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6353884

de Faveri, D. B., dos Santos, V., & Leandro, D. A. (2014). Relación del ciclo de vida organizacional con la planificación: un estudio con empresas prestadoras de servicios contables del estado de Santa Catarina. *8(4)*, 383-403. Brasilia, Brasil: Revista de Educacao e Pesquisa em Contabilidade. Retrieved from https://www.redalyc.org/pdf/4416/441642786004.pdf

Dini, M., & Stumpo, G. (2019). Mipymes en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento. Síntesis. 5 - 489. Santiago, Chile: Comisión Económica para América Latina y el Caribe (CEPAL). Retrieved from https://www.cepal.org/es/publicaciones/44148-mipymes-america-latina-un-fragil-desempeno-nuevos-desafios-politicas-fomento

DispatchTrack. (2023). *Ciclo de PHVA: ejemplo práctico en logística de última milla*. Retrieved julio 19, 2023, from https://www.beetrack.com/es/blog/ciclo-de-deming-etapas-ejemplos

Duque, D. (2017). Modelo teórico para un sistema integrado de gestión (seguridad, calidad y ambiente). *Actualidad y Nuevas Tendencias, V*, 115-130. Carabobo, Venezuela: Universidad de Carabobo. Retrieved from https://www.redalyc.org/articulo.oa?id=215052403009

Editorial Etecé. (2022, junio 13). *Software*. Retrieved julio 19, 2023, from https://concepto.de/software/

Escobar, J., & Cuervo, A. (2008). Validez de contenido y juicio de expertos: una aproximación a su utilización. *Avances en medición, 6*, 27-36. Retrieved from https://www.humanas.unal.edu.co/lab_psicometria/revista-avances-en-medicion/avances-en-medicion-no6

Forbes, R. (2011). Implementación de sistemas de gestión integrados de calidad, ambiente, riesgos laborales y condiciones de trabajo. *Éxito Empresarial, 137*, 1-5. Costa Rica:

CEGESTI. Retrieved from http://www.cegesti.org/exitoempresarial/publicaciones/publicacion_137_140211_es.pdf

Franco-Ángel, M. (2019). Caracterización de las pymes colombianas y de sus fundadores: un análisis desde dos regiones del país. *Estudios Gerenciales, 35*(150), 81-91. Retrieved from https://doi.org/10.18046/j.estger.2019.150.2968

García, J. A. (2020). Diseño de un Sistema Integrado de Gestión basado en las normas ISO 9001:2015 e ISO 27001:2013, para la emisión de documentos deidentificación militar en la matriz de la Dirección de Movilización del Comando Conjunto de las Fuerzas Armadas. *Tesis de Maestría en Gerencia de la Calidad e Innovación.*, 1-241. Quito: Universidad Andina Simón Bolívar. Retrieved from http://hdl.handle.net/10644/7623

Gisbert, V., & Esengeldiev, R. (2014). Sistemas Integrados de Gestión y los beneficios. *3C Empresa*, 246-257. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=4924486

Gorgona, L. (2021). Construyendo un modelo de madurez para COBIT 2019 basado en CMMI. *6*, 1-3. ISACA Journal. Retrieved from https://www.isaca.org/es-es/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi

Heras, I., Bernando, M., & Casadesús, F. (2007, Diciembre). La integración de sistemas de gestión basados en estándares internacionales: resultados de un estudio empírico realizado e la CAPV. 155-174. Revista de Dirección y Administración de Empresas.

Hernández, H. G., Barrios, I., & Martínez, D. (2018, Agosto 3). Gestión de la calidad: elemento clave para el desarrollo de las organizaciones. *Criterio Libre*, *16*(28), 169-185. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6676025

ICONTEC. (2013, diciembre 11). NTC-ISO-IEC 27001:2013 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. 1. Bogotá, Colombia.

ICONTEC. (2015, noviembre 15). NTC ISO 9000:2015 Sistemas de gestión de la calidad - Fundamentos y vocabulario. 1-33. Bogotá, Colombia. Retrieved from https://ecollection-icontec-org.crai-ustadigital.usantotomas.edu.co/pdfview/viewer.aspx?locale=en-US&Q=0F9C3861121C65A9F3BDCDFB1B0D4A06312408EA304CDFA9&Req=

ICONTEC. (2015, septiembre 23). NTC-ISO 9001:2015 Sistemas de gestión de la calidad. Requisitos. i - v. Bogotá, Colombia. Retrieved from https://ecollection-icontec-org.crai-ustadigital.usantotomas.edu.co/pdfview/viewer.aspx?locale=en-US&Q=EF8F94009513D3732979E86636AA01B2312408EA304CDFA9&Req=

ICONTEC. (2018, octubre 17). *Guía Técnica Colombiana GTC-ISO 19011*. (ICONTEC, Editor) Retrieved julio 19, 2023, from https://ecollection-icontec-org.crai-

ustadigital.usantotomas.edu.co/pdfview/viewer.aspx?locale=en-US&Q=5F29777199BF9D51EA0D058C7CDA824696DF3D9C2A164539&Req=

ICONTEC. (2021). GTC-ISO 10014:2021. Sistemas de gestión de la calidad. Gestión de una organización para resultados de calidad. Orientación para obtener beneficios financieros y económicos. 18. Colombia. Retrieved from https://ecollection-icontec-org.crai-ustadigital.usantotomas.edu.co/pdfview/viewer.aspx?locale=en-US&Q=2F484ECE152BBFA05DF8A0420554F89E96DF3D9C2A164539&Req=

ISO 27001. (2013). Referencias normativas ISO 27000. Retrieved julio 19, 2023, from https://normaiso27001.es/referencias-normativas-iso-27000/#terminos

Lacayo, M. H., & García, S. L. (2013). Principales problemas que impiden la permanencia y crecimiento de ls pequeñas y medianas empresas mexicanas. 1 - 22. México: Universidad Autónoma del Estado de México. Retrieved from http://www.aeca1.org/pub/on_line/comunicaciones_aal2011/cd/62c.pdf

Méndez, F. (2020, Julio 6). Webinar - Alianza del Pacífico en el medio del COVID-19 [video]. Youtube. Asociación Nacional de Empresarios (ANDI). Retrieved from https://www.youtube.com/watch?v=yHYFhobYlO0

Mesquida, A. (2012, Mayo). Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros [Tesis de doctorado]. *Tesis doctoral para optar al grado de Doctor en Informática por la Universitat de les Illes Balears*, 92-105.

España: Universitat de les Illes Balears. Retrieved from http://hdl.handle.net/11201/2693

Miguel, J. L. (2013). Especificación de los requisitos comunes del sistema de gestión como marco para la integración. *Universidad*, 8-12. Retrieved from https://www.aec.es/c/document_library/get_file?uuid=d4f00264-ee74-4abd-b1c8-4e48fccd6836&groupId=10128

Ministerio de Comercio, Industria y Turismo. (2022, noviembre 9). *Seis consejos para mejorar la calidad y la productividad en las mipymes*. Retrieved julio 19, 2023, from https://www.colombiaproductiva.com/ptp-comunica/noticias/seis-consejos-para-mejorar-la-calidad-y-la-product

Ministerio de Trabajo. (2019, Septiembre 26). *MinTrabajo*. Retrieved julio 19, 2023, from MiPymes representan más del 90% del sector productivo nacional y generan el 80% del empleo en Colombia: ministra Alicia Arango: https://www.mintrabajo.gov.co/prensa/comunicados/2019/septiembre/mipymes-representan-mas-de-90-del-sector-productivo-nacional-y-generan-el-80-del-empleo-en-colombia-ministra-alicia-arango

Mora, E. H., Vera, M. A., & Melgarejo, Z. A. (2013, Enero). Planificación estratégica y niveles de competitividad de las Mipymes del sector comercio en Bogotá. *Estudios Gerenciales, 31*(134), 80-87. Retrieved from https://www.redalyc.org/articulo.oa?id=21233043009

Murrieta, Y. A., Ochoa, E., & Carballo, B. (2020). Reflexión crítica de los sistemas de gestión de calidad: ventajas y desventajas. *En-Contexto Revista de Investigación en Administración, Contabilidad, Economía y Sociedad*, 115-124.

NQA Organismo de certificación global. (n.d.). Sistemas de gestión integrados. España: NQA. Retrieved julio 19, 2023, from https://www.nqa.com/es-ca/certification/systems/integrated-management-systems

Ortega, D. C., Bustamante, M. O., Gutiérrez, D. F., & Correa, A. A. (2015, Febrero). Mixture experiments in industrial formulations. *DYNA, 82*(189), 149-156. Retrieved from http://www.scielo.org.co/pdf/dyna/v82n189/v82n189a19.pdf

Palacios, M. (2019, Mayo 24). Nueva metodología desarrollada para la integración de Lean Manufacturing, Kaizen e ISO 31000:2009 basados en la ISO 9001:2015. *3C Empresa. Investigación y pensamiento crítico, 8*(2), 12-43. doi:http://dx.doi.org/10.17993/3cemp.2019.080238.12-43

Parra, J. A., Hernández, H. L., & y Rodríguez, Y. L. (n.d.). Medición del nivel de integración de los sistemas de gestión en las organizaciones colombianas. 1-17. Bucaramanga, Colombia: Universidad Santo Tomás. Retrieved from hhttps://repository.usta.edu.co/bitstream/handle/11634/14188/2018haideehernandez2.pdf?sequence=3&isAllowed=y

Pineda, J. (2017). Guía para la implementaciòn de un Sistema de Gestión Integrado ISO 9001:2015 e ISO/IEC 27001:2013. *Monografía para optar por el título de*

Especialista en Gerencia de la Calidad., 14 - 68. Bogotá, Colombia: Fundación Universidad de América. Retrieved from http://repository.uamerica.edu.co/bitstream/20.500.11839/7009/1/882119-2017-I-GC.pdf

Platero, L. C., & Arias, C. (2019). Factores críticos de estancamiento en el crecimiento de empresas Gacela. 4 - 26. Bogotá D.C., Colombia: Universidad de los Andes. Retrieved from https://repositorio.uniandes.edu.co/bitstream/handle/1992/45731/u827977.pdf?sequence=1&isAllowed=y

Quintero, M. (2014, Junio 8). Sistema de gestión de calidad en las pymes colombianas. *Trabajo de grado Especialización de Control Interno*. Bogotá, Colombia: Universidad Militar Nueva Granada. Retrieved from http://hdl.handle.net/10654/13450

Rave, E. D., & Moreno, J. E. (2023). *Los retos gerenciales en la transición generacional en las Mipymes familiares: casos de estudio aplicados.* Envigado: Institución Universitaria de Envigado. Retrieved from https://www.iue.edu.co/wp-content/uploads/2023/03/Los-retos-gerenciales-en-la-transicion-generacional-en-las-Mipymes-familiares.pdf

Rincón, L. A. (2019). Estructuración del Sistema Integrado de Gestión F1 TOP POINT con base en las normas ISO 9001:2015, ISO 27001:2013, ISO 45001:2018 e ISO

14001:2015. *Informe de pasantía para optar por el título de Ingeniero Industrial.* Bogotá, Colombia: Universidad Distrital Francisco José de Caldas. Retrieved from https://repository.udistrital.edu.co/handle/11349/23786

Sandoval, J. H., & Guerrero, D. E. (2010). Empresas familiares en Colombia: hacia la construcción de un modelo de gestión comercial. *U.D.C.A Actualidad & Divulgación Científica*, 135-146. Retrieved from https://revistas.udca.edu.co/index.php/ruadc/article/view/717/747

Santana, L. (2017, Abril-Junio). Determinantes de supervivencia de microempresas en Bogotá: análisis con modelos de duración. *Revista INNOVAR, 27*(64), 51-61. Retrieved from http://www.scielo.org.co/pdf/inno/v27n64/v27n64a05.pdf

Significados. (n.d.). Diagnóstico (Qué es, significado y definición). Retrieved julio 19, 2023, from https://www.significados.com/diagnostico/

Significados. (n.d.). Significado de Diseño. Significados. Retrieved julio 19, 2023, from https://www.significados.com/diseno/

Significados. (n.d.). Significado de Integración. Significados. Retrieved julio 19, 2023, from https://www.significados.com/integracion/

Triana, J. (2020). *Propuesta metodológica para la armonización del sistema de gestión documental con los sistemas de gestión de calidad y seguridad de la información en una institución de educación superior acreditada.* Retrieved from http://hdl.handle.net/11634/27499

Trujillo, E. A., Gamba, M., & Arenas, L. M. (2016). *Las dificultades de las Pymes en América Latina y Colombia para lograr ser competitivas y sostenibles.* Retrieved from http://hdl.handle.net/20.500.12010/3784

Apéndices

Apéndice A. *Hoja de vida experta – Ing. Alexandra Bibiana Cala Moreno*
Nota: véase archivo en fuente externa

Apéndice B. *Diagnóstico preliminar - consolidado de resultados de análisis de brechas – NTC ISO 9001:2015, NTC ISO/IEC 27001:2013 y Anexo A*

Nota: véase archivo en fuente externa.

Apéndice C. *Contexto - 4.1 y 4.2 Comprensión contexto y partes interesadas*
Nota: véase archivo en fuente externa.

Apéndice D. *Contexto - 4.3 y 4.4 Determinación del alcance SIG y sus procesos*
Nota: véase archivo en fuente externa.

Apéndice E. *Liderazgo – 5.1, 5.2 y 5.3 Liderazgo, política y roles y responsabilidades*
Nota: véase archivo en fuente externa.

Apéndice F. *Planificación – 6.2 Objetivos SIG y su planificación*
Nota: véase archivo en fuente externa.

Apéndice G. Apoyo – 7.1, 7.2, 7.4 y 7.5 Recursos, competencia, comunicación e información documentada

Nota: véase archivo en fuente externa.

Apéndice H. Evaluación desempeño – 9.1, 9.2 y 9.3 Seguimiento y medición, auditoría interna y revisión por la dirección

Nota: véase archivo en fuente externa.

Apéndice I. *Mejora – 10.2 y 10.3 No conformidad, acción correctiva y mejora continua*
Nota: véase archivo en fuente externa.

Apéndice J. *Apéndice J: Contexto – 4.4 SIG y sus procesos*
Nota: véase archivo en fuente externa.

Apéndice K. *Planificación - 6.1 Acciones para abordar riesgos y oportunidades*
Nota: véase archivo en fuente externa.

Apéndice L. *Liderazgo – 5.1.2 Enfoque al cliente*

Nota: véase archivo en fuente externa.

Apéndice M. *Planificación – 6.3 Planificación de los cambios*

Nota: véase archivo en fuente externa.

Apéndice N. *Apoyo – 7.1.2, 7.1.3, 7.1.4, 7.1.6 Personas, infraestructura, ambiente de operación y conocimientos de la organización*

Nota: véase archivo en fuente externa.

Apéndice O. *Operación – 8.1 y 8.2 Planificación y control operacional y requisitos para los productos y servicios*

Nota: véase archivo en fuente externa.

Apéndice P. *Operación – 8.3 Diseño y desarrollo*
Nota: véase archivo en fuente externa.

Apéndice Q. *Operación – 8.4 Control de los procesos, productos y servicios suministrados externamente*

Nota: véase archivo en fuente externa.

Apéndice R. *Operación – 8.5 y 8.6 Producción, provisión del servicio y Liberación de los productos y servicios*

Nota: véase archivo en fuente externa.

Apéndice S. *Operación – 8.7 Identificación y control de salidas no conformes*

Nota: véase archivo en fuente externa.

Apéndice T. *Operación – Anexo A Controles de seguridad de la información*
Nota: véase archivo en fuente externa.

Apéndice U. *Informe de validación por concepto de experto*
Nota: véase archivo en fuente externa.

Apéndice V. *Reporte resumido – Certificación de sistema de gestión SGS (auditoría externa)*
Nota: véase archivo en fuente externa.